NAJWYŻSZA IZBA KONTROLI
Delegatura w Krakowie

LKR – 4101-017-03/2014
P/14/004

WYSTĄPIENIE POKONTROLNE

NAJWYŻSZA IZBA KONTROLI
Delegatura w Krakowie
ul. Łobzowska 67, 30-038 Kraków
T +48 12 342 34 00, F +48 12 342 34 44
lkr@nik.gov.pl

I. Dane identyfikacyjne kontroli

Numer i tytuł kontroli	P/14/004 - Wdrażanie wybranych wymagań dotyczących systemów teleinformatycznych, wymiany informacji w postaci elektronicznej oraz Krajowych Ram Interoperacyjności na przykładzie niektórych urzędów gmin miejskich i miast na prawach powiatu.
Jednostka przeprowadzająca kontrolę	Najwyższa Izba Kontroli Delegatura w Krakowie
Kontroler	Małgorzata Kram, specjalista k.p., upoważnienie do kontroli nr 88153 z 10 lipca 2014 r. (dowód: akta kontroli str. 1 do 2)
Jednostka kontrolowana	Urząd Miejski w Chrzanowie, 32 – 500 Chrzanów, Al. Henryka 20 (*Urząd*)
Kierownik jednostki kontrolowanej	Ryszard Kosowski, Burmistrz Miasta i Gminy Chrzanów (*Burmistrz*)

Ocena ogólna[1]

II. Ocena kontrolowanej działalności

W Urzędzie podjęto działania w celu zapewnienia interoperacyjności systemów informatycznych, o czym świadczy spełnianie przez pięć skontrolowanych systemów[2] minimalnych wymogów w tym zakresie. Interoperacyjność uzyskano poprzez wzajemną komunikację (na poziomach informacyjnym, jednostronnym i dwustronnym) oraz udostępnianie danych w formatach określonych w rozporządzeniu KRI[3]. Zapewniono również właściwy dostęp do informacji dla osób niepełnosprawnych poprzez odpowiednie przygotowanie strony internetowej Urzędu. Prawidłowo rozwijano elektroniczną interakcję wewnątrz Urzędu (system elektronicznego obiegu dokumentów tzw. INTRADOK), a także w komunikacji z innymi urzędami. Należy jednak zauważyć, że w Urzędzie, jako podstawowy sposób obiegu dokumentów wskazano, zgodnie z przyjętą Instrukcją Kancelaryjną, formę papierową i taka została zachowana, tj. pisma kierowane z Urzędu (m.in. do MUW) były archiwizowane w formie papierowej (oryginały, bądź wydruki) i do czasu niniejszej kontroli nie rozpoczęto prac nad wprowadzeniem kolejnych usług elektronicznych, poprzestając na trzech usługach dostępnych standardowo poprzez platformę ePUAP (pismo ogólne, wniosek o dopisanie do spisu wyborców i możliwość złożenia skarg lub wniosków). Urząd nie wspierał modelu usługowego w zakresie świadczenia usług elektronicznych. W każdej z trzech usług dostępnych elektronicznie w Urzędzie jako ich właściciela wskazano ogólnie Urząd (bez podania nazwy komórki organizacyjnej lub osoby odpowiedzialnej), nie sporządzono także kart opisu usługi, ani nie wskazano maksymalnego czasu niedostępności usługi, sposobu zgłaszania awarii czy technicznego właściciela usługi (tj. ePUAP[4]).

W Urzędzie w 2014 r. (po przeprowadzeniu na przełomie lat 2013/2014 audytu wewnętrznego) zintensyfikowano działania w sprawie nadzoru i zarządzania

[1] Najwyższa Izba Kontroli stosuje 3-stopniową skalę ocen: pozytywna, pozytywna mimo stwierdzonych nieprawidłowości, negatywna. Jeżeli sformułowanie oceny ogólnej według proponowanej skali byłoby nadmiernie utrudnione, albo taka ocena nie dawałaby prawdziwego obrazu funkcjonowania kontrolowanej jednostki w zakresie objętym kontrolą, stosuje się ocenę opisową, bądź uzupełnia ocenę ogólną o dodatkowe objaśnienie. W niniejszym wystąpieniu pokontrolnym zastosowano ocenę opisową.

[2] systemy: Kadry-Płace; Ewidencja Ludności i Rejestr Wyborców; KGM - system do obsługi gospodarki mieniem gminnym; PB USC - system Urzędu Stan Cywilnego (USC); INTRADOK - system elektronicznego obiegu dokumentów.

[3] Rozporządzenie KRI – rozporządzenie 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 2012 r., poz. 526).

[4] Elektroniczna Platforma Usług Administracji Publicznej.

bezpieczeństwem systemów informatycznych, w tym zapewnienia bezpieczeństwa danych przetwarzanych w Urzędzie. Kontrola wykazała m.in., że w czerwcu i lipcu 2014 r.:

- zaktualizowano i udoskonalono system zarządzania bezpieczeństwem informacji;
- wprowadzono elektroniczną inwentaryzację sprzętu komputerowego i jego oprogramowania;
- wprowadzono wzór dokumentu nadawania stosownych uprawnień użytkownikom systemów informatycznych wykorzystywanych w Urzędzie oraz zablokowano możliwość instalacji nieautoryzowanego oprogramowania na wszystkich dziesięciu poddanych oględzinom komputerach;
- rozpoczęto kolejny wewnętrzny audyt w zakresie bezpieczeństwa informacji.

Ponadto stwierdzono, że zapisy w umowach zawieranych przez Urząd w latach 2012–2014 zabezpieczały zagwarantowanie poufności informacji znajdujących się na nośnikach danych.

Kontrola wykazała jednak:

- brak przeszkolenia w zakresie bezpieczeństwa informacji wszystkich pracowników zaangażowanych w proces przetwarzania informacji;
- zaniechanie dokumentowania przez Administratora Bezpieczeństwa Informacji (*ABI*) odbierania lub zmieniania uprawnień użytkownikom, mimo ustalonych w tym zakresie procedur, zaniechano również sporządzania w tych sprawach pisemnych wniosków kierowników komórek organizacyjnych oraz pozostawienie na 7 notebookach (na 9 skontrolowanych) uprawnień administratora.

W ocenie NIK zarządzanie bezpieczeństwem informacji, mimo niespełnienia wszystkich warunków, o których mowa w rozporządzeniu KRI oraz w PN[5], nie spowodowało zagrożenia systemu bezpieczeństwa systemów IT, niemniej jednak działania Burmistrza w tym zakresie wymagają wzmożenia.

NIK zwraca uwagę, ze chociaż Urząd był przygotowany do świadczenia usług elektronicznych[6] jednak nie zaplanowano i nie podjęto działań zmierzających do popularyzacji komunikacji elektronicznej wśród obywateli i jej rozwoju nie wykonano badań zmierzających do poznania zapotrzebowania na takie usługi . Na stronach internetowych Urzędu i BIP nie zamieszczono linków (odsyłaczy) do trzech usług realizowanych elektronicznie w Urzędzie, poprzestając na zamieszczeniu ogólnego przekierowania do platformy ePUAP. Urząd, zdaniem NIK, nie wykorzystał w pełni posiadanych zasobów organizacyjnych i technicznych dla zwiększenia wykorzystania komunikacji elektronicznej wewnątrz i na zewnątrz jednostki, a w szczególności nie dążył do poszerzenia zakresu wykorzystywania elektronicznych form komunikacji, np. poprzez zwiększenie liczby formularzy elektronicznych, co mogłoby wpłynąć na usprawnienie działania jednostki.

III. Opis ustalonego stanu faktycznego

1. Dostosowanie systemów teleinformatycznych do współpracy z innymi systemami/rejestrami

1.1. Elektroniczne świadczenie usług w dokumentach strategicznych gminy

Opis stanu faktycznego

Kierunki rozwoju Gminy na najbliższe lata ustalono w styczniu 2005 r. w Strategii Rozwoju Gminy Chrzanów na lata 2004 – 2015 (Strategia). Wśród 5 celów strategicznych zagadnienia dotyczące dostosowania Urzędu do elektronicznego świadczenia usług publicznych określono w jednym z kierunków rozwoju pn. „Urząd przyjazny petentowi". Do osiągnięcia tego celu zaplanowano następujące zadania: budowa zintegrowanej platformy urzędu elektronicznego – informatyzacja Urzędu Miejskiego w Chrzanowie i jednostek

[5] Polskiej Normie Technika informatyczna. Techniki bezpieczeństwa. Systemy zarządzania bezpieczeństwem informacji (PN-ISO/EIC 27001:2007).

[6] M.in. wprowadzenie systemu INTRADOK zintegrowanego z ePUAP oraz prowadzenie korespondencji w z innymi jednostkami administracji w sposób elektroniczny.

organizacyjnych; wspieranie rozwoju społeczeństwa informacyjnego w Gminie poprzez integracje systemów informatycznych Urzędu, jednostek organizacyjnych i placówek edukacyjnych; wdrażanie systemów zarządzania jakością wg normy ISO. W Strategii nie określono zakresu działań ani ram czasowych i wielkości wskaźnika (np. liczby udostępnionych usług przez internet) jakie zamierzano osiągnąć w kolejnych latach.

(dowód: akta kontroli str. 42,43, 65, 84)

1.2. Promowanie komunikacji elektronicznej

Opis stanu faktycznego

Strategia Gminy nie zawierała informacji o sposobach promowania komunikacji elektronicznej przez Urząd lub przez kierownika jednostki, nie przyjęto i nie wdrażano programu promocji w ww. zakresie.

(dowód: akta kontroli str. 42,43, 65, 84, 127)

Burmistrz wyjaśnił, że Gmina przewiduje rozwój świadczenia usług elektronicznych w latach 2015 do 2018 co zostanie uwzględnione w aktualizacji Strategii planowanej na 2015 r.

(dowód: akta kontroli str. 139)

1.3. Ankiety lub inne formy poznania potrzeb mieszkańców gminy odnośnie elektronicznej formy komunikacji

Opis stanu faktycznego

W Urzędzie nie dokonywano analiz potrzeb promocyjnych w zakresie komunikacji elektronicznej, nie przeprowadzano ankiet lub innych form poznania potrzeb mieszkańców Gminy dotyczących potrzeb korzystania z elektronicznej formy komunikacji z Urzędem.

(dowód: akta kontroli str. 42 do 43)

Uwagi dotyczące badanej działalności

Zdaniem NIK poznanie potrzeb obywateli i ich oczekiwań w zakresie dostępności do usług elektronicznych jest warunkiem zapewnienia sprawnego świadczenia takich usług przez Urząd. Zwiększenie udziału komunikacji elektronicznej w świadczeniach publicznych realizowanych przez Urząd i zorientowanie na rozwój i poszerzenie usług elektronicznych pozwoliłoby na usprawnienie pracy Urzędu.

1.4. Korespondencja z Ministrem Administracji i Cyfryzacji

Opis stanu faktycznego

Po wejściu w życie rozporządzenia KRI, Urząd nie zwracał się do Ministra Administracji i Cyfryzacji (*MAiC*) z problemami ani z prośbą o pomoc w zakresie dostosowania swoich systemów/rejestrów informatycznych do wymogów KRI.

(dowód: akta kontroli str. 17, 19)

1.5. Procedury regulujące komunikację elektroniczną w Urzędzie

Opis stanu faktycznego

Podstawowym sposobem dokumentowania przebiegu załatwiania i rozstrzygania spraw w Urzędzie był tradycyjny („papierowy") system wykonywania czynności kancelaryjnych, co ustalono zarządzeniem w sprawie przyjęcia Instrukcji Kancelaryjnej

(dowód: akta kontroli str. 19, 54 do 60)

Czynności w Urzędzie były realizowane stosownie do zapisów Rozdziału 3 rozporządzenia Prezesa Rady Ministrów z dnia 18 stycznia 2011 r. w sprawie instrukcji kancelaryjnej, jednolitych rzeczowych wykazów akt oraz instrukcji w sprawie organizacji i zakresu działania archiwów zakładowych[7]. Zarządzeniem nr 693/11 Burmistrza Miasta Chrzanowa z dnia 29 grudnia 2011 r. wskazano tradycyjny system wykonywania czynności kancelaryjnych jako podstawowy sposób dokumentowania przebiegu załatwiania i rozstrzygania spraw w Urzędzie Miejskim w Chrzanowie, z możliwością korzystania z narzędzi informatycznych do wspomagania procesu obiegu dokumentów w tej postaci.
Urząd korzystał równocześnie z elektronicznego systemu obiegu dokumentów (INTRADOK), do którego były automatycznie przekierowywane pisma składane za pośrednictwem platformy ePUAP. Integracja systemów została dokonana 30 listopada 2011 r. co zostało potwierdzone stosownym protokołem.

[7] Dz.U. z 2011 r., Nr 14, poz. 67

Pisma wpływające do Urzędu (w tym za pośrednictwem ePUAP) były rejestrowane w INTRADOK. W przypadku dokumentów składanych w formie tradycyjnej były one skanowane i wprowadzane do systemu INTRADOK, który automatycznie nadawał mu kolejny numer w rejestrze. Pracownik dziennika podawczego przekazywał wydrukowane/otrzymane dokumenty do Burmistrza celem dekretacji (dokumentacja przekazywana wyłącznie w formie papierowej). Po zadekretowaniu dokumenty przekazywano do wydziałów merytorycznych oraz równolegle przesyłano za pomocą systemu INTRADOK do skrzynek poczty elektronicznej naczelników/kierowników komórek organizacyjnych. Odbiór wiadomości był odnotowywany automatycznie w systemie. Dokumenty robocze były tworzone z wykorzystaniem zasobów sieciowych Urzędu i tylko w niektórych przypadkach drukowane do akt sprawy. Projekty odpowiedzi sporządzane w obiegu wewnątrz Urzędu i podpisane/wysłane dokumenty do obywateli nie były skanowane do systemu INTRADOK. W przypadku gdy strona zażyczyła sobie odpowiedzi w formie elektronicznej wtedy dokument był skanowany z wersji papierowej lub generowany do pdf i podpisywany elektronicznie. W Urzędzie na dzień 31 lipca 2014 r. 30 osób spośród 153 pracowników Urzędu miało aktualny kwalifikowany podpis elektroniczny.

(dowód: akta kontroli str. 54 do 60)

1.6. Liczba złożonych dokumentów / wniosków / podań

Opis stanu faktycznego

W okresie od 31 maja 2012 r. do 31 maja 2014 r. złożono do Urzędu 85.932 dokumenty, w tym 9.875 w formie elektronicznej (w tym 4.692 poprzez ePUAP, pozostałe złożono pocztą elektroniczną). Wśród przesłanych pocztą elektroniczną skanów dokumentów były m.in.: akty stanu cywilnego, deklaracje podatkowe, wezwania sądowe, informacje podatkowe. Przykładowo wśród złożonych 40 skarg i wniosków dwie złożono w formie elektronicznej a wśród 312 wniosków o udzielenie informacji publicznej większość z nich (245) złożono w formie elektronicznej.

(dowód: akta kontroli str. 15 do 16)

Usługi elektroniczne realizowane były za pośrednictwem platformy ePUAP i poczty elektronicznej a ich liczba nie przekraczała 13% – w tym ok. 6% stanowiły sprawy przekazane poprzez ePUAP.

(dowód: akta kontroli str. 13 do 14, 15 do 16)

1.7. Zgodność opisu usług elektronicznych z usługami Urzędu

Opis stanu faktycznego

Według stanu na 30 maja 2012 r., tj. przed wejściem w życie rozporządzenia KRI Urząd świadczył dwie usługi elektroniczne. Obywatel miał możliwość złożenia dwóch dokumentów (pismo ogólne oraz wniosek o dopisanie do rejestru wyborców). W czasie niniejszej kontroli stwierdzono, że istniała możliwość realizacji trzech usług elektronicznych za pośrednictwem ePUAP, tj.:

1) wniosku o dopisanie do spisu wyborców;
2) pisma ogólnego do Urzędu;
3) skarg, wniosków, zapytań do Urzędu.

Liczba usług, które można było zrealizować elektronicznie (po wejściu w życie rozporządzenia KRI), wzrosła w badanym okresie z dwóch do trzech.

(dowód: akta kontroli str. 44 do 51)

Opisy usług świadczonych na platformie ePUAP zawierały ogólne dane dotyczące podmiotu (w każdym przypadku Urząd), miejsce świadczenia usługi – opisane jako siedziba Urzędu i aktualną podstawę prawną, natomiast nie zawierały opisu usługi. W odniesieniu do ww. trzech usług w dniu oględzin stwierdzono, że na stronie internetowej Urzędu oraz BIP nie zamieszczono ani formularzy wniosków ani opisów trzech procedur dostępnych przez ePUAP. W żadnym z ww. przypadków (trzech badanych usług) na stronach Urzędu lub BIP nie zamieszczono informacji o możliwości złożenia pism poprzez ePUAP ani linków do odpowiednich formularzy. Poprzestano na zamieszczeniu na głównej stronie Urzędu ogólnego linku do platformy ePUAP.

(dowód: akta kontroli str. 3 do 12, 44 do 51)

1.8. Opisy procedur elektronicznego załatwiania spraw w BIP

Opis stanu faktycznego

Dla udostępnionych przez Urząd trzech usług elektronicznych (wniosek o dopisanie do spisu wyborców, pismo ogólne do Urzędu, pismo w sprawie skarg i wniosków) nie zamieszczono karty opisu usługi ani na stronie Urzędu ani na stronie BIP.

(dowód: akta kontroli str. 3 do 12, 44 do 51)

Uwagi dotyczące badanej działalności

Zdaniem NIK, zamieszczenie ogólnego linku do platformy ePUAP było niewystarczającą informacją o możliwości skorzystania z procedur elektronicznych realizowanych przez Urząd. Umieszczenie bezpośrednich linków do stosownej usługi elektronicznej świadczonej za pomocą ePUAP na stronie Urzędu oraz na stronie BIP, ułatwiłoby obywatelom dostęp i mogłoby zwiększyć ich wykorzystanie. Opisy procedur przedstawione na stronach ePUAP, mimo że ogólnikowe dawały jednak możliwość ich wykorzystania.

1.9. Przekazanie wzorów dokumentów elektronicznych do centralnego repozytorium ePUAP

Opis stanu faktycznego

Do czasu niniejszej kontroli (czerwiec 2014 r.) Urząd nie przesyłał do MAiC wniosków o opublikowanie wzoru w Centralnym Repozytorium Wzorów i Dokumentów Elektronicznych (crd). Urząd nie przygotował innych procedur elektronicznych, korzystano ze wzorów usług dostarczanych przez ePUAP a tym samym obowiązek publikacji nie dotyczył gminy.

(dowód: akta kontroli str. 17 do 20)

1.10. Wspieranie modelu usługowego w zakresie świadczenia usług elektronicznych

Opis stanu faktycznego

Strona internetowa Urzędu działa pod adresem www.chrzanów.pl a strona internetowa BIP Urzędu pod adresem http://bip.malopolska.pl/umchrzanow/Article/id,240590.html. Na stronie www Urzędu znajdują się linki do stron BIP oraz stron ePUAP. Urząd nie wykorzystywał innej strony internetowej do świadczenia usług elektronicznych, natomiast zamieścił na swoich stronach linki m.in. do ePUAP oraz CEIDG.

Ustalono, że Urząd w procesie zarządzania usługami elektronicznymi nie wspierał modelu usługowego.

(dowód: akta kontroli str. 3 do 12, 44 do 51)

W odpowiedzi na pytanie dlaczego działania Urzędu nie wspierały modelu usługowego w zakresie świadczenia usług elektronicznych Burmistrz wyjaśnił, że cyt.: „*Usługa elektroniczna skrzynki podawczej została uruchomiona i działa w postaci modelu usług, którą Urząd uruchomił w ramach ePUAP".*

(dowód: akta kontroli str. 100, 103)

Zgodnie z definicją zawartą w § 2 pkt 8 rozporządzenia KRI, model usługowy to model architektury systemu informatycznego, w którym dla użytkowników zdefiniowano stanowiące odrębną całość funkcje systemu teleinformatycznego oraz opisano sposób korzystania z tych funkcji. Stwierdzono, że w stosunku do wszystkich trzech usług dostępnych elektronicznie w każdym przypadku jako właściciela usługi wskazano Urząd natomiast nie istniały karty opisu usługi. W stosunku do żadnej z usług nie wskazano sposobu zgłaszania awarii, technicznego właściciela usługi (ePUAP), nie wskazano dopuszczalnych okresów niedostępności usługi elektronicznej.

1.11. Zakres i sposób współpracy systemów IT

Opis stanu faktycznego

W czasie oględzin sposobu działania pięciu wybranych systemów IT stwierdzono, że Urząd posiada opisy tych systemów, które zostały zamieszczone w Polityce Bezpieczeństwa załączniku nr 5 pn. „Opis struktury zbiorów danych wskazujący zawartość poszczególnych pól informacyjnych i powiązania miedzy nimi". Załącznik w niezmienionej, niezaktualizowanej formie został umieszczony w nowej Polityce Bezpieczeństwa Informacji z 8 lipca 2014 r. i nadal nie zawiera opisu sposobu działania systemów a w szczególności opisu: w jaki sposób i z jakich rejestrów prowadzonych przez Urząd dany system korzysta, z jakich baz danych korzysta i jaki jest poziom współpracy pomiędzy nimi. Opis zawiera

natomiast dane takie jak np.: spis ulic, spis dowodów osobistych, spis stanów cywilnych, spis geografii wyborczej.

W czasie oględzin sposobu działania systemów stwierdzono, że system:

1. Ewidencja ludności (EI) i Rejestr Wyborców (RW): posiada dwa oddzielne moduły (Moduły: Ewidencja ludności oraz Rejestr Wyborców) ze wspólną bazą danych zawierającą m.in. nr pesel, imiona, nazwiska, adres aktualny stały lub czasowy, imię ojca, rodzaj i numer dokumentu tożsamości wraz z dokonanymi zmianami, daty zmian itd.
(EI) współpracuje z system PESEL na poziomie komunikacji jednostronnej (wymieniane dane obejmują m.in.: imię i nazwisko, datę urodzenia, imiona rodziców, nazwisko rodowe, zmiany w danych meldunkowych w tym z Centralnym Bankiem Danych prowadzonym przez MSW[8] i Terenowym Bankiem Danych prowadzonym przez Małopolski Urząd Wojewódzki);
Moduł Rejestr Wyborców nie współpracuje z żadnym innym systemem.
2. System PB_USC: współpracuje na poziomie informacyjnym z systemem Ewidencja Ludności i Rejestr Wyborców. W systemie PB_USC podczas rejestracji aktu urodzenia/małżeństwa/zgonu, po wprowadzeniu nr pesel osoby można pobrać dane z systemu Ewidencji Ludności dotyczące osoby w zakresie danych gromadzonych w USC (wymieniane dane obejmują m.in imiona, nazwisko, nazwisko rodowe, datę i miejsce urodzenia, stan cywilny, adres zameldowania, nr dokumentu tożsamości).
3. System KGM (do obsługi gospodarki mieniem gminnym) współpracuje z system Finansowo – Księgowym na poziomie komunikacji jednostronnym. W systemie KGM istnieje możliwość wykonania eksportu danych dotyczących faktur, korekt za dzierżawę oraz użytkowanie wieczyste do pliku w formacie xml. (wymieniane dane obejmują m.in. numery faktur oraz korekt, kwoty, daty, imię nazwisko, adres zamieszkania).
4. System KADRY/PŁACE współpracuje z systemami:

- PIT, e-deklaracje – komunikacja jednostronna
- Płatnik – komunikacja jednostronna
- System Bankowości Elektronicznej – komunikacja jednostronna.

Na podstawie wypłat naliczonych w systemie Kadry/Płace można wygenerować PIT-11 oraz PIT-R w formacie XML, który za pomocą aplikacji PIT lub e-deklaracje można wysłać w postaci elektronicznej (wymieniane dane obejmują m.in. imię i nazwisko, PESEL, NIP, adres zamieszkania, kwoty osiągniętego przychodu). W celu przekazania danych rozliczeniowych do systemu Płatnik generowany jest plik z danymi osoby ubezpieczonej.(wymieniane dane obejmowały m.in. imię i nazwisko, PESEL, kod tytułu ubezpieczenia). System umożliwia stworzenie listy przelewów w postaci pliku w odpowiednim formacie dla danego systemu bankowości elektronicznej, który można zaimportować w systemie bankowości elektronicznej.
5. System INTRADOK współpracuje z platformą EPUAP na poziomie jednostronnej komunikacji. Pobierane z ePUAP dokumenty wraz załącznikami są importowane do systemu INTRADOK (wymieniane dokumenty obejmują dane m.in. imię i nazwisko, adres zamieszkania).

(dowód: akta kontroli str. 104 do 105)

1.12. Procedury i praktyki postępowania stosowane we współpracy z innymi jednostkami administracji publicznej

Opis stanu faktycznego

Burmistrz wyjaśnił, że Urząd prowadzi komunikację elektroniczną z innymi jednostkami administracji publicznej za pomocą elektronicznej platformy usług administracji publicznej (ePUAP), poczty elektronicznej, aplikacji, modułów komunikacji elektronicznej i portali (m.in. CEIDG, dzienników elektronicznych (Redakcja Dziennika Urzędowego MUW).
Urząd nie zwracał się do innych jednostek z propozycją prowadzania wzajemnej komunikacji w formie elektronicznej ale w tej sprawie otrzymał pisma od czterech podmiotów, tj. od:

- GUS w zakresie przesyłania sprawozdań dotyczących m.in. informacji o wielkości zatrudnienia, gruntach komunalnych, liczbie urodzeń, masowych imprezach itp.;

[8] Ministerstwo Spraw Wewnętrznych

- MUW w zakresie przekazywania aktów prawnych do ogłoszenia w wojewódzkim dzienniku urzędowym oraz innej korespondencji za pośrednictwem ePUAP;
- Ministerstwa Gospodarki w zakresie umieszczania danych w systemie CEIDG;
- Urzędu Skarbowego w Chrzanowie w zakresie formularzy PIT-11.

(dowód: akta kontroli str. 100 do 103)

Wyjaśniając jaki zakres danych jest wymieniany pomiędzy systemami Urzędu a innymi systemami w administracji publicznej Burmistrz podał, że systemy Urzędu wymieniają z innymi systemami w administracji publicznej dane, takie jak:

- liczba zatrudnionych pracowników z uwzględnieniem stopnia niepełnosprawności (PFRON);
- imię, nazwisko, PESEL, adres, przychód, składka na ubezpieczenie zdrowotne i społeczne (Ministerstwo Finansów – PIT);
- imię, nazwisko, PESEL, adres, przychód, kod tytułu ubezpieczenia, wymiar czasu pracy (ZUS – PŁATNIK);
- imię, nazwisko, PESEL, adres, data urodzenia, adresy zameldowań itp. (Terenowa Baza Danych i Centralna Baza Danych).

(dowód: akta kontroli str. 100 do 103)

Ocena cząstkowa

Najwyższa Izba Kontroli ocenia pozytywnie działalność Urzędu w zakresie dostosowania posiadanych systemów teleinformatycznych do współpracy z innymi informatycznymi. Wymiana informacji z Małopolskim Urzędem Wojewódzkim i kilkoma innymi urzędami odbywała się w formie elektronicznej. System wewnętrznego obiegu dokumentów (INTRADOK) został zintegrowany z platformą ePUAP. Opisy procedur przedstawione na stronach ePUAP, mimo że nie były powielone na stronach Urzędu i BIP pozwalały jednak na skorzystanie z systemów.

W ocenie NIK zwiększenie udziału komunikacji elektronicznej w świadczeniach publicznych realizowanych przez Urząd i większe zorientowanie na rozwój i na poszerzenie usług elektronicznych pozwoliłoby na usprawnienie pracy Urzędu. Dotychczasowy sposób informowania przez Urząd o możliwości skorzystania z procedur elektronicznych ograniczający się do umieszczenia linku do platformy ePUAP na stronie internetowej Urzędu nie zachęcał obywateli do korzystania z usług elektronicznych.

2. Zarządzanie bezpieczeństwem systemów informatycznych

2.1. Aktualizacja regulacji dotyczących zmieniającego się otoczenia

Opis stanu faktycznego

W Urzędzie obowiązywała Polityka bezpieczeństwa danych osobowych oraz Instrukcja zarządzania systemem informatycznym służącym do przetwarzania danych osobowych wprowadzona zarządzeniem Burmistrza w kwietniu 2012 r. Polityka bezpieczeństwa została zaktualizowana 8 lipca 2014 r. i uwzględniała wymogi określone w rozporządzeniu KRI, poza § 20 ust. 2 pkt 6, który wymagał zapewnienia szkolenia osób zaangażowanych w proces przetwarzania informacji i opisu działania systemów (załączniki nr 5).

(dowód: akta kontroli str. 36 do 41, 126, 138)

2.2. Sprzęt informatyczny

Opis stanu faktycznego

Na próbie 10 skontrolowanych komputerów stwierdzono, że dane sprzętu komputerowego ujmowano w układzie tradycyjnej książki inwentarzowej (dla potrzeb rachunkowości) oraz (od lipca 2014 r.) w systemie elektronicznym, który zawierał dane szczegółowe o konfiguracji technicznej urządzeń i o zainstalowanym oprogramowaniu do czego zobowiązywał § 20 ust. 2 pkt 2 rozporządzenia KRI.

(dowód: akta kontroli str. 65 do 77)

2.3. Analizy utraty integralności, poufności lub dostępności informacji

Opis stanu faktycznego

W okresie od 31 maja 2012 r. w Urzędzie przeprowadzano okresowe analizy ryzyka opisane w przeprowadzonym audycie jako analizy utraty integralności, poufności lub dostępności informacji zgodnie z wymogami określonymi w § 20 ust. 2 pkt 3 rozporządzenia KRI. W badanym okresie nie wystąpił przypadek zgłoszenia incydentów naruszenia bezpieczeństwa informacji.

(dowód: akta kontroli str. 25 do 35, 42 do 43)

2.4. Zarządzanie uprawnieniami użytkowników

Opis stanu faktycznego

W czasie kontroli, na podstawie oględzin 10 komputerów stwierdzono, że w żadnym z nich nie była możliwa instalacja dowolnego oprogramowania przez użytkownika tego komputera niebędącego pracownikiem służb informatycznych Urzędu.

Urząd wypełniał zatem postanowienie określone w § 20 ust. 2 pkt 7 c rozporządzenia KRI, który nakłada na kierownictwo podmiotu publicznego obowiązek zapewnienia środków uniemożliwiających nieautoryzowany dostęp na poziomie systemów operacyjnych, usług sieciowych i aplikacji oraz egzekwowanie realizacji powszechnie przyjętej praktyki określonej w Załączniku A normy PN-ISO/IEC 27001:2007, punkt A.11.2.2, który stanowi, że należy ograniczyć i kontrolować przyznawanie i korzystanie z przywilejów w systemach informatycznych.

(dowód: akta kontroli str. 65 do 77, 98 do 99)

W badanym okresie dziesięć osób, które miały dostęp do systemów poddanych kontroli zakończyło zatrudnienie w Urzędzie. Ich konta zostały zablokowane. W żadnym przypadku nie zostały sporządzone formalne wnioski o zamknięcie kont/odebranie im uprawnień. Analizując uprawnienia 15 osób aktualnie pracujących z kontrolowanymi systemami stwierdzono, że posiadają one uprawnienia użytkowników tych systemów, jednak ich zakresy czynności wskazane w upoważnieniach i zakresach czynności nie odpowiadały definicjom wpisanych w systemach, co uniemożliwiało weryfikację zasadności nadanych uprawnień.

(dowód: akta kontroli str. 52 do 53, 80 do 83, 106 do 123)

W odpowiedzi na pytanie: kto i na jakiej podstawie wskazywał zbiory, do których ASI[9] nadawali uprawnienia poszczególnym pracownikom skoro zakresy czynności wskazane w oświadczeniach o dostępie do baz danych osobowych nie odpowiadały definicjom wskazanym jako nazwy baz danych w systemach komputerowych Burmistrz wyjaśnił, że w myśli dobrej praktyki kierownicy komórek organizacyjnych wskazywali ustnie zbiory i zakresy uprawnień do nadania w systemach informatycznych zgodnie z zakresami czynności.

(dowód: akta kontroli str. 88 do 92, 127, 129)

W Urzędzie nie zachowano wymaganej, w myśl postanowień Polityki Bezpieczeństwa Informacji, pisemnej formy nadawania, odbierania i zmiany uprawnień dostępu do systemów. Badanie wybranych pięciu systemów informatycznych wykazało, że również systemy komputerowe nie odnotowywały dokonywanych zmian a w prowadzonym rejestrze uprawnień odnotowano jedynie datę nadania pierwszych uprawnień dostępu do danych osobowych.

(dowód: akta kontroli str. 80 do 83, 106 do 117, 138, 142 do 143)

Burmistrz wyjaśnił, że w myśl tzw. „dobrej praktyki" stosowanej w Urzędzie uprawnienia nadawane i odbierane były na podstawie ustnego wniosku kierownika komórki organizacyjnej.

(dowód: akta kontroli str. 138, 140)

Ustalone nieprawidłowości

W działalności kontrolowanej jednostki w przedstawionym wyżej zakresie stwierdzono nieprawidłowość polegającą na: niepełnym przestrzeganiu procedury nadawania

[9] Administrator systemu Informatycznego

i odbierania uprawnień użytkownikom systemów informatycznych wykorzystywanych w Urzędzie co było niezgodne z § 20 ust. 2 pkt 4 rozporządzenia KRI, który nakłada na kierownictwo podmiotu publicznego obowiązek zapewnienia warunków umożliwiających realizację i egzekwowanie 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.

W Urzędzie nie składano pisemnych wniosków w sprawie nadawania i odbierania uprawnień co było niezgodne z zapisami przyjętej w Urzędzie Polityki Bezpieczeństwa Informacji, która wymagała zachowania formy pisemnej nadawania stosownych uprawnień przez kierowników komórek organizacyjnych. Tym samym nie w pełni zapewniono, że osoby zaangażowane w proces przetwarzania informacji posiadają stosowne uprawnienia i uczestniczą w tym procesie w stopniu adekwatnym do realizowanych przez nie zadań.

Uwagi dotyczące badanej działalności

Niepełna korelacja nazw zakresów czynności wskazanych w upoważnieniach i w zakresach czynności z definicjami zbiorów wpisanych w systemy komputerowe, nie pozwalała na weryfikację zasadności zakresu nadanych uprawnień.

2.5. Szkolenia pracowników przetwarzających informacje

Opis stanu faktycznego

W Urzędzie nie zaplanowano i nie realizowano szkoleń z zakresu bezpieczeństwa informacji i nieprzeszkolono osób zaangażowanych w proces przetwarzania informacji.

(dowód: akta kontroli str. 42, 43, 84 do 87, 126, 137)

Według stanu na 31 maja 2012 r. w Urzędzie było zatrudnionych 142 pracowników, a na 31 lipca 2014 r. 140. W badanym okresie nie zaplanowano i nie zrealizowano szkoleń dotyczących bezpieczeństwa informacji.

(dowód: akta kontroli str. 42, 43, 84 do 87, 126, 137)

Liczba osób posiadających uprawnienia do pracy z kontrolowanymi pięcioma systemami Urzędu wynosiła: KGM – 20 osób, INTRDOK – 140 osób, PB_USC – 6 osób, Ewidencja ludności wraz z rejestrem wyborców – 14 osób i Kadry i Płace – 6 osób.

(dowód: akta kontroli str. 52, 53, 128)

Burmistrz wyjaśnił, że szkolenie zostało zaplanowane i do końca 2014 r. wszyscy pracownicy realizujący zadania w zakresie przetwarzania informacji zostaną przeszkoleni ze szczególnym uwzględnieniem zagadnień bezpieczeństwa informacji.

(dowód: akta kontroli str. 138, 140)

Ustalone nieprawidłowości

W działalności kontrolowanej jednostki w przedstawionym wyżej zakresie stwierdzono nieprawidłowość polegającą na niezapewnieniu szkolenia osób zaangażowanych w proces przetwarzania informacji, co było niezgodne z § 20 ust. 2 pkt 6 rozporządzenia KRI.

Zdaniem NIK nieprzeszkolenie osób zaangażowanych w Urzędzie w proces przetwarzania informacji w zakresie kontrolowanych pięciu systemów mogło mieć wpływ na niewielki zakres wykorzystywania usług elektronicznych.

2.6. Procedury bezpiecznej pracy przy przetwarzaniu mobilnym i pracy na odległość

Opis stanu faktycznego

Zgodnie z zaleceniami audytu wewnętrznego Burmistrz określił zasady korzystania i zabezpieczania urządzeń mobilnych zarządzeniem nr 349/2014 z dnia 23 czerwca 2014 r. Kontrola wykazała, że na dzień 4 września 2014 r. Urząd posiadał dziewięć urządzeń przenośnych tzw. „laptopów" z których jeden był używany w systemie Ewidencja Ludności i posiadał program szyfrujący dysk pozostałe osiem zostało wyposażone w standardowe oprogramowanie użytkowe (typu Windows z pakietem MS Office i przeglądarkami internetowymi). Użytkownicy aż siedmiu z dziewięciu laptopów posiadali uprawnienia administratora.

(dowód: akta kontroli str. 30, 31, 33, 34, 128 do 130, 134 do 136)

ABI[10] Kierownik Referatu Informatyki wyjaśnił, że pozostawił uprawnienia administratora przez przeoczenie i niezwłocznie zostaną zamienione na uprawnienia użytkownika. W odpowiedzi na pytanie dlaczego do czasu przeprowadzenia audytu nie rozpoczęto aktualizacji Polityki Bezpieczeństwa Informacji podał, że wynikało to m.in. z braku czasu i obciążenia pracowników Referatu Informatyki.

(dowód: akta kontroli str. 143)

Ustalone nieprawidłowości

W działalności kontrolowanej jednostki stwierdzono nieprawidłowości polegające na nieustaleniu do czerwca 2014 r. zasad (procedur) gwarantujących bezpieczną pracę przy przetwarzaniu mobilnym i pracy na odległość co było niezgodne z § 20 ust. 2 pkt 8 rozporządzenia KRI oraz nieprzestrzeganie zasady nadawania i odbierania uprawnień użytkownikom systemów informatycznych w zakresie niezbędnym do wykonywanych zadań co było niezgodne z § 20 ust. 2 pkt 4 rozporządzenia KRI.

2.7. Umowy serwisowe

Opis stanu faktycznego

W umowach dotyczących serwisu i nadzoru autorskiego nad funkcjonowaniem i eksploatacją oprogramowania zawarto stosowne zapisy o zobowiązaniu się przez wykonawcę do ochrony danych poufnych, tj. zapisy o zabezpieczeniu danych oraz konieczności przestrzegania procedur wynikających z ustawy o ochronie danych osobowych z dnia 29 sierpnia 1997 r.[11] W okresie objętym kontrolą nie zawierano umów dotyczących serwisowania komputerów a komputery zakupione w tym okresie posiadały rozszerzoną gwarancję producenta zapewniającą usunięcie usterki w miejscu instalacji (Urząd). Sekretarz Urzędu wyjaśniła, że zgodnie z umową naprawy komputerów i nadzór autorski realizowane były na terenie Urzędu, nośników danych nie przekazywano poza Urząd.

(dowód: akta kontroli str. 21 do 24, 124 do 125, 144 do 146)

2.8. Zgłaszanie incydentów naruszenia bezpieczeństwa informacji

Opis stanu faktycznego

Procedury postępowania w sytuacjach zgłoszenia naruszenia bezpieczeństwa informacji określono w zarówno w Polityce bezpieczeństwa zarówno z 2012 r. jak i jej aktualizacji z lipca 2014 r. Zapoznanie się z zasadami określonymi w ww. dokumentach potwierdzili podpisami pracownicy Urzędu. W badanym okresie nie wystąpił przypadek zgłoszenia incydentów naruszenia bezpieczeństwa informacji.

(dowód: akta kontroli str. 17, 20, 130 do 133)

2.9. Audyt wewnętrzny z zakresu bezpieczeństwa informacji

Opis stanu faktycznego

W latach 2012 – 2014 Urząd zaplanował dwukrotnie okresowy audyt wewnętrzny z zakresu bezpieczeństwa informacji, o którym mowa w § 20 ust. 2 pkt 14 rozporządzenia KRI. Na rok 2012 nie zaplanowano (nie dokonywano zmian w planie audytów) i nie realizowano takiego audytu.

Pierwszy audyt został zrealizowany w okresie od 3 grudnia 2013 r. do 31 stycznia 2014 r. a drugi rozpoczął się 17 czerwca 2014 r. i do czasu niniejszej kontroli NIK nie został zakończony. Zalecenia sformułowane w wyniku pierwszego audytu zostały zrealizowane poprzez wprowadzenie zarządzenia nr 394/2014 Burmistrza Miasta Chrzanowa z dnia 23 czerwca 2014 r. w sprawie Polityki bezpieczeństwa dla urządzeń przenośnych służących do przetwarzania danych osobowych w Urzędzie Miejski w Chrzanowie oraz zarządzenia nr 411/2014 Burmistrza Miasta Chrzanowa z dnia 8 lipca 2014 r. w sprawie wprowadzenia Polityki Bezpieczeństwa Informacji. Ponadto w dniu 21 lipca zamontowano zamek cyfrowy do drzwi serwerowni Urzędu.

(dowód: akta kontroli str. 36 do 41, 78 do 79, 128 do 136)

[10] Administrator Bezpieczeństwa Informacji
[11] (Dz.U. z 2002 r., Nr 101, poz. 926 ze zm.)

2.10. Tworzenie i testowanie kopii zapasowych danych i oprogramowania aplikacyjnego

Opis stanu faktycznego

W Polityce określono obowiązek tworzenia i przechowywania kopii zapasowych (codziennie). Sporządzane, zgodnie z przyjętą procedurą, kopie zabezpieczano na nośnikach w serwerowni oraz w sejfie w pomieszczeniu innym niż serwerownia. Urząd nie dysponował programem do testowania utworzonych kopii ale były one wykonywane codziennie, rejestrowane a sporządzone kopie ASI oceniał m.in. po rozmiarze plików. Pomieszczenia, w których przechowywano kopie zostały zabezpieczone w podstawowym zakresie (zamek cyfrowy, alarm).

(dowód: akta kontroli str. 61 do 64)

ABI Kierownik Referatu Informatyki wyjaśnił, że ocena przydatności kopii polegała na sprawdzeniu czy rozmiar kopii plików odpowiada wielkości pliku wyjściowego. Ponadto podał, ze minimalizowanie ryzyka utraty informacji w wyniku awarii polegało na tworzeniu codziennych kopii zapasowych, posiadaniu urządzeń podtrzymujących zasilanie serwerów, urządzeń sieciowych oraz części stanowisk roboczych co pozwalało na poprawne zamknięcie systemów bez utraty integralności danych a kopie posiadanych systemów pozwalały na przywrócenie środowiska informatycznego.

(dowód: akta kontroli str. 142 do 143)

2.11. Format udostępniania zasobów informacyjnych badanych systemów informatycznych

Opis stanu faktycznego

Na przykładzie pięciu wybranych do badania systemów, sprawdzono, że systemy informatyczne udostępniały zasoby informacyjne m.in. w formacie pdf, rtf, tekst lub XML (po wygenerowaniu pliki można było zapisać w ww. formatach). Tym samym spełniony został warunek określony w załączniku nr 2 do rozporządzenia KRI o możliwości zapisywania danych w co najmniej w jednym z formatów wymienionych w KRI.

(dowód: akta kontroli str. 93 do 97)

Ocena cząstkowa

Najwyższa Izba Kontroli ocenia pozytywnie działalność Urzędu w zakresie wdrażania systemu zarządzania bezpieczeństwem systemów informatycznych mimo stwierdzonych nieprawidłowości dotyczących nieustalenia zasad pracy urządzeń przenośnych i pozostawienia na siedmiu z nich (na 9 posiadanych) uprawnień administratora oraz braku przeszkolenia pracowników w zakresie bezpieczeństwa informacji.
Stosownie do wymogów rozporządzenia KRI Urząd zamieścił w umowach dotyczących serwisu bądź oprogramowania sprzętu informatycznego zapisy gwarantujące odpowiedni poziom bezpieczeństwa informacji; zrealizowano wewnętrzny audyt w zakresie bezpieczeństwa informacji, i jego zalecenia a w lipcu 2014 r: opracowano zaktualizowaną Politykę Bezpieczeństwa Informacji (za wyjątkiem załącznika 5) i wprowadzono inwentaryzację sprzętu komputerowego i posiadanego oprogramowania w sposób wymagany przez KRI. Nieprawidłowości dotyczące urządzeń przenośnych zostały również usunięte w czerwcu 2014 r.

3. Dostosowanie sposobu prezentacji informacji przez systemy do potrzeb osób niepełnosprawnych

Opis stanu faktycznego

Strona internetowa Urzędu działa pod adresem www.chrzanow.pl, została dostosowana do potrzeb osób niedowidzących poprzez umieszczenie z lewej strony, pod nazwą miasta, znaczników pozwalających na otwarcie strony w wysokim kontraście lub pisanej większą czcionką (jeden rozmiar). Weryfikacja zgodności strony Urzędu ze standardem WCAG 2.0 w zakresie Zasady 4. - Kompatybilność dokonana poprzez wykorzystanie narzędzi dostępnych na stronie internetowej http://jigsaw.w3.org/css-validator/ wykazała dwie niezgodności ze standardem WCAG 2.0. Sprawdzenie tej samej strony Urzędu za pomocą strony internetowej http://validator.w3.org/ dało wynik 182 błędów i 18 ostrzeżeń. W czasie oględzin Strona Urzędu nie pozwalała na odsłuchanie zapisu informacji (tzw. „czytacza"), natomiast zawierała informacje o sposobie udostępniania obsługi dla osób doświadczających trwale lub czasowo trudności w komunikowaniu się.

Na stronie głównej Urzędu (na górze strony, po lewej stronie) umieszczono link do strony BIP Urzędu. Strona internetowa BIP Urzędu działa pod adresem: http://bip.malopolska.pl/umchrzanow/Article/id,240590.html i została przygotowana do potrzeb osób niedowidzących poprzez umieszczenie w prawym górnym rogu znacznika pozwalającego na otwarcie strony w wysokim kontraście lub pisanej większą czcionką (dwa rozmiary). Weryfikacja zgodności strony Urzędu ze standardem WCAG 2.0 w zakresie Zasady 4. - Kompatybilność dokonana poprzez wykorzystanie narzędzi dostępnych na stronie internetowej http://jigsaw.w3.org/css-validator/ wykazała 1152 niezgodności ze standardem WCAG 2.0. Sprawdzenie tej samej strony BIP Urzędu za pomocą strony internetowej http://validator.w3.org/ dała wynik 10 niezgodności (8 błędów, 2 ostrzeżenia).

(dowód: akta kontroli str. 3 do 12)

Ocena cząstkowa

Najwyższa Izba Kontroli nie formułuje oceny cząstkowej w tym obszarze.

IV. Wnioski

Wnioski pokontrolne

Przedstawiając powyższe oceny i uwagi wynikające z ustaleń kontroli, Najwyższa Izba Kontroli, na podstawie art. 53 ust. 1 pkt 5 ustawy z dnia 23 grudnia 1994 r. o Najwyższej Izbie Kontroli[12], wnosi o:

1) przeszkolenie wszystkich osób zaangażowanych w proces przetwarzania informacji w zakresie, o którym mowa w § 20 ust. 2 pkt 6 rozporządzenia w sprawie KRI;
2) usunięcie uprawnień administratora z urządzeń przenośnych;
3) dostosowanie nazw użytych w zakresach czynności do nazewnictwa baz danych/rejestrów w systemach informatycznych i zachowywanie formy nadawania stosownych uprawnień wskazanej w Polityce Bezpieczeństwa Informacji.

V. Pozostałe informacje i pouczenia

Prawo zgłoszenia zastrzeżeń

Wystąpienie pokontrolne zostało sporządzone w dwóch egzemplarzach; jeden dla kierownika jednostki kontrolowanej, drugi do akt kontroli.

Zgodnie z art. 54 ustawy o NIK kierownikowi jednostki kontrolowanej przysługuje prawo zgłoszenia na piśmie umotywowanych zastrzeżeń do wystąpienia pokontrolnego, w terminie 21 dni od dnia jego przekazania. Zastrzeżenia zgłasza się do dyrektora Delegatury NIK w Krakowie.

Obowiązek poinformowania NIK o sposobie wykorzystania uwag i wykonania wniosków

Zgodnie z art. 62 ustawy o NIK proszę o poinformowanie Najwyższej Izby Kontroli, w terminie 21 dni od otrzymania wystąpienia pokontrolnego, o sposobie wykorzystania uwag i wykonania wniosków pokontrolnych oraz o podjętych działaniach lub przyczynach niepodjęcia tych działań.

W przypadku wniesienia zastrzeżeń do wystąpienia pokontrolnego, termin przedstawienia informacji liczy się od dnia otrzymania uchwały o oddaleniu zastrzeżeń w całości lub zmienionego wystąpienia pokontrolnego.

Kraków, dnia 16 września 2014 r.

Kontroler
Małgorzata Kram
Specjalista k.p.

.....
podpis

Podpisał
Marcin Kopeć
Wicedyrektor

[12] Dz. U. z 2012 r., poz.82, ze zm.