



NAJWYŻSZA IZBA KONTROLI

Delegatura w Krakowie

LKR – 4101-017-02/2014

P/14/004

# WYSTĄPIENIE POKONTROLNE

## 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 88139 z 12 czerwca 2014 r. (dowód: akta kontroli str. 1 do 2)
Jednostka kontrolowana	Urząd Miasta i Gminy Olkusz, 32 – 300 Olkusz, Rynek 1 (Urząd)
Kierownik jednostki kontrolowanej	Dariusz Rzepka, Burmistrz Miasta i Gminy Olkusz (Burmistrz)

Ocena ogólna<sup>1</sup>

## II. Ocena kontrolowanej działalności

W Urzędzie podjęto działania w celu zapewnienia interoperacyjności systemów informatycznych, o czym świadczy spełnianie przez skontrolowane cztery systemy<sup>2</sup> 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<sup>3</sup>. Zapewniono również właściwy dostęp do informacji dla osób niepełnosprawnych poprzez odpowiednie przygotowanie strony internetowej Urzędu. Prawidłowo rozwijano elektroniczną interakcję wewnątrz Urzędu (systemy eSOD<sup>4</sup> oraz ISO), a także w komunikacji z innymi urzędami. O przygotowywaniu się Urzędu do świadczenia usług elektronicznych w szerszym zakresie świadczą m.in. trwające prace nad deklaracją o wysokości opłaty za gospodarowanie odpadami komunalnymi oraz odbieranie od grudnia 2011 r. korespondencji z Małopolskiego Urzędu Wojewódzkiego (MUW) wyłącznie w formie elektronicznej. 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). Urząd w podstawowym stopniu wspierał model usługowy w zakresie świadczenia usług elektronicznych.

W każdej z czterech usług dostępnych elektronicznie w Urzędzie można było zidentyfikować właściciela tych usług, ale tylko w dwóch przypadkach istniały karty opisu usługi. Kart tych nie aktualizowano od 31 maja 2012 r. (mimo zmian w przepisach dotyczących interoperacyjności oraz w Regulaminie Organizacyjnym Urzędu). W stosunku do ww. usług

<sup>1</sup> 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.

<sup>2</sup> ZSI Urząd – tzw. „dziedziny” - Gospodarka Odpadami Komunalnymi, Zarządzanie Mieniem, Masowe Płatności, Ewidencja Nieruchomości.

<sup>3</sup> 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).

<sup>4</sup> Elektroniczny system obiegu dokumentów.

w żadnym dokumencie nie wskazano maksymalnego czasu niedostępności usługi, sposobu zgłaszania awarii czy technicznego właściciela usługi (ePUAP<sup>5</sup>).

Sprawowanie nadzoru nad stworzeniem i wdrożeniem systemów zarządzania bezpieczeństwem systemów IT, w tym zapewnienie bezpieczeństwa danych przetwarzanych w Urzędzie NIK ocenia negatywnie. Kontrola wykazała m.in. niedostosowanie dokumentów tworzących Politykę Bezpieczeństwa Informacji w Urzędzie do wymogów KRI, tj.:

- brak aktualizacji i doskonalenia systemu zarządzania bezpieczeństwem informacji, co nie zapewniło zarządzania bezpieczeństwem informacji w zakresie dotyczącym zmieniającego się otoczenia;
- niekompletną i nieaktualizowaną inwentaryzację sprzętu komputerowego;
- niepełną realizację nadawania stosownych uprawnień użytkownikom systemów informatycznych wykorzystywanych w Urzędzie oraz pozostawienie możliwości instalacji nieautoryzowanego oprogramowania na sześciu z dziesięciu poddanych oględzinom komputerów;
- zaniechanie dokumentowania przez Administratora Bezpieczeństwa Informacji (ABI) odbierania uprawnień użytkownikom, mimo ustalonych procedur;
- brak w umowach zawieranych w latach 2012–2013 zapisów gwarantujących zabezpieczenie poufności informacji znajdujących się na nośnikach danych, co stwarzało zagrożenie ich utraty lub udostępnienia nieuprawnionym podmiotom;
- nierealizowanie wewnętrznego audytu w zakresie bezpieczeństwa informacji, nie rzadziej niż raz na rok;
- brak przeszkolenia w zakresie bezpieczeństwa informacji wszystkich pracowników zaangażowanych w proces przetwarzania informacji.

W ocenie NIK zarządzanie bezpieczeństwem informacji, o którym mowa w rozporządzeniu KRI oraz w PN<sup>6</sup> było nierzetelne a działania Burmistrza dotyczące wdrożenia systemu bezpieczeństwa systemów IT należy uznać za niewystarczające.

NIK zwraca uwagę, że chociaż Urząd był przygotowany do świadczenia usług elektronicznych<sup>7</sup>, to nie podjęto skutecznych działań zmierzających do popularyzacji komunikacji elektronicznej wśród obywateli. Nie zaplanowano działań zmierzających do rozwoju takiej komunikacji w kontaktach z obywatelami, nie wykonano badań zmierzających do poznania zapotrzebowania na takie usługi oraz nie podjęto działań promujących elektroniczny sposób komunikacji. Na stronach internetowych Urzędu i BIP nie zamieszczono linków (odsylaczy) do czterech 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.

<sup>5</sup> Elektroniczna Platforma Usług Administracji Publicznej.

<sup>6</sup> Polskiej Normie Technika informatyczna. Techniki bezpieczeństwa. Systemy zarządzania bezpieczeństwem informacji (PN-ISO/EIC 27001:2007).

<sup>7</sup> M.in. wprowadzenie systemu eSOD zintegrowanego z ePUAP oraz prowadzenie korespondencji w z innymi jednostkami administracji w sposób elektroniczny.

### III. Opis ustalonego stanu faktycznego

#### 1. Dostosowanie systemów teleinformatycznych do współpracy z systemami innych podmiotów administracji publicznej

##### 1.1. Elektroniczne świadczenie usług w dokumentach strategicznych gminy

Opis stanu faktycznego

Kierunki rozwoju Gminy na najbliższe lata ustalono w maju 2008 r. w Strategii Rozwoju Miasta i Gminy Olkusz na lata 2008 – 2015 (*Strategia*)<sup>8</sup>. Wśród 26 wiodących projektów strategicznych (tzw. lista syntetyczna) zagadnienia dotyczące dostosowania Urzędu do elektronicznego świadczenia usług publicznych określono tylko w jednym z kierunków rozwoju pn. „*Wdrożenie systemu elektronicznego obiegu dokumentów w Urzędzie Miasta i Gminy Olkusz*”. Kierunek ten realizowano w ramach głównego celu operacyjnego C5.1.3 pn. „*Wzmacnianie pozycji miasta i gminy w otoczeniu oraz budowanie wizerunku obszaru przyjaznego dla mieszkańców, inwestorów i odwiedzających*”. Zapis o wdrożeniu systemu elektronicznego obiegu dokumentów w Urzędzie jest jedynym zapisem odnoszącym się do dostosowania jednostki do elektronicznego świadczenia usług publicznych i w żadnej części obydwu Strategii nie został omówiony lub szerzej opisany. Nie określono zatem zakresu działań ani ram czasowych i wielkości wskaźnika (np. liczby udostępnionych usług przez internet) jakie zamierzano osiągnąć w kolejnych latach.

(dowód: akta kontroli str. 16, 43, 44)

##### 1.2. Promowanie komunikacji elektronicznej

Opis stanu faktycznego

Strategia ani inne dokumenty Gminy nie zawierały 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. 16, 20, 43, 44)

Burmistrz wyjaśnił, że Gmina Olkusz przewiduje rozwój świadczenia usług elektronicznych dla mieszkańców i przedsiębiorców mimo braku konkretnych zapisów odnoszących się do przygotowania jednostki do elektronicznego świadczenia usług publicznych. Wskazał, że świadczą o tym m.in. aplikacje do programów pomocowych zorientowane na rozwój i usprawnienie usług elektronicznych oraz poprawę infrastruktury niezbędnej do prawidłowego funkcjonowania obsługiwanych systemów. Ponadto podał, że w „*przypadku pojawienia się ostatecznego zakresu wsparcia ze strony środków UE oraz możliwości aplikowania w nowym okresie programowania, a przez co ubiegania się o dofinansowanie projektów usprawniających rozwój usług świadczonych drogą elektroniczną, Gmina uaktualni listę programów strategicznych, tak aby były realne do zrealizowania*”.

(dowód: akta kontroli str. 125, 127)

Urząd realizował usługi korzystając z aplikacji do programów pomocowych tzw. „dziedzinowych” służących pracownikom Urzędu. Usługi elektroniczne realizowane były wyłącznie za pośrednictwem platformy ePUAP a ich liczba nie przekraczała 0,2% (co zostało opisane w dalszej części wystąpienia pkt 1.6).

(dowód: akta kontroli str. 6 do 8)

<sup>8</sup> Strategia Rozwoju Miasta i Gminy Olkusz na lata 2008 – 2015, przyjęta uchwałą nr XXI/212/2008 Rady Miejskiej w Olkuszu z dnia 6 maja 2008 r. w sprawie przyjęcia Strategii Rozwoju Miasta i Gminy Olkusz na lata 2008 – 2015, zaktualizowana uchwałą nr XXI/274/2012 z 27 listopada 2012 r.

### 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 przeprowadzono ankiet lub innych form poznania potrzeb mieszkańców Gminy dotyczących potrzeb korzystania z elektronicznej formy komunikacji z Urzędem. Jedyną formą poznania opinii na temat jakości świadczonych w Urzędzie usług była ankieta – badanie satysfakcji klienta zewnętrznego – prowadzona w ramach funkcjonowania systemu zarządzania jakością wg normy ISO 9001:2008. Odnośnie do poznania potrzeb korzystania z elektronicznej formy komunikacji ankieta ograniczała się do jednego pytania: „Czy pozytywnie ocenia Pan/Pani przydatność informacji zawartych na stronie internetowej Urzędu oraz w Biuletynie Informacji Publicznej (BIP)”. W okresie od 31 maja 2012 r. do czerwca 2014 r. ankietę wypełniły 73 osoby, z których 35 odpowiedziało twierdząco, 8 udzieliło negatywnej oceny a 30 osób udzieliło odpowiedzi „nie korzystam” ze strony internetowej. Odnotowanie liczby osób korzystającej lub nie korzystających ze stron internetowych było jedynym działaniem Urzędu w sprawie analizy zainteresowania usługami elektronicznymi.

(dowód: akta kontroli str. 16, 43 do 62)

Uwagi dotyczące badanej działalności

W ocenie NIK poznanie potrzeb obywateli i poznanie 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 lub z prośbą o pomoc w zakresie dostosowania swoich systemów/rejestrów informatycznych do wymogów KRI.

(dowód: akta kontroli str. 9, 11, 16)

### 1.5. Procedury regulujące komunikację elektroniczną w Urzędzie

Opis stanu faktycznego

Podstawowym sposobem dokumentowania przebiegu załatwiania i rozstrzygnięcia spraw w Urzędzie był tradycyjny („papierowy”) system wykonywania czynności kancelaryjnych, co ustalono zarządzeniem nr 0050.1.2011 Burmistrza Miasta i Gminy Olkusz z dnia 1 lutego 2011 r. w sprawie podstawowego sposobu dokumentowania przebiegu załatwiania i rozstrzygnięcia spraw oraz stosowania Instrukcji Kancelaryjnej. W Regulaminie Urzędu<sup>9</sup> wskazano m.in., że: zasady obiegu korespondencji (w wersji papierowej oraz elektronicznej) i podpisywania pism zostaną określone w odrębnym zarządzeniu w sprawie obiegu pism. Zarządzenie takie wprowadzono 16 sierpnia 2010 r., a zmieniono 1 marca 2012 r.<sup>10</sup>

(dowód: akta kontroli str. 11, 18 do 22, 91 do 96, 195 do 197, 203 do 220)

Wewnętrzna procedura w sprawie obiegu korespondencji i podpisywania pism w Urzędzie wprowadzona ww. zarządzeniem w sprawie obiegu pism stanowiła m.in., że:

- korespondencję wpływającą do Urzędu przyjmuje Punkt Informacyjny – Podawczy, który prowadzi rejestr korespondencji w formie papierowej i elektronicznej, Rejestr kancelaryjny prowadzony jest również w systemie eSOD. Korespondencja dostarczona do Urzędu wyłącznie w formie elektronicznej przekazywana jest za pomocą systemu eSOD. Dokumenty w formie elektronicznej po wprowadzeniu elektronicznie dekretacji przez Sekretarza Urzędu przekazywane są do odpowiednich wydziałów;

<sup>9</sup> Regulamin Organizacyjny Urzędu Miasta i Gminy w Olkuszu wprowadzony zarządzeniem Nr 0050.2490.2014 Burmistrza Miasta i Gminy Olkusz z dnia 12 lutego 2014 r. (i poprzednie wprowadzane m.in. zarządzeniem Nr 0050.1981.2013 Burmistrza Miasta i Gminy Olkusz z dnia 17 czerwca 2013 r. i zarządzeniem Nr 0050.850.2012 Burmistrza Miasta i Gminy Olkusz z dnia 13 lutego 2012 r.).

<sup>10</sup> Zarządzenie Nr 0152/230/2010 Burmistrza z dnia 16 sierpnia 2010 r. w sprawie obiegu korespondencji i podpisywania pism w Urzędzie Miasta i Gminy w Olkuszu, zmienione zarządzeniem nr 0050.918b.2012 Burmistrza Miasta i Gminy Olkusz z dnia 1 marca 2012 r. w sprawie zmiany Zarządzenia nr 0152/230/2010 Burmistrza Miasta i Gminy Olkusz z dnia 16 sierpnia 2010 r. w sprawie zasad obiegu korespondencji i podpisywania pism w Urzędzie Miasta i Gminy w Olkuszu.

- obieg korespondencji w systemie elektronicznym wykorzystywany był do wewnętrznego obiegu korespondencji oraz załatwiania i ewidencjonowania spraw w Urzędzie. Z ww. systemu wyłączono sprawy realizowane za pomocą odrębnych programów elektronicznych np.: dodatki mieszkaniowe i przydział mieszkań komunalnych; lokalny transport zbiorowy; ewidencja działalności gospodarczej; ewidencja podatkowa; wydawanie aktów stanu cywilnego.

(dowód: akta kontroli str. 9, 11, 16, 27, 28)

Czynności kancelaryjne w eSOD wykonywano zgodnie z Instrukcją kancelaryjną, z zachowaniem przewidzianej dla niej formy i sposobu identyfikacji w następujący sposób:

- pisma składane przez klienta za pomocą platformy ePUAP były automatycznie przekierowywane do systemu obiegu dokumentów elektronicznych eSOD i rejestrowane w tym systemie (stosownie do zapisów Regulaminu Urzędu);
- pisma w formie elektronicznej, po zarejestrowaniu, były dekretowane elektronicznie przez Sekretarza Urzędu a następnie przekazywane elektronicznie do właściwych Wydziałów;
- dekretację do pracowników podległych kierownikowi/naczelnikowi prowadzono stosownie do zakresów czynności pracowników opisanych w „Karcie Opisu Stanowiska Pracy” każdego z nich. Sprawy załatwiane elektronicznie prowadzono według takiego samego schematu jak prowadzone w tradycyjnie. Po rozpatrzeniu sprawy przygotowany przez merytorycznego pracownika projekt odpowiedzi był przekazywany w formie elektronicznej (na ogół na nośniku typu pendrive, nie wykorzystywano funkcji przesyłania projektu) do Burmistrza, jego zastępców, Skarbnika lub Sekretarza. W stosunku do obiegu dokumentów „papierowych” pominięty został etap dokumentowania faktu weryfikacji projektu odpowiedzi przez Naczelnika/Kierownika Wydziału. Po podpisaniu elektronicznie przez Burmistrza (jego zastępców, Skarbnika lub Sekretarza) dokument wysyłano odbiorcy z użyciem eSOD za pośrednictwem ePUAP.

(dowód: akta kontroli str. 69, 155 do 157, 198 do 202, 221 do 222)

## 1.6. Liczba złożonych dokumentów / wniosków / podań

Opis stanu faktycznego

W okresie od 31 maja 2012 r. do 31 maja 2014 r. obywatele złożyli do Urzędu 66.006 dokumentów, w tym tylko 72 w formie elektronicznej (głównie wnioski o udostępnienie informacji publicznej - 48), pozostałe 65.934 dokumenty wpłynęły w postaci „papierowej”. W analogicznym okresie podmioty gospodarcze złożyły 7.015 dokumentów, w tym 91 w formie elektronicznej i 6.924 w formie tradycyjnej. Ponadto inne urzędy złożyły 1.509 dokumentów, w tym w formie elektronicznej 1.358 a 151 w formie tradycyjnej.

(dowód: akta kontroli str. 6 do 8)

## 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, wniosek o dopisanie do rejestru wyborców). W czasie niniejszej kontroli stwierdzono, że istniała możliwość realizacji czterech usług elektronicznych za pośrednictwem ePUAP, tj.:

1. wniosku o dopisanie do spisu wyborców,
2. pisma ogólnego do Urzędu,
3. skarg, wniosków, zapytań do Urzędu,
4. deklaracji o wysokości opłaty za gospodarowanie odpadami komunalnymi (formularz w trakcie trwających uzgodnień z MAiC).

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

(dowód: akta kontroli str. 18 do 22)

Usługi świadczone na platformie ePUAP zawierały dane dotyczące podmiotu (Urząd), miejsce świadczenia usługi – siedziba Urzędu, podstawę prawną oraz sposób realizacji usługi.

W odniesieniu do ww. czterech usług w dniu oględzin stwierdzono, że:

- deklaracja o wysokości opłaty za gospodarowanie odpadami komunalnymi w formacie pdf wraz z opisem procedury została zamieszczona na stronie www Urzędu (z adnotacją o możliwości złożenia jej w formie elektronicznej – jednak bez wskazania linku lub adresu www tej usługi), a na BIP zamieszczono sam tekst uchwały wraz z załącznikiem (wzór deklaracji) bez opisu procedury załatwienia sprawy;
- w sprawie wniosku o dopisanie do spisu wyborców strona www Urzędu przekierowywała klientów na stronę internetową BIP Urzędu, gdzie umieszczono formularz wniosku o wpisanie do rejestru wyborców (pdf) i opis procedury załatwienia sprawy, natomiast brak było informacji o możliwości złożenia wniosku o dopisanie do spisu wyborców w formie elektronicznej poprzez ePUAP;
- wzór pisma ogólnego do Urzędu został umieszczony tylko na ePUAP, nie zamieszczono takiego dokumentu na stronie www Urzędu i BIP;
- pismo w sprawie skarg i wniosków umieszczone zostało tylko na stronie internetowej BIP Urzędu wraz z opisem procedury, nie zamieszczono go na stronie www Urzędu.

Opisy procedur zamieszczone na ePUAP nie były tożsame z opisami procedur zamieszczonymi na stronie internetowej Urzędu i BIP.

W żadnym z ww. przypadków (czterech 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. 129 do 150)

## **1.8. Opisy procedur elektronicznego załatwiania spraw w BIP**

Opis stanu faktycznego

Urząd udostępniał cztery usługi elektroniczne (deklaracja o wysokości opłaty za gospodarowanie odpadami komunalnymi, wniosek o dopisanie do spisu wyborców, pismo ogólne do Urzędu, pismo w sprawie skarg i wniosków). Dla trzech usług nie zamieszczono karty opisu usługi, tj. na stronie Urzędu dla: wniosku o dopisanie do spisu wyborców, pisma ogólnego do Urzędu, pisma w sprawie skarg i wniosków, a na stronie BIP dla: deklaracji o wysokości opłaty za gospodarowanie odpadami komunalnymi, wniosku o dopisanie do spisu wyborców, pisma ogólnego do Urzędu. W każdym przypadku ustalono komórkę Urzędu odpowiedzialną za realizację usługi a jej pracownicy w kartach opisu stanowiska mieli określone zadania związane z realizacją tych usług. Na platformie ePUAP opisano szczegółowo usługę dopisania do spisu wyborców (ze wskazaniem komórki organizacyjnej Urzędu i pokoju, w którym można załatwić sprawę) w pozostałych trzech przypadkach jako miejsce obsługi wskazano dziennik podawczy Urzędu. Opisy świadczonych usług zamieszczone na stronach internetowych Urzędu i BIP opisano również w punkcie 1.7.

(dowód: akta kontroli str. 129 do 150)

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 do usług elektronicznych i mogłoby zwiększyć ich wykorzystanie. Opisy procedur przedstawione na stronach ePUAP, mimo że nie były całkowicie tożsame z opisami zamieszczonymi na stronach Urzędu i BIP pozwalały jednak na skorzystanie z nich.

## **1.9. Przekazanie wzorów dokumentów elektronicznych do centralnego repozytorium ePUAP**

Opis stanu faktycznego

Do czasu niniejszej kontroli (czerwiec 2014 r.) Urząd przesłał do MAiC dwa wnioski o opublikowanie wzoru w Centralnym Repozytorium Wzorów i Dokumentów Elektronicznych (crd) - oba dotyczyły deklaracji o wysokości opłat za odpady. W obu przypadkach Urząd

otrzymał informację o przyczynach nieopublikowania wzoru dokumentu elektronicznego w crd (zakwestionowano m.in. identyfikator podstawy prawnej, wykropkowania i odnośniki charakterystyczne tylko dla wzorów nieelektronicznych, np. niepotrzebne skreślić itp., jakie zawierał zwizualizowany dokument elektroniczny). Do czasu niniejszej kontroli te wzory nie zostały ostatecznie zaakceptowane przez MAiC i opublikowane w crd.

(dowód: akta kontroli str. 20, 129 do 150)

### **1.10. Wspieranie modelu usługowego w zakresie świadczenia usług elektronicznych**

Opis stanu faktycznego

Strona internetowa Urzędu działa pod adresem [www.umig.olkusz.pl](http://www.umig.olkusz.pl) a strona internetowa BIP Urzędu pod adresem [bip.malopolska.pl/umigolkusz/Article/id,240778.html](http://bip.malopolska.pl/umigolkusz/Article/id,240778.html). Na stronie [www](http://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 w podstawowym zakresie wspiera model usługowy. Zgodnie z definicją zawartą w § 2 pkt 8 rozporządzenia KRI, model usługowy jest modelem 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 czterech usług dostępnych elektronicznie w każdym przypadku można zidentyfikować właściciela usługi, w dwóch przypadkach istnieją karty opisu usługi ale nie były one aktualizowane po 31 maja 2012 r. W stosunku do żadnej z usług nie wskazano maksymalnego czasu niedostępności usługi, sposobu zgłaszania awarii, technicznego właściciela usługi (ePUAP), nie wskazano dopuszczalnych okresów niedostępności usługi elektronicznej.

(dowód: akta kontroli str. 199 do 200)

Burmistrz wyjaśnił, że Urząd wspiera model usługowy poprzez elektroniczne przekazywanie danych do Urzędu Skarbowego, GUS, ZUS, CEIDG. Ponadto poinformował, że w zakresie zadań Wydziału Spraw Obywatelskich od 1 stycznia 2015 r. wejdą w życie przepisy pozwalające na składanie wniosków i załatwianie ich w formie elektronicznej. Obecnie możliwe jest udostępnianie danych osobowych ze zbiorów meldunkowych, zbioru PESEL oraz ewidencji wydanych i unieważnionych dowodów osobistych za pomocą środków komunikacji elektronicznej. Informacja o tym zamieszczona jest w karcie informacyjnej F13/PG-1.4 w BIP Urzędu. Jednostką odpowiedzialną jest Wydział Spraw Obywatelskich, a odpowiedzialność osobista pracowników wydziału wynika z kart opisu stanowisk pracy.

(dowód: akta kontroli str. 70, 74)

### **1.11. Zakres i sposób współpracy systemów IT**

Opis stanu faktycznego

W czasie oględzin sposobu działania systemów stwierdzono, że Urząd posiada instrukcje użytkownika dla tych systemów (w formie elektronicznej), jednakże nie zawierają one opisu sposobu ich działania (w szczególności opisu: w jaki sposób i z jakich rejestrów prowadzonych przez Urząd dany system korzysta, jakie dane referencyjne są niezbędne, z jakich baz danych korzystają i jaki jest poziom współpracy pomiędzy nimi).

System Gospodarka Odpadami Komunalnymi (ERP) współpracuje na poziomie dwustronnej komunikacji<sup>11</sup> z systemem KASA (obsługującym również Masowe Płatności) oraz został przygotowany do współpracy z systemem Masowe Płatności (jeszcze nie był wykorzystywany), a z systemem Ewidencja ludności współpracuje na poziomie informacyjnym<sup>12</sup>. Dotychczas nie złożono Deklaracji za pomocą ePUAP.

<sup>11</sup> Poziom współpracy dwustronnej komunikacji, - tj. dane z jednego systemu informatycznego przekazywane są do innego systemu, wymagane jest zatwierdzenie wyników przez operatora, odpowiedź z systemu jest przekazywana analogicznie.

<sup>12</sup> Poziom współpracy informacyjny - gdy pracownicy wiedzą, że konkretne systemy gromadzą dane i że w razie potrzeb mogą z nich skorzystać, znają też sposób dostępu do danych zgromadzonych w systemach, np. jak wygenerować odpowiednie dane do pliku.



System Zarządzanie Mieniem współpracuje tylko z systemem ZAMEK (Księgowość dochodów niepodatkowych) na poziomie dwustronnej komunikacji<sup>9</sup>. System Zarządzanie Mieniem przekazuje wprowadzone dane umów dzierżaw i najmu (m.in.: imię nazwisko, nazwa podmiotu -osoba fizyczna lub prawna, numer umowy, nazwa celu, adres, kwota) do modułu Księgowość dochodów niepodatkowych, który automatycznie przekazuje informacje o zaksięgowanych dochodach.

Aplikacja Masowe Płatności współpracuje z systemem bankowym na poziomie informacyjnym (pobieranie pliku csv przez pracownika Urzędu) oraz z system KASA na poziomie komunikacji jednostronnej (pobór danych z plików przelewów przez pracownika w Wydziale Podatków).

Aktualnie dla systemu Ewidencja Nieruchomości (KTRM) jest tworzona ręcznie baza danych (dane są wprowadzane przez pracowników Urzędu). Planowane jest komunikowanie się tego systemu z system Zarządzanie Mieniem (EMKA) oraz Księgowości dochodów niepodatkowych na poziomie dwustronnym.

Z ustaleń tych wynika, że dwa systemy (Gospodarka Odpadami Komunalnymi, Zarządzanie Mieniem) wymieniają dane z innymi systemami na poziomie dwustronnej komunikacji, system Masowe Płatności działa z innym systemem na poziomie komunikacji jednostronnej a system Ewidencja Nieruchomości jest w trakcie realizacji etapu ręcznego tworzenia bazy danych. W przypadku ww. czterech systemów nie stwierdzono współpracy z systemem wewnętrznego obiegu dokumentów (eSOD) oraz ePUAP.

(dowód: akta kontroli str. 151 do 157)

## **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:

- portali internetowych (Portal Informacyjny Administracji, Centralna Ewidencja Pojazdów i Danych - CEPiK, Baza Azbestowa, Urząd Zamówień Publicznych Portal Centralny Serwis Informacyjny);
- systemu Wydawania Dowodów Osobistych – SWDO;
- dzienników elektronicznych (Redakcja Dziennika Urzędowego MUW);
- platform internetowych (ePUAP, platforma wyborcza);
- poczty elektronicznej (m.in. przekazywanie sprawozdań ze statystyki zdarzeń w ewidencji ludności, sprawozdania Rb-WSa, Rb-N, Rb-Z);
- programów służących do wymiany informacji (Płatnik, Besti@);
- systemów Informacyjnych, sprawozdawczych (e-pefron, GUS, CAS, ISRB, System Harmonogramowania Rejestracji i Monitorowania Pomocy - SHRIMP).

Urząd od grudnia 2011 r. odbierał korespondencję od MUW wyłącznie w formie elektronicznej. Pisma kierowane z Urzędu (m.in. do MUW) były archiwizowane w formie papierowej (oryginały, bądź wydruki), natomiast przesyłane w formie elektronicznej na życzenie strony.

(dowód: akta kontroli str. 69, 70 do 74)

Ponadto Burmistrz podał, że Urząd zwrócił się 17 kwietnia 2013 r. do Ministra Spraw Wewnętrznych o udostępnienie danych lub informacji z centralnej ewidencji pojazdów oraz danych z centralnej ewidencji kierowców za pośrednictwem sieci publicznej z wykorzystaniem urządzeń teletransmisji danych, na rzecz Straży Miejskiej w Olkuszu. W dniu 14 sierpnia 2013 r. Minister Spraw Wewnętrznych wyraził zgodę na udostępnienie ww. danych i informacji. W odpowiedzi na pytanie czy inny organ administracji publicznej zwrócił się z wnioskiem do Urzędu o prowadzenie wzajemnej komunikacji elektronicznej, a jeśli tak, to jaki był wynik tych działań, Burmistrz wyjaśnił, że:

- W czerwcu 2012 r. Biuro Informatyki MUW zwróciło się z wnioskiem o wzajemne komunikowanie się przez platformę ePUAP w sprawie przekazywania aktualizacji z lokalnej bazy danych zbiorów meldunkowych wyłącznie w formie elektronicznej; od lipca 2012 r. aktualizacja ww. bazy danych jest realizowana przez ePUAP;

- Urzędy Skarbowe zwróciły się z prośbą o podanie adresu elektronicznej skrzynki umieszczonej na platformie ePUAP, w formie elektronicznej przekazywane są stosowne sprawozdania.

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

- informacje związane z aktami stanu cywilnego i danymi statystycznymi;
- sprawozdania Rb-27S, Rb-28S, Rb-NDS, Rb-N, Rb-Z, Rb-PDP, Rb-UZ, Rb-UN, Rb-ST i bilans skonsolidowany (opatrzone bezpiecznym podpisem elektronicznym); Rb-50, Rb-27ZZ, Rb-ZN (bez podpisu elektronicznego);
- dokumenty do Komisji Nadzoru Finansowego – raporty espi i Krajowego Depozytu Papierów Wartościowych;
- REGON, NIP, dane osobowe itp., w zakresie zamieszczania danych na podstawie ustawy o utrzymaniu czystości i porządku w gminach oraz ustawy o zbiorowym zaopatrzeniu w wodę i zbiorowym odprowadzaniu ścieków;
- sprawozdania z finansowania ośrodków wsparcia, plan finansowy danego roku, karta dużej rodziny;
- korespondencję pomiędzy gminami dotyczącą obowiązku meldunkowego oraz aktualizacja danych osobowych zawartych w zbiorach meldunkowych mieszkańców;
- korespondencję z Departamentem Ewidencji Państwowych Ministerstwa Spraw Wewnętrznych w sprawie nadania numeru PESEL;
- rejestry kart dodatkowych w rejestrze wyborców, czyli przesyłanie informacji o dopisaniu lub skreśleniu z rejestru wyborców gminy;
- informacje o rodzaju, ilości i miejscu występowania odpadów zawierających azbest (Baza azbestowa);
- dane o wytwarzaniu i gospodarowaniu odpadami, z rejestrem udzielanych zezwoleń;
- akty prawa miejscowego w postaci „tekstu strukturalnego w formacie XML”
- zapytania o właściciela pojazdu na podstawie nr rejestracyjnego w prowadzonych postępowaniach;
- obsługa dokumentów ubezpieczeniowych i wymiana informacji z ZUS;
- w zakresie obowiązkowych wpłat na PFRON;
- ogłoszenia zamówień publicznych;
- wnioski, sprawozdania, rozliczenia (dotacja w zakresie zwrotu podatku akcyzowego zawartego w cenie oleju napędowego wykorzystywanego do produkcji rolnej producentom rolnym) i ankiet (dot. planowania budżetu państwa);
- informacje i sprawozdania w zakresie pomocy publicznej.

(dowód: akta kontroli str. 70 do 74)

#### Ocena cząstkowa

Najwyższa Izba Kontroli ocenia pozytywnie działalność Urzędu w zakresie dostosowania posiadanych systemów teleinformatycznych do współpracy z systemami używanymi przez inne podmioty administracji publicznej. Wymiana informacji z Małopolskim Urzędem Wojewódzkim i kilkoma innymi urzędami odbywała się w formie elektronicznej. System wewnętrznego obiegu dokumentów (eSOD) został zintegrowany z platformą ePUAP. Opisy procedur przedstawione na stronach ePUAP, mimo że nie były całkowicie tożsame z opisami zamieszczonymi na stronach Urzędu i BIP pozwalały jednak na skorzystanie z nich.

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 dla przetwarzania danych osobowych wprowadzona zarządzeniem nr 0151/846/2004 Burmistrza Miasta i Gminy w Olkuszu z dnia 4 października 2004 r. Polityka bezpieczeństwa do czasu niniejszej kontroli NIK nie była aktualizowana ani zmieniana.

(dowód: akta kontroli str. 18 do 22, 195 do 197, 203 do 220)

W ramach wykonywania innych zadań służbowych zleconych przez przełożonych Burmistrz zlecił 1 lipca 2012 r. Naczelnikowi Wydziału Zarządzania Kryzysowego, Ochrony Ludności i Spraw Obronnych nadzór nad ochroną danych osobowych w Urzędzie jako Administratorowi Bezpieczeństwa Informacji. W dokumencie nie zamieszczono żadnego odniesienia do realizacji zadań lub obowiązków wynikających z rozporządzenia KRI.

(dowód: akta kontroli str. 23 do 26)

Instrukcję Zarządzania Systemem Informatycznym (Instrukcja) wprowadzono zarządzeniem Nr 0152/94/2009 Burmistrza Miasta i Gminy Olkusz z dnia 22 czerwca 2009 r. Określało ono m.in. Administratorów Systemu Informatycznego w Urzędzie (ASI), tj. informatyków zatrudnionych w Urzędzie, zobowiązywało do zapoznania się z Instrukcją wszystkich pracowników przetwarzających dane osobowe w postaci cyfrowej a wykonanie zarządzenia powierzało ABI. Do dokumentu dołączono kartę potwierdzeń otrzymania w listopadzie 2009 r. zarządzenia przez poszczególne komórki organizacyjne Urzędu. Instrukcja do czasu niniejszej kontroli NIK nie była aktualizowana ani zmieniana.

(dowód: akta kontroli str. 18 do 22, 91 do 96, 269 do 271)

Burmistrz wyjaśnił, że „*W przepisach (...) do dnia dzisiejszego nie nastąpiły żadne zmiany, które wymuszałyby konieczność wykonania ich na nowo. Obecnie dokonywana jest aktualizacja Polityki Bezpieczeństwa w zakresie ochrony danych, jak również Instrukcja zarządzania Systemem Informatycznym, które zostaną wdrożone w bieżącym roku*”.

(dowód: akta kontroli str. 125 do 128)

W Urzędzie od czasu sporządzenia Polityki bezpieczeństwa ochrony danych osobowych (2006 r.) oraz Instrukcji Zarządzania Systemem Informatycznym (2009 r.) zakupiono licencje na kolejne programy komputerowe (m.in. w 2009 r. na system elektronicznego obiegu dokumentów – tzw. eSOD, w latach 2012 – 2013 na oprogramowanie dotyczące Ewidencji ludności, Rejestru Wyborców, Urzędu Stanu Cywilnego oraz na moduły systemu ZSI Urząd: Ewidencja Nieruchomości, Zarządzanie Mieniem, Księgowość Niepodatkowa, Masowe Płatności). Zapisy w Polityce bezpieczeństwa w obszarze przetwarzania danych osobowych były nieaktualne w zakresie wskazania numerów pomieszczeń lub ich części, nazw referatów/wydziałów/biur. Dane te zmieniane były od czasu sporządzenia Polityki bezpieczeństwa w 2004 r. kilkukrotnie, w tym w latach 2012 – 2014 (m.in. zmiany Regulaminu Organizacyjnego zawierające m.in. zmiany komórek organizacyjnych Urzędu z 13 lutego 2012 r., 17 czerwca 2013 r. i 12 lutego 2014 r.).

(dowód: akta kontroli str. 3 do 5, 13 do 15, 197)

W badanym okresie zmieniano m.in. zasady obiegu korespondencji w 2012 r. wprowadzając nowe załączniki wyłączające z zasad obiegu korespondencji elektronicznej w eSOD m.in. sprawy podlegające rejestracji w innych systemach tzw. „dziedzinowych”.

W 2012 r. ustalono również zakresy czynności dla Koordynatora Zarządzania Jakością (odpowiedzialnego za koordynację i wdrożenie systemu eSOD) oraz Administratora Bezpieczeństwa Informacji (nadzór nad ochroną danych osobowych). W zakresach czynności tych osób nie odniesiono się do zadań lub obowiązków wynikających z KRI.

(dowód: akta kontroli str. 16, 18 do 22, 23 do 26, 27, 28)

Ustalone  
nieprawidłowości

W Urzędzie nie opracowano i nie wdrożono nowej Polityki Bezpieczeństwa Informacji, która jest elementem systemu zarządzania bezpieczeństwem informacji. Zauważyć należy, że w myśl § 20 ust. 3 rozporządzenia KRI, wymagania w zakresie systemu zarządzania bezpieczeństwem informacji uznaje się za spełnione jeżeli została opracowana na podstawie Polskiej Normy: PN-ISO/IEC 27001:2007 Technika informatyczna. Techniki bezpieczeństwa. Systemy zarządzania bezpieczeństwem informacji oraz powiązanej z nią Polskiej Normy PN-ISO/IEC 17799:2007 Technika informatyczna. Techniki bezpieczeństwa. Praktyczne zasady zarządzania bezpieczeństwem informacji. W pkt 5.1.1. normy PN-ISO/IEC17799 wskazano opracowanie i stosowanie dokumentu polityki bezpieczeństwa informacji. W 2004 r. w Urzędzie opracowano Politykę bezpieczeństwa dla przetwarzania danych osobowych. Nie dotyczyła ona jednak wszystkich danych jakie są obecnie przetwarzane w Urzędzie. Nie uwzględniała np. zmian wprowadzonych w 2012 r., zasad obiegu korespondencji w związku z wprowadzeniem systemu eSOD, systemów zakupionych lub modernizowanych po 31 maja 2012 r.

## 2.2. Sprzęt informatyczny

Opis stanu  
faktycznego

Na próbie 10 skontrolowanych komputerów stwierdzono, że inwentaryzacja zasobów informatycznych jednostki była niekompletna i nieaktualizowana. Dane sprzętu komputerowego ujmowano w układzie tradycyjnej książki inwentarzowej (dla potrzeb rachunkowości), która nie zawierała danych szczegółowych o konfiguracji technicznej urządzeń czy też o zainstalowanym oprogramowaniu. Dla 10 skontrolowanych komputerów Urząd nie posiadał aktualnych informacji o zainstalowanym na nich oprogramowaniu oraz kompletnych danych o ich konfiguracji (np. rodzaj karty graficznej opisany tylko jako „zintegrowana”, brak informacji o aktualnym oprogramowaniu antywirusowym i zainstalowanych programach systemowych dla pracy Urzędu, np. programy tzw. „dziedziczne” jak gospodarowanie odpadami). Ponadto dla czterech komputerów przekazanych do użytkowania przez Ministerstwo Spraw Wewnętrznych i Administracji porozumieniem z 5 listopada 2010 r. (aneksowanym 31 grudnia 2013 r.) Urząd nie posiadał dokumentów dotyczących inwentaryzacji sprzętu, o której mowa w § 20 ust. 2 pkt 2 rozporządzenia KRI. W porozumieniu tym wskazano m.in. (§ 3, pkt 9), że Użytkownik zobowiązał się do zachowania należytej staranności w celu zabezpieczenia Produktów Projektu (tj. m.in. zestawów komputerowych, oprogramowania standardowego, aplikacji itd.) od momentu ich przekazania, w tym zabezpieczenia przed dostępem osób trzecich.

(dowód: akta kontroli str. 75 do 90)

W Zasadach zarządzania oprogramowaniem w Urzędzie<sup>13</sup> (Zasady) określono m.in., że aktualny stan zainstalowanego oprogramowania musi być zgodny z przeprowadzoną inwentaryzacją odnotowaną w karcie informacyjnej, która jest przechowywane przez ASI. Odpowiadali oni za funkcjonowanie systemu informatycznego w Urzędzie.

(dowód: akta kontroli str. 91 do 96, 108 do 113)

Zgodnie z § 20 ust. 2 pkt 2 rozporządzenia KRI Urząd zobowiązany jest do zapewnienia przez kierownictwo podmiotu publicznego warunków umożliwiających realizację i egzekwowanie utrzymywania aktualności inwentaryzacji sprzętu i oprogramowania służącego do przetwarzania informacji obejmującej ich rodzaj i konfigurację. Zgodnie z normą PN-ISO/IEC 17799:2007, pkt 7.1.1, wszystkie aktywa informatyczne powinny być zidentyfikowane i aktualizowane. Aktualna inwentaryzacja m.in. sprzętu informatycznego powinna także zawierać informację o jego rodzaju i konfiguracji, przez co możliwe będzie odtworzenie po katastrofie lub innym zdarzeniu losowym.

W trakcie przeprowadzonych oględzin 10 komputerów i jednego serwera stwierdzono, że mimo iż Urząd posiadał trzy segregatory kart informacyjnych to odnaleziono jedynie cztery karty informacyjne urządzeń spośród 11 poddanych oględzinom (w tym dla serwera). Siedem komputerów, z 10 które zostały poddane oględzinom, nie posiadało kart informacyjnych. W żadnej z kart informacyjnych nie umieszczono daty jej sporządzenia, numeru seryjnego urządzenia, adnotacji o dokonywanych przeglądach, konserwacjach,

<sup>13</sup> Zarządzenie nr 0152/22/2007 Burmistrza Miasta i Gminy Olkusz z dnia 7 maja 2007 r. w sprawie zasad zarządzania oprogramowaniem w Urzędzie Miasta i Gminy w Olkuszach zmienione zarządzeniem nr 0050.2558.2014 z dnia 3 marca 2014 r.

wymianach, naprawach lub aktualizacjach/zmianach oprogramowania, które były dokonywane po dacie zakupu urządzenia. Wszystkie cztery przedstawione karty informacyjne nie zawierały aktualnych danych o oprogramowaniu zainstalowanym na danym urządzeniu (m.in. informacji o użytkowanych na przedmiotowych 10 komputerach: programach dziedzinowych i oprogramowaniu antywirusowym).

(dowód: akta kontroli str. 3 do 5, 75 do 76, 87 do 89, 107)

W opinii Burmistrza dokumentacja zasobów informatycznych prowadzona w formie papierowej zawierała informacje o konfiguracji sprzętowej zestawu komputerowego oraz zainstalowanego oprogramowania. Cyt.: „Karta informacyjna zawiera wyszczególnione elementy (procesor, pamięć ram, dysk, napęd optyczny, karta grafiki, karta dźwiękowa, karta sieciowa) jednostki komputerowej z podaniem ogólnych parametrów. Karty informacyjne w miarę możliwości są aktualizowane poprzez ręczne wpisy nowo instalowanego/odinstalowanego oprogramowania oraz wymienianych podzespołów”, jednak przyznał, że: „Uchybienia zaistniałe podczas oględzin przez specjalistę kontroli państwowej zostają sukcesywnie usuwane” (...) Urząd w budżecie na rok 2015 „zaplanuje zakup niezbędnego oprogramowania do zarządzania siecią LAN (w tym moduł zarządzania zasobami).”

(dowód: akta kontroli str. 127 do 128)

Ustalone  
nieprawidłowości

W działalności kontrolowanej jednostki w przedstawionym wyżej zakresie stwierdzono nieprawidłowość polegającą na braku kompletnej i aktualizowanej inwentaryzacji kontrolowanego sprzętu komputerowego, co było niezgodne z § 20 ust. 2 pkt 2 rozporządzenia KRI.

### **2.3. Analizy utraty integralności, poufności lub dostępności informacji**

Opis stanu  
faktycznego

W okresie od 31 maja 2012 r. w Urzędzie nie przeprowadzono okresowych analiz utraty integralności, poufności lub dostępności informacji. W badanym okresie nie wystąpił przypadek zgłoszenia incydentów naruszenia bezpieczeństwa informacji.

(dowód: akta kontroli str. 16, 195, 196)

Burmistrz wyjaśnił, że w nowooperacowanej Polityce Bezpieczeństwa Informacji zostaną uwzględnione procedury dotyczące przeprowadzania okresowych analiz utraty integralności, poufności lub dostępności informacji.

(dowód: akta kontroli str. 265, 267)

Obowiązek przeprowadzania okresowych analiz ryzyka utraty integralności, dostępności lub poufności informacji oraz podejmowania działań minimalizujących to ryzyko, stosownie do wyników przeprowadzonej analizy, został nałożony na podmiot realizujący zadania publiczne w § 20 ust. 2 pkt 3 rozporządzenia KRI.

### **2.4. Realizacja nadawania uprawnień użytkownikom**

Opis stanu  
faktycznego

W czasie kontroli, na podstawie oględzin stwierdzono, że na 6 z 10 komputerów, na których realizowane były przez pracowników Urzędu zadania związane z: ewidencją ludności, ewidencją nieruchomości, zarządzaniem mieniem, gospodarowaniem odpadami komunalnymi i masowymi płatnościami, była możliwa instalacja dowolnego oprogramowania przez użytkownika tego komputera niebędącego pracownikiem służb informatycznych Urzędu. Możliwość zainstalowania dowolnego oprogramowania naruszała postanowienia (§ 20 ust. 2 pkt 7 c rozporządzenia KRI), który nakłada na kierownictwo podmiotu publicznego realizację i egzekwowanie zapewnienia środków uniemożliwiających nieautoryzowany dostęp na poziomie systemów operacyjnych, usług sieciowych i aplikacji. Stan ten był niezgodny także z powszechnie przyjętą praktyką określoną 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. 75 do 90)

Burmistrz wyjaśnił, że cyt.: „Uchybienie dotyczące posiadania przez niektórych użytkowników komputerów uprawnień administratora (...) zostają sukcesywnie usuwane”.

(dowód: akta kontroli str. 125, 128)

W Instrukcji Zarządzania Systemem Informatycznym Urzędu określono, że bezpośredni dostęp do systemu informatycznego może mieć miejsce wyłącznie po podaniu identyfikatora i właściwego hasła. W Polityce bezpieczeństwa opracowano zasady nadawania uprawnień użytkownikom, polegającą na wypełnieniu przez kierowników komórek organizacyjnych Urzędu dokumentu pn. „Karta nadania upoważnienia dla użytkownika do przetwarzania danych osobowych”. W Urzędzie zaniechano przekazywania wniosków o odebranie uprawnień dostępu do systemów informatycznych skutkiem czego odbieranie uprawnień przez ASI<sup>14</sup> odbywało się na podstawie tzw. „Karty Obiegowej Rozliczenie pracownika w związku z ustaniem stosunku pracy”, zamiast wskazanego w Polityce Bezpieczeństwa wniosku przekazywanego przez ABI do ASI, ponieważ ABI nie przekazywał do ASI wniosków o odebranie uprawnień.

(dowód: akta kontroli str. 75 do 90, 196, 197, 198, 201, 202, 228, 229, 272 do 309)

Burmistrz wyjaśnił, że nie zaniechano wniosków o odebranie uprawnień, bo w sytuacji braku informacji od naczelnika wydziału, odebranie uprawnień przez ASI następowało na podstawie „Karty Obiegowej Rozliczenie pracownika w związku z ustaniem stosunku pracy”.

(dowód: akta kontroli str. 265-267)

W badanym okresie osiem osób, które miały dostęp do systemów tzw. „dziedzinowych” 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 systemami, tzw. „dziedzinowymi” stwierdzono, że posiadają one uprawnienia do systemów, jednak ich zakresy czynności wskazane w upoważnieniach i w kartach opisu stanowisk pracy nie odpowiadały definicjom „nazw ról” i zasobów/zakładek wpisanych w systemy dziedzinowe, co uniemożliwiało weryfikację zasadności nadanych uprawnień.

(dowód: akta kontroli str. 151 do 154, 223, 257, 272 do 310)

W odpowiedzi na pytanie: kto i na jakiej podstawie wskazywał zbiory, do których ASI nadawali uprawnienia poszczególnym pracownikom skoro zakresy czynności wskazany w upoważnieniu i karcie opisu stanowiska pracy nie odpowiadały definicjom „nazw ról” i zasobów/zakładek wpisanych w systemy dziedzinowe, Burmistrz wyjaśnił m.in., że ASI nadają uprawnienia poszczególnym pracownikom na podstawie podpisanego przez niego Upoważnienia sporządzonego przez ABI w oparciu o Kartę nadania upoważnienia dla użytkownika do przetwarzania danych osobowych. Upoważnienie to zawiera zakresy uprawnień dla poszczególnych użytkowników, a jego aktualizacja jest dokonywana przez naczelników po pisemnej prośbie ABI. Zdarza się, iż nazwa rejestru w tym upoważnieniu nie wskazuje wprost nazwy programu, lub modułu programu, do którego użytkownik otrzymał uprawnienia. I wtedy ASI przydziela uprawnienia na podstawie własnej wiedzy kto jakie programy w Urzędzie obsługuje.

(dowód: akta kontroli str. 265, 268)

Ustalone  
nieprawidłowości

W działalności kontrolowanej jednostki w przedstawionym wyżej zakresie stwierdzono następujące nieprawidłowości:

- posiadanie uprawnień administratora przez użytkowników systemów informatycznych niebędących pracownikami służb informatycznych, co dawało im możliwość nieuprawnionego instalowania oprogramowania na komputerach służbowych<sup>15</sup>. Zgodnie z zapisami normy PN-ISO/IEC 17799:2007 pkt 11.2.2 lit. b) należy ograniczyć i kontrolować przyznawanie oraz korzystanie z przywilejów w systemach informatycznych według minimalnych wymagań wynikających z przydzielonych pracownikom zadań służbowych. Zdaniem NIK potrzeba ograniczenia uprawnień

<sup>14</sup> Administrator Systemu Informatycznego

<sup>15</sup> Sprawdzono na próbie 10 komputerów.

związana jest również z ryzykiem polegającym na możliwości nieświadomego zainstalowania przez użytkownika złośliwego oprogramowania. Oprogramowanie antywirusowe nie zawsze jest gwarancją bezpiecznej pracy w systemie informatycznym;

- niepełne przestrzeganie procedury nadawania uprawnień użytkownikom systemów informatycznych wykorzystywanych w Urzędzie.

Uwagi dotyczące badanej działalności

Niepełna korelacja nazw zakresów czynności wskazanych w upoważnieniach i w kartach opisu stanowisk pracy z definicjami „nazw ról” i zasobów/zakładek wpisanych w systemy dziedzinowe, nie pozwalała na weryfikację zasadności zakresu nadanych uprawnień.

## 2.5. Szkolenia pracowników przetwarzających informacje

Opis stanu faktycznego

W Urzędzie zaplanowano i zrealizowano szkolenia z zakresu e-usług, na które skierowano 9 osób (m.in. szkolenia pn. „małopolski konwent informatyków”, „forum IT”, „nowoczesny sekretariat” i kancelaria w administracji publicznej”, „praktyczne warsztaty komputerowe z korzystania z platformy ePUAP”). Tematyka żadnego z nich nie odnosiła się bezpośrednio do zagadnień zagrożenia bezpieczeństwa informacji. Ponadto 15 osób odbyło kurs eUrządnik i uzyskało certyfikat na kursie zorganizowanym przez ZDZ w Katowicach Centrum Kształcenia Zawodowego w Olkuszu. Kurs ten obejmował kształcenie w zakresie uzyskania podstawowych umiejętności komputerowych w posługiwaniu się aplikacjami (CEIDG, ePUAP, BIP, eWokanda itd.).

(dowód: akta kontroli str. 43 do 62, 258 do 264)

Według stanu na 31 maja 2012 r. w Urzędzie było zatrudnionych 193 pracowników, a na 30 czerwca 2014 r. 189 (164 na stanowisku urzędniczym). W zakresie wdrożenia systemu usług elektronicznych w okresie od czerwca 2012 r. do czerwca 2014 r. przeszkolono 24 pracowników. W badanym okresie nie zaplanowano i nie zrealizowano szkoleń dotyczących bezpieczeństwa informacji.

(dowód: akta kontroli str. 17, 43 do 62)

Liczba osób posiadających uprawnienia do pracy z kontrolowanymi czterema systemami tzw. „dziedzinowymi” Urzędu wynosiła 41. Ponadto w czasie kontroli stwierdzono, że według stanu na 13 czerwca 2014 r. 170 pracowników posiadało 239 uprawnień do systemów informatycznych Urzędu (jeden pracownik posiadał uprawnienia do kilku systemów).

(dowód: akta kontroli str. 99 do 106, 223 do 227, 228 do 257)

Burmistrz wyjaśnił, że szkolenie wszystkich pracowników posiadających upoważnienie do przetwarzania danych osobowych odbyło się w sierpniu 2010 r. a kolejne planowane jest na IV kwartał 2014 r., po opracowaniu i wdrożeniu „nowej Polityki bezpieczeństwa przy przetwarzaniu danych osobowych w Urzędzie Miasta i Gminy w Olkuszu (...) Zapis § 20 ust. 2 pkt 6 rozporządzenia KRI (...) obejmuje szerszą problematykę dot. Ochrony informacji, która wydaje się być poza kompetencją ABI, którego funkcja i zadania wynikają z art. 36 pkt 3 ustawy o ochronie danych osobowych, w którym zapisano, że Administrator danych wyznacza administratora bezpieczeństwa informacji nadzorującego przestrzeganie zasad ochrony danych osobowych”.

(dowód: akta kontroli str. 265, 267)

W zakresie czynności ustalonym przez Burmistrza dla ABI określono, że jest on zobowiązany do: opracowywania i aktualizacji polityki bezpieczeństwa w zakresie danych osobowych oraz instrukcji zarządzania systemem informatycznym, wnioskowania w sprawie wyznaczania zasad zabezpieczenia i ochrony danych osobowych, szkolenia i kontroli pracowników Urzędu zatrudnionych przy przetwarzaniu danych osobowych ze znajomości /cyt./: „przepisów o ochronie danych i ich stosowaniu”.

(dowód: akta kontroli str. 23 do 26)

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 liczba osób przeszkolonych w odniesieniu do liczby osób zaangażowanych w Urzędzie w proces przetwarzania informacji w zakresie kontrolowanych czterech systemów tzw. „dziedzinowych” była niewystarczająca i stanowiła mniej niż 25 % (9 z 41).

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

Opis stanu faktycznego

W Urzędzie obowiązywało oświadczenie, które podpisywały osoby użytkujące przenośny sprzęt komputerowy, nie zawierało w nim jednak zapisów odnośnie wymogów określonych w § 20 ust. 2 pkt 8 rozporządzenia KRI. Dokument taki sporządzony dla 27 z 36 aktualnie użytkowanych w Urzędzie urządzeń tego typu stanowił załącznik do instrukcji gospodarki majątkiem trwałym z 27 września 2010 r. Ponadto w zarządzeniu Burmistrza nr 0152/22/2007 z 7 maja 2007 r. w sprawie: zarządzania oprogramowaniem w Urzędzie zawarto zapis mówiący o obowiązku zgłoszenia informatykom cyt.: „faktu opuszczenia budynku” przez sprzęt oraz pisemnego oświadczenia o odpowiedzialności za sprzęt i dane na nim się znajdujące. Zapis ten nie został utrzymany w obowiązującym od 3 marca 2014 r. zarządzeniu nr 0050.2558.2014. W okresie od 31 maja 2012 r. do czasu niniejszej kontroli nie złożono do informatyków żadnego zgłoszenia o wyniesieniu sprzętu komputerowego z budynku Urzędu.

(dowód: akta kontroli str. 97, 98, 108 do 113, 122 do 124)

Burmistrz wyjaśnił, że cyt.: „*W UMiG Olkusz do dnia dzisiejszego przetwarzanie mobilne w tym praca zdalna, praca na odległość, tj. możliwość uruchamiania programów wewnątrz sieci lokalnej Urzędu z dowolnego miejsca poza urzędem jest niemożliwa. (...) Uchybienia odnośnie ustanowienia podstawowych zasad gwarantujących bezpieczną pracę przy przetwarzaniu mobilnym i pracy na odległość zostaną usunięte w zaktualizowanej Instrukcji Zarządzania Systemem Informatycznym*”.

(dowód: akta kontroli str. 266, 268)

Ustalone nieprawidłowości

W działalności kontrolowanej jednostki stwierdzono nieprawidłowość polegającą na nieustaleniu zasad (procedur) gwarantujących bezpieczną pracę przy przetwarzaniu mobilnym i pracy na odległość co było niezgodne z § 20 ust. 2 pkt 8 rozporządzenia KRI.

## **2.7. Umowy serwisowe**

Opis stanu faktycznego

W umowie zawartej z firmą Sygnity SA na okres od 1 stycznia do 31 grudnia 2014 r., dotyczącej czterech wybranych do kontroli systemów tzw. „dziedzinowych”, tj. Urząd NT (świadczenie nadzoru autorskiego oraz usług serwisowych) zawarto zapis o zobowiązaniu się przez wykonawcę do ochrony danych poufnych a ich przetwarzanie zostało zastrzeżone w zakresie i celu związanym z realizacją umowy. We wcześniejszych dwóch umowach z ww. firmą (w roku 2012 i 2013) dotyczących systemów Urząd NT nie zawarto żadnych zapisów dotyczących poufności danych. W sumie na 22 umowy przedstawione do kontroli w pięciu nie zawarto stosownych zapisów o zobowiązaniu się przez wykonawcę do ochrony danych poufnych. W dokumentacji serwisowej zawarto zapis o przekazywaniu do naprawy sprzętu komputerowego bez nośników danych (dysków).

(dowód: akta kontroli str. 158 , 159, 160 do 194)

Burmistrz wyjaśnił m.in., że uchybienia w zapisach umów na zakup oprogramowania dotyczące zobowiązania się wykonawcy do ochrony danych poufnych zostaną usunięte.

(dowód: akta kontroli str. 266, 268)

Ustalone nieprawidłowości

W działalności kontrolowanej jednostki w przedstawionym wyżej zakresie stwierdzono nieprawidłowość polegającą na nieuwzględnieniu zapisów o zobowiązaniu się przez wykonawcę do ochrony danych poufnych w 5 umowach z 22, co było niezgodne z postanowieniami § 20 ust. 2 pkt 10 rozporządzenia KRI.



## **2.8. Zgłaszanie incydentów naruszenia bezpieczeństwa informacji**

Opis stanu faktycznego

Procedury postępowania w sytuacjach zgłoszenia naruszenia bezpieczeństwa informacji określono w Instrukcji zarządzania systemem informatycznym w Urzędzie, wprowadzonej zarządzeniem nr 0152/94/2009 Burmistrza Miasta i Gminy w Olkuszu, której otrzymanie potwierdzili naczelnicy wydziałów Urzędu.

Burmistrz wyjaśnił, że w Urzędzie nie wystąpił przypadek zgłaszania incydentów naruszenia bezpieczeństwa informacji. Procedura opisująca postępowanie w przypadku stwierdzenia takiego naruszenia została określona w Rozdziale IX Instrukcji.

(dowód: akta kontroli str. 11, 16, 93)

## **2.9. Audyt wewnętrzny z zakresu bezpieczeństwa informacji**

Opis stanu faktycznego

W okresie od 31 maja 2012 r. w Urzędzie nie przeprowadzono okresowego audytu wewnętrznego z zakresu bezpieczeństwa informacji, w związku z tym nie sformułowano i nie wdrażano rekomendacji związanych z audytem. Na lata 2012–2013 nie zaplanowano audytu bezpieczeństwa informacji (ani audytu systemów informatycznych). W obowiązującym planie audytu na 2014 r. zatwierdzonym przez Burmistrza zarządzeniem nr 0050.2393b.2013 z 30 grudnia 2013 r. przewidziano audyt bezpieczeństwa informacji dla systemu informatycznego (cyt.: „*audyt obligatoryjne wynikający z ustawy o informatyzacji*”).

(dowód: akta kontroli str. 16)

Burmistrz wyjaśnił, że plany audytu na lata 2012 i 2013 zostały sporządzone stosownie do wymogów ustawy o finansach publicznych, a obowiązek przeprowadzania corocznego audytu wewnętrznego bezpieczeństwa informacji został nałożony na podmiot realizujący zadania publiczne w § 20 ust.2 pkt 14 rozporządzenia KRI, w związku z czym audyt bezpieczeństwa informacji został ujęty w planie audytu wewnętrznego na rok 2014.

(dowód: akta kontroli str. 265, 267)

Ustalone nieprawidłowości

W działalności kontrolowanej jednostki w przedstawionym wyżej zakresie stwierdzono nieprawidłowość polegającą na niezrealizowaniu w latach 2012 - 2014 (30 lipca 2014 r.) wewnętrznego audytu w zakresie bezpieczeństwa informacji, co było niezgodne z § 20 ust. 2 pkt 14 rozporządzenia KRI.

## **2.10. Tworzenie i testowanie kopii zapasowych danych i oprogramowania aplikacyjnego**

Opis stanu faktycznego

W Instrukcji<sup>16</sup> określono obowiązek tworzenia i przechowywania kopii zapasowych (codziennie w dni robocze). Sporządzane w każdy dzień roboczy, zgodnie z przyjętą procedurą, kopie zabezpieczano na nośnikach w serwerowni oraz w sejfie w pomieszczeniu innym niż serwerownia. Utworzone kopie zapasowe nie były testowane, a Instrukcja nie zawierała takiego wymogu. Pomieszczenia, w których przechowywano kopie zostały zabezpieczone w podstawowym zakresie (kraty, alarm).

(dowód: akta kontroli str. 114 do 121)

ASI wyjaśnił, że w momencie zgrzywania z serwera utworzonej automatycznie kopii zapasowej oceniano czy spakowany plik kopii zapasowej ma poprawną datę, rozszerzenie i rozmiar co najmniej równy poprzedniej kopii a możliwości zgrania pliku z serwera na główny komputer (skąd są zgrywane na CD i przenoszone do sejfu) potwierdzała poprawność utworzenia pliku. Ponadto wskazał, że ocena przydatności kopii nie była możliwa na pracującym systemie a nie było sytuacji zaplanowanego wyłączenia systemów Urzędu.

(dowód: akta kontroli str. 310 do 311)

---

<sup>16</sup> Instrukcja Zarządzania Systemem Informatycznym Urzędu Miasta i Gminy Olkusz.

## 2.11. Format udostępniania zasobów informacyjnych badanych systemów informatycznych

Opis stanu faktycznego

Na przykładzie czterech wybranych do badania systemów dziedzinowych (podsystemy: Gospodarka Odpadami Komunalnymi, Zarządzanie Mieniem, Masowe Płatności, Ewidencja Nieruchomości), 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. 115)

Ocena częściowa

Najwyższa Izba Kontroli ocenia negatywnie działalność Urzędu w zakresie wdrażania systemu zarządzania bezpieczeństwem systemów informatycznych ponieważ w badanym okresie:

- nienależycie zrealizowano wymagania określone w § 20 ust. 3 rozporządzenia KRI gdyż nie opracowano i nie zaktualizowano Polityki Bezpieczeństwa Informacji, co nie zapewniło rzetelnego nadzoru nad bezpieczeństwem informacji w Urzędzie;
- brak było kompletnej i aktualnej inwentaryzacji sprzętu komputerowego i posiadanego oprogramowania;
- nie w pełni realizowano procedurę nadawania stosownych uprawnień użytkownikom systemów informatycznych wykorzystywanych w Urzędzie;
- nie zapewniono przeszkolenia osób zaangażowanych w proces przetwarzania informacji;
- nie ustalono zasad (procedur) gwarantujących bezpieczną pracę przy przetwarzaniu mobilnym i pracy na odległość;
- w części umów dotyczących zakupu, serwisu bądź oprogramowania sprzętu informatycznego zawartych przez Urząd w latach 2012 - 2013 brak było zapisów gwarantujących odpowiedni poziom bezpieczeństwa informacji;
- nie zrealizowano wewnętrznego audytu w zakresie bezpieczeństwa informacji, mimo że na podstawie § 20 ust. 2 pkt. 14 rozporządzenia KRI powinien odbywać się nie rzadziej niż raz na rok.

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

Opis stanu faktycznego

Strona internetowa Urzędu działa pod adresem [www.umig.olkusz.pl](http://www.umig.olkusz.pl) i została przygotowana do potrzeb osób niedowidzących poprzez umieszczenie w prawym górnym rogu znaczników pozwalających na otwarcie strony w wysokim kontraście lub pisanej większą czcionką. Weryfikacja zgodności strony Urzędu ze standardem WCAG 2.0 dokonana poprzez wykorzystanie narzędzi dostępnych na stronie internetowej <http://jigsaw.w3.org/css-validator/> nie wykazała istotnych niezgodności ze standardem WCAG 2.0. w zakresie zasady 4-Kompatybilność z uwzględnieniem poziomu A (informacja o wystąpieniu 2 błędów i 13 ostrzeżeń). Strona Urzędu nie dawała możliwości odsłuchania zapisu informacji, natomiast zawierała informacje o sposobie udostępniania obsługi dla osób doświadczających trwale lub czasowo trudności w komunikowaniu się (m.in. informacje o dostępności komunikatora internetowego Skype – umig\_olkusz).

Na stronie głównej Urzędu (na samym dole po lewej stronie) umieszczono link do strony BIP Urzędu, która działa pod adresem: [bip.malopolska.pl/umigolkusz/Article/id,240778.html](http://bip.malopolska.pl/umigolkusz/Article/id,240778.html) i została przygotowana do potrzeb osób niedowidzących.

(dowód: akta kontroli str. 29 do 42)

Ocena częściowa

Najwyższa Izba Kontroli nie formułuje oceny częściowej w tym obszarze.

## IV. Uwagi i 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<sup>17</sup>, wnosi o:

- 1) opracowanie i wdrożenie Polityki Bezpieczeństwa Informacji określającej zasady bezpieczeństwa informacji oraz wykonywanie corocznych audytów w tym zakresie;
- 2) uniemożliwienie instalowania oprogramowania przez osoby nieuprawnione oraz przestrzeganie procedury nadawania i odbierania uprawnień;
- 3) zaktualizowanie inwentaryzacji sprzętu komputerowego i jego oprogramowania;
- 4) przeszkolenie wszystkich osób zaangażowanych w proces przetwarzania informacji w zakresie, o którym mowa w § 20 ust. 2 pkt 6 rozporządzenia w sprawie KRI.

## 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 7 sierpnia 2014 r.

Kontroler  
Małgorzata Kram  
Specjalista k.p.

Podpisał  
Marcin Kopec  
Wicedyrektor

.....  
*podpis*

<sup>17</sup> Dz. U. z 2012 r., poz.82, ze zm.