



NAJWYŻSZA IZBA KONTROLI  
Departament Administracji Publicznej

KAP – 4110-01-01/2013  
R/13/006/KAP

# WYSTĄPIENIE POKONTROLNE

NAJWYŻSZA IZBA KONTROLI  
ul. Filtrowa 57, 02-056 Warszawa  
T +48 22 444 53 08, F +48 22 444 52 52  
[kap@nik.gov.pl](mailto:kap@nik.gov.pl)  
Adres korespondencyjny: Skr. poczt. P-14, 00-950 Warszawa 1

## I. Dane identyfikacyjne kontroli

<i>Numer i tytuł kontroli</i>	R/13/006/KAP – Ocena postępu wdrożenia wybranych wymagań nałożonych na systemy informatyczne przez rozporządzenie Rady Ministrów w sprawie Krajowych Ram Interoperacyjności
<i>Jednostka przeprowadzająca kontrolę</i>	Najwyższa Izba Kontroli Departament Administracji Publicznej
<i>Kontrolerzy</i>	1. Mariusz Stolarz, główny specjalista kontroli państwowej, upoważnienie do kontroli nr 89264 z dnia 21 listopada 2013 r. 2. Maciej Mierzejewski, główny specjalista kontroli państwowej, upoważnienie do kontroli nr 89262 z dnia 21 listopada 2013 r. <p style="text-align: right;">[dowód: akta kontroli str. 1-4]</p>
<i>Jednostka kontrolowana</i>	Urząd Miasta w Bielsku-Białej (dalej Urząd)
<i>Kierownik jednostki kontrolowanej</i>	Jacek Krywult, Prezydent Miasta (dalej Prezydent Miasta)
<i>Zakres kontroli</i>	Ocena prawidłowości i skuteczności działań podjętych przez Prezydenta Miasta Bielska-Białej, dotyczących spełnienia przez funkcjonujące w Urzędzie Miejskim w Bielsku-Białej systemy teleinformatyczne wymagań wprowadzonych rozporządzeniem Rady Ministrów w sprawie Krajowych Ram Interoperacyjności <sup>1</sup> (dalej rozporządzenie KRI), w szczególności: <ul style="list-style-type: none"><li>– dostosowania posiadanych systemów teleinformatycznych do współpracy z systemami/rejestrami używanymi przez podmioty administracji publicznej,</li><li>– stopnia wdrożenia zarządzania bezpieczeństwem systemów IT,</li><li>– zapewnienia dostępności informacji dla osób niepełnosprawnych.</li></ul>
<i>Okres objęty kontrolą</i>	Od 31 maja 2012 r. do 20 grudnia 2013 r.
<i>Kryteria kontroli</i>	Kontrolę przeprowadzono na podstawie art. 2 ust. 2 ustawy z dnia 23 grudnia 1994 r. o Najwyższej Izbie Kontroli <sup>2</sup> z uwzględnieniem art. 5 ust. 1 wymienionej ustawy, tj. pod względem legalności, gospodarności i rzetelności.

<sup>1</sup> 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>2</sup> Dz. U. z 2012 r., poz. 82 ze zm.

## II. Ocena kontrolowanej działalności

Najwyższa Izba Kontroli ocenia pozytywnie<sup>3</sup> działalność kontrolowanej jednostki w zakresie wdrożenia wybranych wymagań nałożonych na systemy informatyczne przez rozporządzenie KRI w okresie od 31 maja 2012 r. do 20 grudnia 2013 r.

Pozytywną ocenę uzasadniają podjęte i prawidłowo realizowane przez Prezydenta Miasta działania w celu zapewnienia interoperacyjności systemów informatycznych funkcjonujących w Urzędzie i bezpieczeństwa informacji oraz zakres świadczonych usług elektronicznych<sup>4</sup>. Podstawę pozytywnej oceny stanowi w szczególności:

- zapewnienie współpracy pomiędzy wybranymi do badania systemami informatycznymi w sposób spełniający minimalne wymogi w zakresie interoperacyjności, w szczególności poprzez wzajemną komunikację oraz udostępnianie danych w formatach określonych w rozporządzeniu KRI,
- rzetelne zarządzanie bezpieczeństwem informacji w Urzędzie oparte na zaleceniach zawartych w Polskiej Normie *Technika informatyczna. Techniki bezpieczeństwa. Systemy zarządzania bezpieczeństwem informacji* (PN-ISO/EIC 27001:2007), a także fakt, że strona internetowa Urzędu oraz BIP spełniały wymagania sformułowane w rozporządzeniu KRI dotyczące dostosowania systemów prezentujących treści do wymagań dotyczących dostępności dla osób niepełnosprawnych<sup>5</sup> w zakresie zasady kompatybilności,
- wdrożenie w Urzędzie w ramach Zintegrowanego Systemu Zarządzania (dalej ZSZ) procesów dotyczących udostępniania usług z wykorzystaniem systemów informatycznych w sposób pozwalający na należyłą i uporządkowaną organizacyjnie obsługę mieszkańców,
- udostępnienie klientom Urzędu 200 usług elektronicznych

Pozytywnie należy również ocenić i wskazać jako dobrą praktykę fakt, że Urząd publikuje i uaktualnia opisy procedur obowiązujących przy załatwianiu spraw drogą elektroniczną w Biuletynie Informacji Publicznej Urzędu oraz na stronie internetowej (poprzez odesłanie do systemu SEKAP).

Stwierdzone w toku kontroli nieprawidłowości dotyczyły:

- nieujęcia jednego urządzenia informatycznego w oprogramowaniu ewidencyjnym, co było niezgodne z § 20 ust. 2 pkt 2 rozporządzenia KRI,
- nieusunięcia z systemu informatycznego konta jednego użytkownika (pracownika), który zakończył pracę w Urzędzie, co wymagane jest przepisem § 20 ust. 2 pkt 5 ww. rozporządzenia.

Ponadto, do dnia zakończenia kontroli nie został w pełni wdrożony do eksploatacji system e-Audytor, pomimo, że środki publiczne w wysokości 55 974 zł na jego zakup wydatkowano w 2012 r., co NIK ocenia jako nierzetelność.

Nieprawidłowości nie miały istotnego wpływu na wdrażanie wymagań określonych w rozporządzeniu KRI i nie skutkowały obniżeniem oceny.

<sup>3</sup> Najwyższa Izba Kontroli (dalej NIK) stosuje 3-stopniową skalę ocen: pozytywna, pozytywna, mimo stwierdzonych nieprawidłowości, negatywna.

<sup>4</sup> Usługą elektroniczną w myśl art. 2 pkt 4 ustawy z dnia 18 lipca 2002 r. o świadczeniu usług drogą elektroniczną (Dz. U. z 2013 r., poz. 1422) jest usługa świadczona bez jednoczesnej obecności stron (na odległość), poprzez przekaz danych na indywidualne żądanie usługobiorcy, przesyłanej i otrzymywanej za pomocą urządzeń do elektronicznego przetwarzania.

<sup>5</sup> Wymagania w zakresie Web Content Accesibility Guideliness (WCAG 2.0) określone w załączniku nr 4 do rozporządzenia KRI.

NIK zauważa, że dla zapewnienia zwiększenia poziomu interoperacyjności objętych badaniem systemów informatycznych Urzędu zasadnym jest podjęcie działań mających na celu:

- wprowadzenie zasady rozpatrywania spraw (wpływających i wewnętrznych) w systemie elektronicznym, jako podstawowego sposobu ich załatwiania, w miejsce stosowanej aktualnie formy papierowej,
- wykorzystywanie w szerszym zakresie danych z rejestrów centralnych, takich jak np. CEIDG<sup>6</sup>, PESEL na potrzeby własnych systemów informatycznych i usług elektronicznych.

### **III. Opis ustalonego stanu faktycznego**

Rozporządzenie KRI wykonuje upoważnienie ustawowe zawarte w art. 18 ustawy z dnia 17 lutego 2005 r. o informatyzacji działalności podmiotów realizujących zadania publiczne<sup>7</sup> w zakresie:

- minimalnych wymagań dla systemów informatycznych,
- minimalnych wymagań dla rejestrów publicznych i wymiany informacji w postaci elektronicznej,
- Krajowych Ram Interoperacyjności<sup>8</sup>.

Rozporządzenie KRI określa podstawowe wymogi zapewnienia interoperacyjności w zakresie wymiany danych zawartych w rejestrach publicznych i systemach informatycznych, a także wymogi w zakresie zarządzania bezpieczeństwem informacji. Przepisy rozporządzenia KRI zobowiązują podmioty realizujące zadania publiczne m.in. do opracowania, ustanowienia, wdrożenia, monitorowania i dokonywania przeglądów systemu zarządzania bezpieczeństwem informacji. Zgodnie z § 22 rozporządzenia KRI systemy teleinformatyczne podmiotów realizujących zadania publiczne funkcjonujące w dniu wejścia w życie ww. rozporządzenia, tj. od 31 maja 2012 r. należy dostosować w powyższym zakresie, nie później niż w dniu ich pierwszej istotnej modernizacji. Systemy informatyczne nabywane po tej dacie obligatoryjnie podlegają wymogom rozporządzenia KRI.

Rozporządzenie KRI nałożyło także obowiązek dostosowania stron internetowych instytucji publicznych do międzynarodowych standardów, których wdrożenie przeciwdziała wykluczeniu cyfrowemu osób niepełnosprawnych. Zgodnie z § 19 tego rozporządzenia dostosowanie serwisów internetowych podmiotów publicznych do potrzeb osób niepełnosprawnych powinno nastąpić poprzez wdrożenie wymagań standardu WCAG 2.0. zawartych w załączniku nr 4.

---

<sup>6</sup> Centralna Ewidencja i Informacja o Działalności Gospodarczej.

<sup>7</sup> Dz. U. z 2013 r., poz. 235.

<sup>8</sup> KRI stanowią zbiór zasad i sposobów postępowania podmiotów dotyczących zapewnienia systemom informatycznym interoperacyjności działania rozumianej jako zdolność tych systemów oraz wspieranych przez nie procesów do wymiany danych oraz do dzielenia się informacjami i wiedzą.

# 1. Współpraca posiadanych systemów informatycznych oraz ich dostosowanie do wymiany danych z systemami/rejestrami innych podmiotów administracji publicznej

## 1.1. Obieg dokumentów w Urzędzie

Opis stanu faktycznego

W *Strategii Rozwoju Bielska-Białej do 2020 roku* z czerwca 2012 r. zostały ujęte m.in. zagadnienia dotyczące dostosowania jednostki do elektronicznego świadczenia usług publicznych. W *Strategii* określono, że Bielsko-Biała posiada stosunkowo dobrą dostępność do sieci teleinformatycznych, a także, że Urząd uczestniczy w projekcie SEKAP<sup>9</sup> - strategicznym dla rozwoju regionu śląskiego projekcie gmin i powiatów Województwa Śląskiego umożliwiającym realizację usług publicznych drogą elektroniczną. Ponadto w *Strategii* w ramach jednego z kierunków rozwoju dla celu strategicznego: *Bielsko-Biała miastem rozbudowanej infrastruktury informacyjno-komunikacyjnej zapewniającej aktywne uczestnictwo w procesach globalizacji* wskazano rozwój usług publicznych poprzez *Wdrażanie systemów teleinformatycznych w procesie świadczenia usług publicznych*.

[dowód: akta kontroli str. 106]

W Urzędzie, w celu zarządzania biegiem dokumentów i dokumentacją stosowane są procedury i zasady postępowania z dokumentami wpływającymi do Urzędu zawarte w Instrukcji Kancelaryjnej stanowiącej załącznik do rozporządzenia Prezesa Rady Ministrów z dnia 18 stycznia 2011 r. w sprawie instrukcji kancelaryjnej, jednolitych rzeczowych wykazów akt oraz instrukcji w sprawie organizacji i zakresu działania archiwów zakładowych<sup>10</sup>. Przyjęto, stosownie do § 1 pkt 3 Instrukcji Kancelaryjnej, tradycyjny (papierowy) system wykonywania czynności kancelaryjnych, jako podstawowy sposób dokumentowania przebiegu załatwiania i rozstrzygania spraw w Urzędzie<sup>11</sup>.

Rejestracja i dystrybucja korespondencji, w tym wpływającej do Prezydenta Miasta, zastępców i Sekretarza Miasta oraz obsługa interesantów odbywa się w oparciu o opisane w ZSZ procesy i wyodrębnione w ich ramach procedury. W zakresie niniejszej kontroli istotne były przede wszystkim dwa procesy, tj. *Obsługa pracy Prezydenta Miasta, Zastępców Prezydenta i Sekretarza Miasta* (proces ON-3) oraz *Obsługa interesantów* (proces ON-4). Dla tych procesów określono stosowane procedury m.in. w zakresie rejestracji i obiegu dokumentów oraz obsługi kancelaryjnej Urzędu.

Zgodnie z § 6 ust. 1 regulaminu organizacyjnego<sup>12</sup> Kierownictwo Urzędu i pracownicy realizują procesy w oparciu o wymagania zawarte w przepisach prawnych oraz opracowane i przyjęte do stosowania wewnętrzne standardy jakościowe dla wykonywanych zadań. Wdrożony w Urzędzie ZSZ jest zgodny m.in. z normami: PN-ISO/IEC 27001:2007 *Technika informatyczna. Techniki bezpieczeństwa. Systemy zarządzania bezpieczeństwem informacji* oraz PN-ISO/IEC 17799:2007 *Technika informatyczna. Techniki bezpieczeństwa. Praktyczne zasady zarządzania bezpieczeństwem informacji*.

[dowód: akta kontroli str. 5-6, 14-16, 114-117, 418-422]

<sup>9</sup> System Elektronicznej Komunikacji Administracji Publicznej.

<sup>10</sup> Dz. U. z 2011 r. Nr 14, poz. 67 ze zm.

<sup>11</sup> Wprowadzony zarządzeniem Nr ON.120.22.2012.ON Prezydenta Miasta Bielska-Białej z 21 marca 2012 r. w sprawie określenia systemu wykonywania czynności kancelaryjnych, obiegu dokumentów, terminów załatwiania spraw oraz przyjmowania i rozpatrywania skarg i wniosków w Urzędzie Miejskim w Bielsku-Białej.

<sup>12</sup> Załącznik nr 1 do zarządzenia nr ON-0152/88/10/ON Prezydenta Miasta Bielska-Białej z dnia 28 września 2010 r. ze zm. (tekst jednolity ogłoszony został obwieszczeniem Nr ON.120.42.1.2013.ON Prezydenta Miasta Bielska-Białej z dnia 3 czerwca 2013 r.).

Wdrożenie ZSZ, zgodnego m.in. z ww. normami stanowiło spełnienie wymagań określonych w § 5 ust. 4 pkt 2 rozporządzenia KRI, który stanowi, że interoperacyjność na poziomie technologicznym osiągnana jest m.in. poprzez stosowanie regulacji uwzględniających postanowienia odpowiednich Polskich Norm. Działanie Urzędu w oparciu o wyżej wymienione normy (szczegółowy opis na str. 11-15) jest zgodne z § 15 ust. 1 rozporządzenia KRI, który stanowi m.in., że systemy informatyczne używane przez podmioty publiczne eksploatuje się przy zastosowaniu norm oraz uznanych w obrocie profesjonalnym standardów i metodyk. Sposób obsługi mieszkańców z wykorzystaniem systemów informatycznych jest zatem uporządkowany organizacyjnie.

[dowód: akta kontroli str. 179-220]

W Urzędzie, z uwagi na przyjęty tradycyjny (papierowy) system wykonywania czynności kancelaryjnych, jako podstawowy sposób dokumentowania przebiegu spraw nie wyodrębniono elektronicznego sposobu komunikowania się „bez papieru”, dlatego też nie została opracowana i wdrożona procedura zarządzania i obiegu dokumentami w systemie elektronicznym. W związku z tym dokumenty wpływające do Urzędu w postaci papierowej, częściowo przetwarzane są na postać elektroniczną, tj. wniosek interesanta jest skanowany, a następnie wprowadzany jako załącznik sprawy podczas rejestracji w systemie [...] <sup>13</sup> służącym do elektronicznego obiegu dokumentów w Urzędzie. Po zarejestrowaniu, w dalszej kolejności dokument nie jest procedowany jako dokument elektroniczny, lecz jako dokument papierowy.

[dowód: akta kontroli str. 5, 15-16, 106]

Uwagi dotyczące  
badanej działalności

Zdaniem NIK należałoby rozważyć wprowadzenie w nieodległej przyszłości systemu elektronicznego prowadzenia spraw, jako podstawowego systemu wykonywania czynności kancelaryjnych w Urzędzie, w miejsce aktualnie wykorzystywanego systemu tradycyjnego w postaci papierowej. W ocenie NIK w pierwszej kolejności należałoby wprowadzić tą zasadę dla korespondencji wytwarzanej wewnątrz jednostki. Wdrożenie jej mogłoby się przyczynić do przyspieszenia obiegu dokumentów i rozpatrywania spraw oraz do ograniczenia kosztów związanych z ich wytwarzaniem w postaci papierowej. Należy przy tym zwrócić uwagę, że na potrzebę stosowania elektronicznej formy prowadzenia korespondencji wewnętrznej wskazano w regulaminie organizacyjnym, w którym § 41 pkt 6 stanowi, że *W komunikacji wewnętrznej należy w pierwszej kolejności wykorzystywać drogę elektroniczną przekazywania informacji oraz dokumentów.*

## **1.2. Świadczenie i zarządzanie usługami elektronicznymi Urzędu**

1. Z przepisu § 3 ust. 1 pkt 1 lit. a rozporządzenia KRI wynika, że wymogi dotyczące Krajowych Ram Interoperacyjności mają zastosowanie do zapewnienia obywatelom i przedsiębiorcom dostępności usług świadczonych w postaci elektronicznej przez podmioty realizujące zadania publiczne.

Usługi elektroniczne Urzędu są świadczone za pomocą platformy SEKAP, do której dostęp jest możliwy pod adresem internetowym [www.sekap.pl](http://www.sekap.pl). Urząd na dzień 30 maja 2012 r. <sup>14</sup> świadczył 194 usługi elektroniczne dla interesantów, natomiast w czasie kontroli świadczył 200 usług elektronicznych.

[dowód: akta kontroli str. 5-14, 420]

<sup>13</sup> Anonimizacja na podstawie § 10 ust. 1 pkt 3 zarządzenia nr 23/2012 Prezesa Najwyższej Izby Kontroli z 21 czerwca 2012 r. w sprawie udostępniania informacji publicznych przez Najwyższą Izbę Kontroli zmienionego zarządzeniem nr 43 Prezesa Najwyższej Izby Kontroli z 25 września 2013 r.

<sup>14</sup> Przed wejściem w życie rozporządzenia KRI.

Szczegółowym badaniem w zakresie zgodności świadczonej usługi z jej opisem zamieszczonym na stronie internetowej platformy SEKAP objęto pięć usług elektronicznych świadczonych przez Urząd, tj.:

- zgłoszenie problemu w zakresie technicznej obsługi e-usługi,
- wydanie zaświadczenia z akt dotyczących dowodu osobistego,
- przeniesienie decyzji o pozwoleniu na budowę,
- wydanie decyzji o pozwoleniu na rozbiórkę,
- wpis do rejestru działalności regulowanej w zakresie odbierania odpadów komunalnych od właścicieli nieruchomości.

Kontrola wykazała, że opisy wszystkich objętych badaniem usług były zgodne z faktycznie świadczonymi, a ostatnia aktualizacja opisów i usług nastąpiła w dniu 21 listopada 2013 r., co było w ocenie NIK działaniem rzetelnym.

[dowód: akta kontroli str. 379-385]

2. Ustalono, że w procesie zarządzania usługami elektronicznymi Urząd 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 (usługi sieciowe) oraz opisano sposób korzystania z tych funkcji.

Zarządzanie usługami realizowanymi przez badane systemy teleinformatyczne (szczegółowy opis na str. 11-15) odbywa się w oparciu o udokumentowane w ZSZ procedury niezbędne dla określenia zakresu i sposobu świadczenia usług elektronicznych z wykorzystaniem systemów informatycznych. Urząd nie posiadał jednak spisanych wewnętrznych kart wymagań dla usług elektronicznych, co uniemożliwiało ustalenie wewnątrz Urzędu właściciela usługi<sup>15</sup>, tj. konkretnej osoby pełniącej określoną rolę - odpowiedzialnej za realizację poszczególnych elementów świadczonej usługi. Ustalenie takiej osoby wymagało wykorzystywania wielu źródeł informacji<sup>16</sup>. Zapewnienie funkcjonowania usług elektronicznych wymaga realizacji w Urzędzie szeregu usług informatycznych np. transmisji danych, sporządzania kopii danych, zapewnienia bezpieczeństwa pracy systemów informatycznych. Dla części usług informatycznych wspierających realizację usług elektronicznych zawarte zostały umowy serwisowe z ustalonym poziomem SLA<sup>17</sup>, na podstawie których można ustalić maksymalny czas niedostępności poszczególnych elementów technicznych usługi oraz sposób zgłaszania awarii. Nie określono jednak punktu zgłaszania awarii przez użytkowników systemów informatycznych Urzędu, np. Service Desk pozwalającego w sposób scentralizowany oraz jednorodny zarządzać otrzymanymi zgłoszeniami.

[dowód: akta kontroli str. 330-372, 379]

Uwagi dotyczące  
badanej działalności

Zarządzanie usługami realizowanymi przez badane systemy teleinformatyczne odbywa się w oparciu o udokumentowane w ZSZ procedury, stanowiące podstawę modelu usługowego. W ocenie NIK, zapewnienie sprawnego świadczenia usług elektronicznych wymaga jednak podjęcia dalszych działań dla jego usprawnienia. W tym celu konieczne jest opracowanie odrębnych wymagań dla każdej ze świadczonych usług elektronicznych zawierających co najmniej imiennie wskazanego jej właściciela, dopuszczalnych okresów niedostępności usługi, określenie zakładanego rozłożonego w czasie zapotrzebowania klientów Urzędu na usługę (obciążenie). Zdaniem NIK, wymagać to będzie również spisania

<sup>15</sup> Wskazanie odpowiedzialnego pracownika.

<sup>16</sup> Regulamin organizacyjny, zarządzenia Prezydenta, strona internetowa Urzędu.

<sup>17</sup> Ang. Service Level Agreement - umowa utrzymania i systematycznego poprawiania ustalonego między klientem a usługodawcą poziomu jakości usług.

wewnętrznych porozumień (OLA<sup>18</sup>), ponieważ za utrzymanie poszczególnych elementów usług odpowiedzialne są różne komórki organizacyjne Urzędu.

### 1.3. Współpraca badanych systemów informatycznych z innymi systemami

1. Zakres współpracy systemów informatycznych wewnątrz Urzędu zbadano w oparciu o dobór celowy czterech systemów, zakupionych po 31 maja 2012 r.<sup>19</sup> tj.:

- system informatyczny wspierający działalność Urzędu w zakresie zarządzania odpadami komunalnym - Odpady komunalne firmy [...] <sup>20</sup>,
- system informatyczny wykorzystywany głównie do telefonicznego wsparcia obsługi klienta oraz integracji central telefonicznych jednostek Urzędu - Zintegrowana Platforma Obsługi Interesanta firmy [...] <sup>21</sup> (dalej ZPOI),
- system informatyczny wspierający sprawy z zakresu działania Wydziału Urbanistyki i Architektury - [...] <sup>22</sup>,
- system informatyczny służący do elektronicznego obiegu dokumentów w całym Urzędzie - [...] <sup>23</sup>.

[dowód: akta kontroli str. 107]

W wyniku badania ustalono, że:

- **System Odpady komunalne** nie wymienia danych z innymi systemami wewnątrz Urzędu. Umożliwia tylko zaimportowanie danych w zakresie płatności z pliku wygenerowanego w innym systemie poprzez operacje wykonywane przez użytkownika systemu. Współpraca z innymi systemami obejmuje jeden element na poziomie *jednostronnej komunikacji* <sup>24</sup>, a zatem system można sklasyfikować jako *informacyjny*. Oznacza to, że pracownicy Urzędu wiedzą, że dany system gromadzi dane i że w razie potrzeby mogą z nich skorzystać, znają też sposób dostępu do danych zgromadzonych w systemie.

[dowód: akta kontroli str. 101-104, 378, 395]

- **System ZPOI** ma wiele funkcjonalności telefonicznych IVR <sup>25</sup> umożliwiających interaktywną obsługę osoby dzwoniącej. System umożliwia automatyczne połączenie z pracownikiem prowadzącym sprawę. Dzwoniący za pomocą aparatu z wybieraniem tonowym lub za pomocą głosu po wysłuchaniu nagranych wcześniej komunikatów ma możliwość wyboru dostępnych informacji poprzez wielopoziomowe

---

<sup>18</sup> Ang. Operational Level Agreement - Umowa (porozumienie) o gwarantowanym poziomie wsparcia.

<sup>19</sup> Data wejścia w życie rozporządzenia KRI.

<sup>20</sup> Anonimizacja na podstawie § 10 ust. 1 pkt 3 zarządzenia nr 23/2012 Prezesa Najwyższej Izby Kontroli z 21 czerwca 2012 r. w sprawie udostępniania informacji publicznych przez Najwyższą Izbę Kontroli zmienionego zarządzeniem nr 43 Prezesa Najwyższej Izby Kontroli z 25 września 2013 r.

<sup>21</sup> Anonimizacja na podstawie § 10 ust. 1 pkt 3 zarządzenia nr 23/2012 Prezesa Najwyższej Izby Kontroli z 21 czerwca 2012 r. w sprawie udostępniania informacji publicznych przez Najwyższą Izbę Kontroli zmienionego zarządzeniem nr 43 Prezesa Najwyższej Izby Kontroli z 25 września 2013 r.

<sup>22</sup> Anonimizacja na podstawie § 10 ust. 1 pkt 3 zarządzenia nr 23/2012 Prezesa Najwyższej Izby Kontroli z 21 czerwca 2012 r. w sprawie udostępniania informacji publicznych przez Najwyższą Izbę Kontroli zmienionego zarządzeniem nr 43 Prezesa Najwyższej Izby Kontroli z 25 września 2013 r.

<sup>23</sup> Anonimizacja na podstawie § 10 ust. 1 pkt 3 zarządzenia nr 23/2012 Prezesa Najwyższej Izby Kontroli z 21 czerwca 2012 r. w sprawie udostępniania informacji publicznych przez Najwyższą Izbę Kontroli zmienionego zarządzeniem nr 43 Prezesa Najwyższej Izby Kontroli z 25 września 2013 r.

<sup>24</sup> Dane z jednego systemu informatycznego są przekazywane do innego systemu z udziałem użytkownika systemu - brak automatyzacji działania systemu.

<sup>25</sup> IVR (ang. Interactive Voice Response).



menu. System umożliwia również automatyczne sprawdzanie statusu realizacji sprawy oraz współpracuje z systemem [...]<sup>26</sup>, a zatem można go sklasyfikować jako *dwustronna komunikacja*<sup>27</sup>.

[dowód: akta kontroli str. 17, 24,394-395]

• **System [...] <sup>28</sup>** komunikuje się w sposób *transakcyjny* z systemem [...] <sup>29</sup>, tj. dane pomiędzy systemami informatycznymi przesyłane i odbierane są w sposób automatyczny bez dodatkowych operacji wykonywanych przez użytkownika. Komunikacja odbywa się w ten sposób, że system [...] <sup>30</sup> automatycznie przesyła do systemu [...] <sup>31</sup> m.in. numer sprawy, dane adresowe, opis sprawy oraz dokumenty w wersji elektronicznej, zaś ten ma możliwość procedowania sprawy i przesłania do systemu [...] <sup>32</sup> informacji o stanie załatwiania sprawy. Dane pomiędzy systemami są natychmiast automatycznie synchronizowane.

[dowód: akta kontroli str. 393, 395]

• **System [...] <sup>33</sup>** poza wyżej opisaną współpracą z systemami ZPOI i [...] <sup>34</sup> komunikuje się także z systemem SEKAP i platformą ePUAP<sup>35</sup>. Ponadto, jest zintegrowany z systemem informatycznym Urzędu zawierającym dane o mieszkańcach. Integracja przebiega w następujący sposób: użytkownik systemu wprowadzając dane interesanta poprzez wpisanie numeru PESEL, automatycznie uzyskuje odpowiedź w zakresie jego danych adresowych. Poziom współpracy

---

<sup>26</sup> Anonimizacja na podstawie § 10 ust. 1 pkt 3 zarządzenia nr 23/2012 Prezesa Najwyższej Izby Kontroli z 21 czerwca 2012 r. w sprawie udostępniania informacji publicznych przez Najwyższą Izbę Kontroli zmienionego zarządzeniem nr 43 Prezesa Najwyższej Izby Kontroli z 25 września 2013 r.

<sup>27</sup> Dane z jednego systemu informatycznego przekazywane są do innego systemu, wymagane jest zatwierdzenie wyników przez operatora, odpowiedź z systemu jest przekazywana analogicznie.

<sup>28</sup> Anonimizacja na podstawie § 10 ust. 1 pkt 3 zarządzenia nr 23/2012 Prezesa Najwyższej Izby Kontroli z 21 czerwca 2012 r. w sprawie udostępniania informacji publicznych przez Najwyższą Izbę Kontroli zmienionego zarządzeniem nr 43 Prezesa Najwyższej Izby Kontroli z 25 września 2013 r.

<sup>29</sup> Anonimizacja na podstawie § 10 ust. 1 pkt 3 zarządzenia nr 23/2012 Prezesa Najwyższej Izby Kontroli z 21 czerwca 2012 r. w sprawie udostępniania informacji publicznych przez Najwyższą Izbę Kontroli zmienionego zarządzeniem nr 43 Prezesa Najwyższej Izby Kontroli z 25 września 2013 r.

<sup>30</sup> Anonimizacja na podstawie § 10 ust. 1 pkt 3 zarządzenia nr 23/2012 Prezesa Najwyższej Izby Kontroli z 21 czerwca 2012 r. w sprawie udostępniania informacji publicznych przez Najwyższą Izbę Kontroli zmienionego zarządzeniem nr 43 Prezesa Najwyższej Izby Kontroli z 25 września 2013 r.

<sup>31</sup> Anonimizacja na podstawie § 10 ust. 1 pkt 3 zarządzenia nr 23/2012 Prezesa Najwyższej Izby Kontroli z 21 czerwca 2012 r. w sprawie udostępniania informacji publicznych przez Najwyższą Izbę Kontroli zmienionego zarządzeniem nr 43 Prezesa Najwyższej Izby Kontroli z 25 września 2013 r.

<sup>32</sup> Anonimizacja na podstawie § 10 ust. 1 pkt 3 zarządzenia nr 23/2012 Prezesa Najwyższej Izby Kontroli z 21 czerwca 2012 r. w sprawie udostępniania informacji publicznych przez Najwyższą Izbę Kontroli zmienionego zarządzeniem nr 43 Prezesa Najwyższej Izby Kontroli z 25 września 2013 r.

<sup>33</sup> Anonimizacja na podstawie § 10 ust. 1 pkt 3 zarządzenia nr 23/2012 Prezesa Najwyższej Izby Kontroli z 21 czerwca 2012 r. w sprawie udostępniania informacji publicznych przez Najwyższą Izbę Kontroli zmienionego zarządzeniem nr 43 Prezesa Najwyższej Izby Kontroli z 25 września 2013 r.

<sup>34</sup> Anonimizacja na podstawie § 10 ust. 1 pkt 3 zarządzenia nr 23/2012 Prezesa Najwyższej Izby Kontroli z 21 czerwca 2012 r. w sprawie udostępniania informacji publicznych przez Najwyższą Izbę Kontroli zmienionego zarządzeniem nr 43 Prezesa Najwyższej Izby Kontroli z 25 września 2013 r.

<sup>35</sup> Elektroniczna Platforma Usług Administracji Publicznej.

systemu [...] <sup>36</sup> z innymi systemami można określić jako *dwustronna komunikacja*. System ten poprzez elektroniczny formularz dostępny na stronie Urzędu, umożliwia także weryfikację przez interesanta statusu sprawy oraz osoby odpowiedzialnej za jej realizację (dane pobierane są z systemu [...] <sup>37</sup>). Weryfikacja następuje po wpisaniu przez klienta do formularza numeru sprawy otrzymanego przy złożeniu dokumentu do Urzędu.

[dowód: akta kontroli str. 17, 24, 377, 379-385, 393-395]

W ocenie NIK badane systemy informatyczne spełniają minimalne wymogi interoperacyjności w zakresie współpracy z innymi systemami Urzędu określone w § 5 ust. 3 pkt 3 rozporządzenia KRI <sup>38</sup>. Uwagi NIK dotyczą systemu Odpady Komunalne (szczegółowy opis str. 10).

2. W zakresie współpracy systemów informatycznych Urzędu z systemami zewnętrznymi ustalono, że zarządzenia i regulacje wewnętrzne nie zawierały procedur postępowania we współpracy z innymi jednostkami administracji publicznej określających komunikację elektroniczną „bez wykorzystania papieru”. Systemy informatyczne Urzędu nie posiadają bezpośrednich odwołań <sup>39</sup> do rejestrów centralnych jak np. CEIDG, PESEL, a korzystają jedynie z własnych zbiorów danych. Każdy system jest odrębny, a bazy danych tych systemów są zasilane indywidualnie. Stąd poziom organizacyjny współpracy systemów informatycznych Urzędu z systemami innych urzędów administracji publicznej, zdaniem NIK, należy sklasyfikować jako brak interoperacyjności, o której mowa w przywołanym wyżej § 5 ust. 3 pkt 3 rozporządzenia KRI.

[dowód: akta kontroli str. 418-421]

W okresie objętym badaniem (od 31 maja 2012 r. do 4 grudnia 2013 r.) do Urzędu wpłynęło 238 299 dokumentów, z czego 1 516 dokumentów/wniosek/podań zostało wniesionych przez obywateli, podmioty gospodarcze i inne urzędy w postaci elektronicznej, co stanowiło 0,6% ogółu dokumentów wpływających. Do Urzędu wpłynęło za pomocą systemu SEKAP 936 szt. dokumentów elektronicznych a za pośrednictwem platformy ePUAP 580 szt.

[dowód: akta kontroli str. 457]

Na podstawie losowo dobranej próby 30 dokumentów kontrolerzy NIK zbadali sposób procedowania w Urzędzie przy przetwarzaniu korespondencji elektronicznej. Spośród badanych dokumentów 16 złożyły podmioty gospodarcze, 10 inne urzędy, a cztery obywatele <sup>40</sup>. Analiza ww. dokumentów wykazała, że 14 z nich wymagało rozpatrzenia <sup>41</sup>, a załatwienie spraw wiązało się z wysłaniem siedmiu pism do innych urzędów, pięciu pism do obywateli, a dwóch do innych podmiotów. Siedem z tych

---

<sup>36</sup> Anonimizacja na podstawie § 10 ust. 1 pkt 3 zarządzenia nr 23/2012 Prezesa Najwyższej Izby Kontroli z 21 czerwca 2012 r. w sprawie udostępniania informacji publicznych przez Najwyższą Izbę Kontroli zmienionego zarządzeniem nr 43 Prezesa Najwyższej Izby Kontroli z 25 września 2013 r.

<sup>37</sup> Anonimizacja na podstawie § 10 ust. 1 pkt 3 zarządzenia nr 23/2012 Prezesa Najwyższej Izby Kontroli z 21 czerwca 2012 r. w sprawie udostępniania informacji publicznych przez Najwyższą Izbę Kontroli zmienionego zarządzeniem nr 43 Prezesa Najwyższej Izby Kontroli z 25 września 2013 r.

<sup>38</sup> Przepis stanowi, że interoperacyjność na poziomie semantycznym osiągnięta jest m.in. poprzez stosowanie w rejestrach prowadzonych przez podmioty publiczne odwołań do rejestrów zawierających dane referencyjne w zakresie niezbędnym do realizacji zadań.

<sup>39</sup> Nie pobierają danych z innych systemów informatycznych.

<sup>40</sup> Z 30 zbadanych dokumentów 25 złożono za pomocą wniosków elektronicznych a pięć z wykorzystaniem formularzy usług elektronicznych.

<sup>41</sup> Szesnaście wpływających pism elektronicznych miało charakter informacyjny, niewymagający udzielenia odpowiedzi.

pism zostało przesłanych w formie papierowej i tyle samo za pomocą środków komunikacji elektronicznej.

Wyniki kontroli wykazały jednak, że w okresie objętym badaniem w Urzędzie nie powstał żaden dokument wyłącznie w postaci elektronicznej. Praktyką było bowiem, że w przypadku dokumentów wychodzących z Urzędu w postaci elektronicznej tworzona była również wersja papierowa, pomimo że wybrani pracownicy Urzędu posiadali kwalifikowane podpisy elektroniczne.

[dowód: akta kontroli str. 418-453]

Z badań opinii klientów wykonanych przez Urząd w 2013 r. wynika, że 60,2% badanych wybiera tradycyjny sposób załatwienia sprawy, tj. osobiście w Urzędzie, wskazując, że sprawa, którą muszą załatwić wymaga osobistego kontaktu lub, że wolą osobiście odwiedzić Urząd. Spośród 27,9% osób, które wiedziały jakie sprawy można załatwić w Urzędzie przez Internet, tylko 6,5% załatwiło sprawę za pomocą środków komunikacji elektronicznej.

[dowód: akta kontroli str. 422]

Urząd nie świadczył usług sieciowych<sup>42</sup> w rozumieniu rozporządzenia KRI, w związku z tym nie był zobowiązany do przekazania opisu protokołów i struktur danych usługi sieciowej do repozytorium interoperacyjności, o którym mowa w § 8 pkt 3 rozporządzenia KRI.

[dowód: akta kontroli str. 5-7, 108, 377-385]

Uwagi dotyczące  
badanej działalności

1. W ocenie NIK funkcjonalność systemu Odpady komunalne w zakresie współpracy z innymi systemami informatycznym w Urzędzie powinna uwzględniać funkcję automatycznej wymiany (pobierania i dostarczania) danych z innymi systemami informatycznymi Urzędu (np. z systemem ewidencji ludności, czy finansowo-księgowym). Warto rozważyć uruchomienie formularza usługi elektronicznej, z którego dane będą bezpośrednio przekazywane do systemu obsługującego odpady komunalne. Mogłoby to spowodować wzrost zainteresowania mieszkańców miasta wykorzystaniem tej usługi do składania deklaracji o wysokości opłaty za gospodarowanie odpadami komunalnymi bez konieczności stawienia się w Urzędzie.

2. Zdaniem NIK Urząd w miarę możliwości winien dążyć do zwiększenia wykorzystywania danych z rejestrów centralnych (np. CEIDG, PESEL) przez własne systemy informatyczne i usługi elektroniczne. Pozwoliłoby to na większą automatyzację w zakresie wymiany danych i przyczyniłoby się do usprawnienia realizacji zadań Urzędu m.in. poprzez skrócenie czasu pozyskiwania niezbędnych danych, jak również do obniżenia kosztów korespondencji. W tym celu zasadnym jest opracowanie i wdrożenie procedur i praktyk w zakresie współpracy z systemami informatycznymi innych jednostek administracji publicznej.

Najwyższa Izba Kontroli ocenia pozytywnie w zbadanym zakresie działalność kontrolowanej jednostki w obszarze wdrażania wymogów rozporządzenia KRI dotyczących współpracy systemów informatycznych i ich dostosowania do wymiany danych z innymi systemami i podmiotami. W Urzędzie zapewniono współpracę pomiędzy wybranymi do kontroli systemami informatycznymi w sposób spełniający minimalne wymogi w zakresie interoperacyjności poprzez wzajemną komunikację

Ocena cząstkowa

<sup>42</sup> Usługa sieciowa – właściwość systemu teleinformatycznego polegająca na powtarzalnym wykonywaniu przez ten system z góry określonych funkcji po otrzymaniu, za pomocą sieci teleinformatycznej, danych uporządkowanych w określonej strukturze, np. w systemie Centralnej Ewidencji Działalności Gospodarczej zawarte są dane o podmiotach gospodarczych, a dzięki usłudze sieciowej na zapytanie innych systemów informatycznych system CEIDG może przesyłać innym systemom automatycznie informacje np. nt. daty rejestracji działalności gospodarczej.

systemów. Urząd posiada jednak wystarczające zasoby pozwalające, zdaniem NIK, zwiększyć zakres wykorzystania komunikacji elektronicznej wewnątrz i na zewnątrz jednostki. Urząd posiada bowiem zarówno środki techniczne (dostosowany do wymogów Instrukcji Kancelaryjnej system zarządzania dokumentami [...] <sup>43</sup>), jak i niezbędne regulacje wewnętrzne, w których określone zostały zasady współpracy międzywydziałowej przy załatwianiu spraw z wykorzystaniem funkcjonujących systemów informatycznych.

## **2. Stopień wdrożenia zarządzania bezpieczeństwem systemów informatycznych**

Opis stanu faktycznego

Zgodnie z § 20 ust. 2 rozporządzenia KRI, zarządzanie bezpieczeństwem informacji realizowane jest m.in. przez zapewnienie przez kierownictwo podmiotu publicznego warunków umożliwiających realizację i egzekwowanie m.in. następujących działań:

- zapewnienia aktualizacji regulacji wewnętrznych w zakresie dotyczącym zmieniającego się otoczenia (pkt 1),
- utrzymywania aktualności inwentaryzacji sprzętu i oprogramowania służącego do przetwarzania informacji obejmującej ich rodzaj i konfigurację (pkt 2),
- przeprowadzania okresowych analiz ryzyka utraty integralności, dostępności lub poufności informacji oraz podejmowania działań minimalizujących to ryzyko, stosownie do wyników przeprowadzonej analizy (pkt 3),
- podejmowania 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 (pkt 4),
- ustalenia zasad postępowania z informacjami, zapewniających minimalizację wystąpienia ryzyka kradzieży informacji i środków przetwarzania informacji, w tym urządzeń mobilnych (pkt 11),
- kontroli zgodności systemów teleinformatycznych z odpowiednimi normami i politykami bezpieczeństwa (pkt 12 lit. h),
- zapewnienia okresowego audytu wewnętrznego w zakresie bezpieczeństwa informacji, nie rzadziej niż raz na rok (pkt 14).

---

<sup>43</sup> Anonimizacja na podstawie § 10 ust. 1 pkt 3 zarządzenia nr 23/2012 Prezesa Najwyższej Izby Kontroli z 21 czerwca 2012 r. w sprawie udostępniania informacji publicznych przez Najwyższą Izbę Kontroli zmienionego zarządzeniem nr 43 Prezesa Najwyższej Izby Kontroli z 25 września 2013 r.

Zgodnie z § 15 rozporządzenia KRI:

- systemy teleinformatyczne używane przez podmioty realizujące zadania publiczne projektuje się, wdraża oraz eksploatuje z uwzględnieniem ich funkcjonalności, niezawodności, używalności, wydajności, przenoszalności i pielęgnowalności, przy zastosowaniu norm oraz uznanych w obrocie profesjonalnym standardów i metodyk (ust. 1),
- zarządzanie usługami realizowanymi przez systemy teleinformatyczne ma na celu dostarczanie tych usług na deklarowanym poziomie dostępności i odbywa się w oparciu o udokumentowane procedury (ust. 2),
- wymagania określone w ust. 1 i 2 uznaje się za spełnione, jeśli projektowanie, wdrażanie, eksploatowanie, monitorowanie, przeglądanie, utrzymanie i udoskonalanie zarządzania usługą podmiotu realizującego zadania publiczne odbywają się z uwzględnieniem Polskich Norm: PN-ISO/IEC 20000-1 i PN-ISO/IEC 20000-2 (ust. 3).

Zgodnie z § 20 ust. 1 rozporządzenia KRI podmiot realizujący zadania publiczne opracowuje i ustanawia, wdraża i eksploatuje, monitoruje i przegląda oraz utrzymuje i doskonali system zarządzania bezpieczeństwem informacji zapewniający poufność, dostępność i integralność informacji z uwzględnieniem takich atrybutów, jak autentyczność, rozliczalność, niezaprzeczalność i niezawodność.

Zgodnie z Załącznikiem nr 2 do rozporządzenia KRI system teleinformatyczny używany do realizacji zadań publicznych musi spełniać standardy zapewniające dostęp do zasobów informacji oraz formaty danych określone w załączniku.

Urząd posiadał opracowaną i wdrożoną do stosowania Politykę Bezpieczeństwa Informacji (dalej PBI), ustanowioną i zatwierdzoną przez Prezydenta Miasta, co jest zgodne z § 20 ust. 1 rozporządzenia KRI. Zmiany do PBI proponuje Pełnomocnik Prezydenta Miasta ds. Systemu Zarządzania. Stosownie do § 20 ust. 2 pkt 1 rozporządzenia KRI, w okresie objętym kontrolą, Urząd dokonał (dwukrotnie) przeglądu PBI w ramach oceny wdrożonego w Urzędzie Zintegrowanego Systemu Zarządzania. W wyniku dokonanych przeglądów treść PBI nie uległa zmianie.

[dowód: akta kontroli str. 17-19, 25-30, 135]

Kontrola wykazała, że inwentaryzacja<sup>44</sup> zasobów informatycznych Urzędu była realizowana przy wykorzystaniu programu Alloy Navigator. Kontrolerzy NIK przeprowadzili oględziny zapisów zawartych w ww. programie na podstawie losowo wybranych 10 komputerów oraz jednego urządzenia pełniące rolę centralną<sup>45</sup>. Wyniki oględzin wykazały, że program Alloy Navigator zawierał szczegółowe informacje o komputerach, brak było natomiast danych odnośnie urządzenia pełniącego rolę centralną.

[dowód: akta kontroli str. 121-134, 397]

Ponadto ustalono, że do inwentaryzacji zasobów informatycznych jednostki Urząd zakupił w dniu 15 listopada 2012 r. za kwotę 55 974 zł program e-Audyt. Na dzień 16 grudnia 2013 r. program ten nie był wykorzystywany jako narzędzie ewidencjonujące zasoby informatyczne Urzędu. Zastępca Prezydenta Miasta Pan Zbigniew Michniowski wyjaśnił, że *zasoby informacji zgromadzone w programie Alloy Navigator zawierają pełną dokumentację historyczną i ta informacja gromadzona przez wiele lat musi zostać przeniesiona do nowego środowiska bez*

<sup>44</sup> W rozumieniu stałego posiadania aktualnych informacji w zakresie posiadanego sprzętu informatycznego, oprogramowania, konfiguracji i miejsca użytkowania.

<sup>45</sup> Urządzenie wykorzystywane do zarządzania elektronicznym dostępem do pomieszczeń.

utrąty danych. Uruchomione zostały wybrane funkcje programu e-Audytor jak np.: skanowanie zasobów lub możliwości raportowania. Dodatkowo podał, iż program e-Audytor zostanie wdrożony do użytkowania do połowy 2014 r.

[dowód: akta kontroli str. 101-104]

Urząd w badanym okresie przeprowadził dwie analizy ryzyka bezpieczeństwa informacji, co było zgodne z § 20 ust. 2 pkt 3 rozporządzenia KRI. W ich wyniku Urząd nie stwierdził utraty poufności, dostępności oraz integralności informacji.

[dowód: akta kontroli str. 19-83]

Kontrolerzy NIK dokonali przeglądu uprawnień do systemów i zasobów informatycznych dla 15 losowo wybranych pracowników Urzędu. Stwierdzono, iż posiadali oni stosowne uprawnienia adekwatne do realizowanych zadań określonych w zakresach obowiązków, co było zgodne z § 20 ust. 2 pkt 4 rozporządzenia KRI.

[dowód: akta kontroli str. 373-376]

Nadawanie/modyfikowanie/odbieranie uprawnień w systemach informatycznych było realizowane w oparciu o funkcjonujące w Urzędzie procedury, zgodnie z § 20 ust. 2 pkt 4 i pkt 5 rozporządzenia KRI (pkt 5 stanowi, że kierownictwo podmiotu publicznego powinno podjąć działania w celu zapewnienia bezzwłocznej zmiany uprawnień w przypadku zmiany zadań osób przetwarzających informacje). O uprawnieniach pracowników w systemach informatycznych decydują kierownicy komórek organizacyjnych poprzez odpowiedni wpis w „Karcie użytkownika zasobów informatycznych”. Kontrolerzy NIK dokonali sprawdzenia zablokowania dostępu do systemów informatycznych dla 10 byłych pracowników, którzy jako ostatnio zakończyli pracę w Urzędzie. Badaniem objęto dostęp do systemu sieciowego Microsoft Windows, systemu poczty elektronicznej oraz systemu elektronicznego obiegu dokumentów [...]<sup>46</sup>. Stwierdzono, iż wszyscy wskazani pracownicy nie mieli dostępu do systemu sieciowego Microsoft Windows oraz do systemu elektronicznego obiegu dokumentów [...]<sup>47</sup>. Przełożeni sporządzili stosowne wnioski o zablokowanie dostępu do kont w systemach informatycznych. W przypadku systemu poczty elektronicznej w stosunku do jednego pracownika wniosku o odebranie uprawnień przełożony nie złożył i dostępu do konta nie zablokowano.

[dowód: akta kontroli str. 23, 283-288, 386-392]

W badanym okresie Urząd zapewnił szkolenia pracowników zaangażowanych w proces przetwarzania informacji, stosownie do § 20 ust. 2 pkt 6 rozporządzenia KRI. Zakres tematyczny szkoleń obejmował: zagrożenia bezpieczeństwa informacji, skutki naruszenia bezpieczeństwa informacji, odpowiedzialność prawną.

[dowód: akta kontroli str. 17-22, 84]

W Urzędzie ustanowiono podstawowe zasady w zakresie bezpiecznej pracy użytkowników przy wykorzystaniu komputerów przenośnych<sup>48</sup>, zgodnie z § 20 ust. 2

---

<sup>46</sup> Anonimizacja na podstawie § 10 ust. 1 pkt 3 zarządzenia nr 23/2012 Prezesa Najwyższej Izby Kontroli z 21 czerwca 2012 r. w sprawie udostępniania informacji publicznych przez Najwyższą Izbę Kontroli zmienionego zarządzeniem nr 43 Prezesa Najwyższej Izby Kontroli z 25 września 2013 r.

<sup>47</sup> Anonimizacja na podstawie § 10 ust. 1 pkt 3 zarządzenia nr 23/2012 Prezesa Najwyższej Izby Kontroli z 21 czerwca 2012 r. w sprawie udostępniania informacji publicznych przez Najwyższą Izbę Kontroli zmienionego zarządzeniem nr 43 Prezesa Najwyższej Izby Kontroli z 25 września 2013 r.

<sup>48</sup> Instrukcja z dnia 20 września 2011 r. *Zasady bezpiecznego korzystania z systemów informatycznych przez użytkowników.*

pkt 8 rozporządzenia KRI. W myśl tych zasad pracownik przyjmuje na siebie odpowiedzialność za sprzęt komputerowy i zapisane na nim informacje. Komputery przenośne na etapie instalacji są przygotowywane tak przez pracowników Wydziału Informatyki, aby zabezpieczyć je przed zagrożeniami zewnętrznymi. Korzystanie z obcych sieci bezprzewodowych jest dopuszczalne po uzyskaniu zgody Naczelnika Wydziału Informatyki. Praca zdalna, telepraca, praca na odległość rozumiana jako możliwość uruchamiania programów wewnątrz sieci lokalnej Urzędu z dowolnego punktu poza urzędem nie była dopuszczona. Zgodnie z instrukcją *użytkownik komputera przenośnego jest odpowiedzialny za uaktualnienie oprogramowania na nim zainstalowanego. W tym celu raz na kwartał dokonuje podpięcia do sieci LAN*<sup>49</sup> Urzędu.

[dowód: akta kontroli str. 85-88, 154-159]

Według wyjaśnień Zastępcy Naczelnika Wydziału Informatyki w Urzędzie komputery są serwisowane w ramach gwarancji dostawcy. W pojedynczych przypadkach zlecała jest ich naprawa do serwisu. Zgodnie z instrukcją INF 1/6/3 *Przekazanie sprzętu do i z eksploatacji, do i z naprawy* na czas przekazania komputera do serwisu zewnętrznego demontuje się nośnik z danymi, co jest działaniem zgodnym z wymaganiem określonym w punkcie 10.7 Polskiej Normy ISO/IEC 17799:2007. Wskazano w nim, że w celu ochrony nośników komputerowych przed ich nieautoryzowanym ujawnieniem, modyfikacją, usunięciem lub zniszczeniem należy wdrożyć odpowiednie procedury eksploatacyjne.

[dowód: akta kontroli str. 133-134, 292-294, 416-417]

W Urzędzie stosownie do § 20 ust. 2 pkt 13 rozporządzenia KRI, wprowadzono procedurę PSZ-4/2 *Postępowanie z incydentem* nakazującą pracownikom niezwłoczne zgłaszanie incydentów naruszenia bezpieczeństwa informacji w sposób umożliwiający podjęcie działań korygujących.

[dowód: akta kontroli str. 142-144]

W okresie objętym kontrolą Urząd przeprowadził łącznie 23 audyty (dziewięć w 2012 r i 14 w 2013 r.) obejmujące proces *System Zarządzania Bezpieczeństwem Informacji* funkcjonujący w ramach ZSZ, co było zgodne z § 20 ust. 2 pkt 14 rozporządzenia KRI. Sformułowane w ramach przeprowadzonych audytów postrzeżenia/rekomendacje zostały zrealizowane.

[dowód: akta kontroli str. 398-400]

W Urzędzie wprowadzono instrukcję INF/4/2 *Tworzenie i przechowywanie kopii bezpieczeństwa danych*, w której określono zasady sporządzania i testowania kopii zapasowych danych i oprogramowania aplikacyjnego. Kopie zapasowe badanych systemów informatycznych były tworzone raz dziennie i zapisywane w określonych katalogach sieciowych. Testowanie prawidłowości sporządzenia wykonanych kopii zapasowych następowało co najmniej raz w miesiącu. Dodatkowo na bieżąco była weryfikowana prawidłowość tworzenia plików kopii zapasowych. Urząd posiada także zapasowy ośrodek danych. Dane w obydwu serwerowniach były synchronizowane natychmiastowo. Kopie zapasowe były przechowywane w serwerowni, a pomieszczenie było właściwie zabezpieczone. Stan taki spełniał wymogi określone w § 20 ust. 2 pkt 12 lit. b rozporządzenia KRI, dzięki czemu minimalizowano ryzyko utraty informacji w wyniku awarii.

[dowód: akta kontroli str. 247-255, 408-415]

---

<sup>49</sup> Ang. Local Area Network – Lokalna sieć komputerowa.

Dla prawidłowego funkcjonowania systemów informatycznych [...] <sup>50</sup>, ZPOI, „Odpady komunalne” w umowach zawartych z dostawcami lub producentami zapewniono serwis gwarancyjny związany z ich utrzymaniem. W przypadku systemu [...] <sup>51</sup> po zakończeniu okresu gwarancyjnego nie podpisano z dostawcą umowy serwisowej gwarantującej właściwy poziom obsługi oprogramowania (SLA). Jak wyjaśnił Zastępca Prezydenta Miasta Pana Zbigniew Michniowski z dostawcą systemu [...] <sup>52</sup> umowa nie została zawarta, ponieważ wykonawca chciał w niej zawrzeć klauzulę rozliczania usług, zgodnie z którą płatność następowałaby na podstawie ilości godzin roboczych świadczonej usługi określanych po jej wykonaniu. Wskazał również, że zmiany w oprogramowaniu są realizowane dla każdego przypadku na podstawie odrębnego zlecenia.

[dowód: akta kontroli str. 85-100]

Badane systemy informatyczne udostępniały dane w następujących formatach:

- System [...] <sup>53</sup>: generuje pliki w formatach PDF, XML, CSV, ODT,
- System „Odpady komunalne”: generuje pliki w formatach ODT, CSV,
- System [...] <sup>54</sup>: generuje pliki w formacie RTF,

tj. zgodnie z wymogami określonymi w § 18 ust. 1 rozporządzenia KRI.

System ZPOI ze względu na swoją specyfikę (realizuje wyłącznie funkcje telefoniczne) nie udostępnia eksportu danych.

Dodatkowo systemy [...] <sup>55</sup> umożliwiają wymianę danych z systemami informatycznymi w sposób zautomatyzowany z wykorzystaniem formatu danych XML.

[dowód: akta kontroli str. 395-396]

Ustalone  
nieprawidłowości

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

1. Stwierdzono, iż w oprogramowaniu Alloy Navigator inwentaryzującym infrastrukturę informatyczną Urzędu nie było ujęte urządzenie komputerowe wykorzystywane do zarządzania elektronicznym dostępem do pomieszczeń

<sup>50</sup> Anonimizacja na podstawie § 10 ust. 1 pkt 3 zarządzenia nr 23/2012 Prezesa Najwyższej Izby Kontroli z 21 czerwca 2012 r. w sprawie udostępniania informacji publicznych przez Najwyższą Izbę Kontroli zmienionego zarządzeniem nr 43 Prezesa Najwyższej Izby Kontroli z 25 września 2013 r.

<sup>51</sup> Anonimizacja na podstawie § 10 ust. 1 pkt 3 zarządzenia nr 23/2012 Prezesa Najwyższej Izby Kontroli z 21 czerwca 2012 r. w sprawie udostępniania informacji publicznych przez Najwyższą Izbę Kontroli zmienionego zarządzeniem nr 43 Prezesa Najwyższej Izby Kontroli z 25 września 2013 r.

<sup>52</sup> Anonimizacja na podstawie § 10 ust. 1 pkt 3 zarządzenia nr 23/2012 Prezesa Najwyższej Izby Kontroli z 21 czerwca 2012 r. w sprawie udostępniania informacji publicznych przez Najwyższą Izbę Kontroli zmienionego zarządzeniem nr 43 Prezesa Najwyższej Izby Kontroli z 25 września 2013 r.

<sup>53</sup> Anonimizacja na podstawie § 10 ust. 1 pkt 3 zarządzenia nr 23/2012 Prezesa Najwyższej Izby Kontroli z 21 czerwca 2012 r. w sprawie udostępniania informacji publicznych przez Najwyższą Izbę Kontroli zmienionego zarządzeniem nr 43 Prezesa Najwyższej Izby Kontroli z 25 września 2013 r.

<sup>54</sup> Anonimizacja na podstawie § 10 ust. 1 pkt 3 zarządzenia nr 23/2012 Prezesa Najwyższej Izby Kontroli z 21 czerwca 2012 r. w sprawie udostępniania informacji publicznych przez Najwyższą Izbę Kontroli zmienionego zarządzeniem nr 43 Prezesa Najwyższej Izby Kontroli z 25 września 2013 r.

<sup>55</sup> Anonimizacja na podstawie § 10 ust. 1 pkt 3 zarządzenia nr 23/2012 Prezesa Najwyższej Izby Kontroli z 21 czerwca 2012 r. w sprawie udostępniania informacji publicznych przez Najwyższą Izbę Kontroli zmienionego zarządzeniem nr 43 Prezesa Najwyższej Izby Kontroli z 25 września 2013 r.



Wydziału Informatyki (nr K/997), czym naruszono przepis § 20 ust. 2 pkt 2 rozporządzenia KRI, w myśl którego Urząd jest zobowiązany do utrzymywania aktualności inwentaryzacji sprzętu i oprogramowania służącego do przetwarzania informacji obejmującego ich rodzaj i konfigurację. Jak wyjaśnił Zastępca Prezydenta Pan Zbigniew Michniowski powyższe spowodowane było faktem, iż wskazane urządzenie stanowi system integralny niepołączony z siecią Active Directory. W trakcie kontroli urządzenie zostało dodane do spisu urządzeń komputerowych prowadzonych w programie Alloy Navigator.

[dowód: akta kontroli str. 397, 101-103]

2. W przypadku jednego z dziesięciu byłych pracowników Urzędu konto użytkownika systemu poczty elektronicznej do dnia 6 grudnia 2013 r. nie zostało zablokowane, pomimo iż nie był on pracownikiem Urzędu od dnia 24 sierpnia 2013 r. Było to niezgodne z § 20 ust. 2 pkt 5 rozporządzenia KRI, w myśl którego zarządzanie bezpieczeństwem informacji realizowane jest w szczególności poprzez bezzwłoczną zmianę uprawnień w przypadku zmiany zadań pracowników. Stwierdzonej nieprawidłowości nie tłumaczą podane w wyjaśnieniach Zastępcy Prezydenta Miasta Pana Zbigniewa Michniowskiego argumenty, że sytuacja ta wystąpiła ponieważ pracownik ten był zatrudniony w „Inkubatorze przedsiębiorczości” na zewnątrz sieci LAN Urzędu oraz że miał on dopuszczenie jedynie do funkcji, które mógł wykorzystywać w tej lokalizacji. Nieprawidłowość ta została usunięta w trakcie kontroli NIK.

[dowód: akta kontroli str. 386-389, 85-88, 105]

Uwagi dotyczące  
badanej działalności

1. Kontrola wykazała, że zbyt wolno przebiega wdrażanie do eksploatacji systemu e-Audytor, który pomimo upływu ponad roku od dnia zakupu nie został w pełni wdrożony. NIK zauważa przy tym, że system ten, jako nowocześniejszy od dotychczas użytkowanego Alloy Navigator usprawniłby proces inwentaryzacji zasobów informatycznych Urzędu.

2. Zdaniem NIK, obowiązek podłączenia przez pracowników komputera przenośnego do lokalnej sieci komputerowej Urzędu raz na kwartał nie spełnia swojej funkcji. Należy wskazać, że w Urzędzie funkcjonuje centralne zarządzanie zasobami informatycznymi przy wykorzystaniu usługi centralnego katalogu Active Directory. Zarządzanie to opiera się na przesyłaniu szeregu ustawień jakie mają być wprowadzone na urządzeniu mobilnym, co wymaga podpięcia urządzenia do sieci lokalnej (LAN). Obowiązek aby następowało to w okresach kwartalnych, w ocenie NIK, powoduje, że przez okres nawet ponad dwóch miesięcy użytkownik może pracować na nieaktualnych ustawieniach systemu operacyjnego, a ponadto może skutkować to zmniejszeniem bezpieczeństwa informatycznego. W związku z tym Urząd powinien wprowadzić znacznie krótszy, przynajmniej miesięczny czas w jakim pracownicy są zobowiązani podłączyć posiadany komputer przenośny do sieci lokalnej. Zdaniem NIK, zasadnym byłoby aby następowało to w każdym dniu obecności pracownika w Urzędzie.

Ocena częściowa

Najwyższa Izba Kontroli ocenia pozytywnie działalność kontrolowanej jednostki w zakresie stopnia wdrożenia zarządzania systemem bezpieczeństwa informacji w badanym okresie. Stwierdzone nieprawidłowości nie miały istotnego wpływu na zarządzanie bezpieczeństwem informacji w systemach informatycznych Urzędu i nie spowodowały obniżenia oceny.

### 3. Zapewnienie dostępności informacji zawartych na stronach internetowych Urzędu dla osób niepełnosprawnych

Opis stanu faktycznego

W toku kontroli dokonano weryfikacji zgodności strony internetowej Urzędu Miejskiego w Bielsku-Białej<sup>56</sup> oraz strony BIP Urzędu<sup>57</sup> ze standardem WCAG 2.0. W jej wyniku ustalono, iż strona internetowa Urzędu nie zawiera żadnych błędów. Na stronie BIP Urzędu wystąpił jeden błąd stwierdzony przy badaniu z wykorzystaniem narzędzia dostępnego na stronie <http://validator.w3.org> oraz dwa błędy stwierdzone z wykorzystaniem narzędzia dostępnego na stronie <http://jigsaw.w3.org/css-validator>. Wskazane wyżej błędy nie miały istotnego wpływu na prezentowanie treści dla osób niepełnosprawnych. W ocenie NIK strona www Urzędu oraz BIP spełniają wymagania sformułowane w § 19 rozporządzenia KRI dotyczące dostosowania systemów prezentujących treści do wymagań WCAG 2.0 w zakresie Zasady 4 – Kompatybilność. Zgodnie z § 22 rozporządzenia KRI systemy teleinformatyczne podmiotów realizujących zadania publiczne należy dostosować do wymagań określonych w § 19 rozporządzenia KRI, nie później niż w terminie 3 lat od dnia wejścia w życie rozporządzenia, czyli do dnia 30 maja 2015 r.

[dowód: akta kontroli str. 401-407]

Ustalone nieprawidłowości

W działalności kontrolowanej jednostki w przedstawionym wyżej zakresie nie stwierdzono nieprawidłowości.

Ocena cząstkowa

Najwyższa Izba Kontroli ocenia pozytywnie działalność kontrolowanej jednostki w zakresie zapewnienia dostępności informacji dla osób niepełnosprawnych na stronie internetowej Urzędu i w BIP.

### 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 o Najwyższej Izbie Kontroli, wnosi o:

1. Przyspieszenie działań dla pełnego wdrożenia do eksploatacji systemu e-Audytor.
2. Wprowadzenie obowiązku podłączania komputerów przenośnych co najmniej raz w okresie miesiąca.

### V. Pozostałe informacje i pouczenia

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

Prawo zgłoszenia zastrzeżeń

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 Departamentu Administracji Publicznej Najwyższej Izby Kontroli.

<sup>56</sup> <http://www.um.bielsko.pl>.

<sup>57</sup> <http://bip.um.bielsko.pl>.

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 14 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.

Warszawa, dnia     lutego 2014 r.

Kontrolerzy  
Mariusz Stolarz  
główny specjalista kontroli państwowej

.....  
*podpis*

Maciej Mierzejewski  
główny specjalista kontroli państwowej

.....  
*podpis*

Najwyższa Izba Kontroli  
Departament Administracji Publicznej  
Dyrektor  
Bogdan Skwarka

.....  
*Podpis*