NAJWYŻSZA IZBA KONTROLI
Delegatura w Katowicach

LKA – 4101-019-02/2014
P/14/004

WYSTĄPIENIE POKONTROLNE

NAJWYŻSZA IZBA KONTROLI
Delegatura w Katowicach
ul. Powstańców 29, 40-039 Katowice
T +48 32 784 42 00, F +48 32 784 42 30
lka@nik.gov.pl

I Dane identyfikacyjne kontroli

Numer i tytuł kontroli

P/14/004 - Wdrażanie wybranych wymagań dotyczących systemów teleinformatycznych, wymiany informacji w postaci elektronicznej oraz Krajowych Ram Interoperacyjności na przykładzie niektórych urzędów gmin miejskich i miast na prawach powiatu

Jednostka przeprowadzająca kontrolę

Najwyższa Izba Kontroli
Delegatura w Katowicach

Kontrolerzy

1. Jerzy Horodecki, główny specjalista kontroli państwowej, upoważnienie do kontroli nr 91672 z dnia 25 sierpnia 2014 r.

[dowód: akta kontroli str. 3÷4]

2. Arkadiusz Przytulski, specjalista k.p., upoważnienie do kontroli nr 90667 z dnia 25 czerwca 2014 r.

[dowód: akta kontroli str. 1÷2]

Jednostka kontrolowana

Urząd Miejski w Mysłowicach, ul. Powstańców 1, 41-400 Mysłowice[1]

Kierownik jednostki kontrolowanej

Edward Lasok, Prezydent Miasta.

[dowód: akta kontroli str. 5÷6]

II Ocena kontrolowanej działalności

Ocena ogólna

Najwyższa Izba Kontroli ocenia pozytywnie[2] działalność kontrolowanej jednostki w zbadanym zakresie.

Uzasadnienie oceny ogólnej

Prezydent Miasta realizując zadania określone w rozporządzeniu 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[3], m.in.:

- podjął działania, w wyniku których wybrane do badania systemy informatyczne współpracowały z systemami Urzędu, co spełniało minimalne wymogi interoperacyjności, o których mowa w § 5 ust. 3 pkt 3 rozporządzenia KRI,
- przeprowadził analizę zagrożeń występujących przy przetwarzaniu informacji, stosownie do wymogów § 20 ust. 2 pkt 3 rozporządzenia KRI,
- zapewnił, że pracownicy wykonujący zadania w wybranych systemach informatycznych uczestniczyli w procesie przetwarzania informacji w stopniu adekwatnym do zadań wynikających z ich zakresów obowiązków, co było wymagane § 20 ust. 2 pkt 4 rozporządzenia KRI,

---

[1] Zwany dalej „Urzędem".

[2] Najwyższa Izba Kontroli stosuje 3-stopniową skalę ocen: pozytywna, pozytywna mimo stwierdzonych nieprawidłowości, negatywna.

[3] Dz. U. z 2012 r., poz. 526 zwane dalej „rozporządzeniem KRI".

– zapewnił właściwe przyznawanie i odbieranie pracownikom uprawnień do pracy w systemach informatycznych, zgodnie z § 20 ust. 2 pkt 4 i 5 rozporządzenia KRI,

– zapewnił szkolenia dla pracowników zaangażowanych w proces przetwarzania informacji, stosownie do § 20 ust. 2 pkt 6 rozporządzenia KRI,

– zawarł w umowach na zakup i serwis sprzętu komputerowego i oprogramowania zapisy dotyczące zapewnienia zachowania bezpieczeństwa informacji.

III Opis ustalonego stanu faktycznego

1 Działania w zakresie dostosowania posiadanych systemów teleinformatycznych do współpracy z systemami / rejestrami informatycznymi

Opis stanu faktycznego

Dokumenty strategiczne

Strategia zrównoważonego rozwoju Mysłowice 2020+ opracowana przez Zespół do spraw rewitalizacji i strategii rozwoju miasta pod przewodnictwem Prezydenta Miasta, została przyjęta uchwałą Rady Miejskiej z dnia 27 marca 2014 r. jako aktualizacja dokumentu pn. „Strategia zrównoważonego rozwoju dla miasta Mysłowice do roku 2020”[4] i opublikowana w Biuletynie Informacji Publicznej (BIP) http://www.bip.myslowice.pl/ » Akty prawne i dokumenty » Plany i programy miejskie » Strategie. Podczas prac nad aktualizacją Strategii stworzono zainteresowanym możliwość przesyłania uwag i wniosków do powstającego dokumentu na specjalnie utworzoną skrzynkę e-mail.

W omawianym dokumencie wśród problemów, w *Obszarze instytucjonalnym*, wyszczególniono słabą bazę lokalową i wyposażenie Urzędu oraz podległych jednostek samorządowych niezapewniające odpowiedniego standardu obsługi mieszkańców i warunków pracy. Za istotne uznano również potrzeby w zakresie usprawnienia systemów informatycznych działających w Urzędzie. Dotyczy to w szczególności budowy nowej serwerowni zgodnie z obowiązującymi standardami dla tego typu pomieszczeń (tzw. *data center*), objęcie siecią komputerową wszystkich jednostek urzędu przy zapewnieniu odpowiedniego oprogramowania usprawniającego obieg dokumentów oraz prowadzenie wymaganych ewidencji i rejestrów. W dokumencie odnotowano, że nadal pozostaje dużo do zrobienia w zakresie usprawnienia komunikacji między jednostkami Urzędu (sprawna sieć komputerowa) oraz zapewnienia oprogramowania. Działania takie mają na celu usprawnienie pracy Urzędu, a w szczególności umożliwienie szybkiego dotarcia do kompleksowej i wyczerpującej informacji, co ma szczególne znaczenie w przypadku obsługi inwestorów. Jako słabą stronę w omawianym obszarze wykazano niewystarczające wykorzystanie środków informatycznych i telekomunikacyjnych w zakresie świadczenia usług publicznych.

Omawiany dokument nie zawierał terminów wdrożenia działań.

[Dowód: akta kontroli str. 7÷20]

[4] Przyjętego uchwałą z dnia 27 marca 2008 r.

Promowanie komunikacji elektronicznej

Dla zapewnienia możliwości wymiany dokumentów elektronicznych Urząd przystąpił do projektu *System Elektronicznej Komunikacji Administracji Publicznej* (SEKAP) realizowanego od 2011 r. Działania promocyjne podjęto w lutym 2012 r. Były to artykuły prasowe, ulotki i banery internetowe. Ze względu na brak środków nie zakupiono m.in. plakatów i banerów. W informacji dla Prezydenta Miasta ze stycznia 2013 r., wskazano na brak materiałów promocyjnych dotyczących platformy SEKAP.

[Dowód: akta kontroli str. 21÷27]

Ankiety lub inne formy poznania potrzeb mieszkańców gminy odnośnie elektronicznej formy komunikacji z Urzędem

Badania opinii klientów Urzędu prowadzone były na zlecenie Śląskiego Związku Gmin i Powiatów (dofinansowane ze środków unijnych). Wyniki badań z 2014 r. wskazywały, że tylko 9,8 % badanych załatwiało kiedykolwiek sprawę przez Internet. Było to najczęściej: uiszczenie opłaty (45 wskazań) i uzyskanie decyzji lub innego dokumentu (36 wskazań). Większość respondentów (69,2 %) nie wiedziało jakie sprawy można załatwić w Urzędzie drogą elektroniczną, a 58,8 % badanych stwierdziło, że woli załatwiać sprawy w Urzędzie osobiście.

W Raporcie przygotowanym przez Pełnomocnika ds. Zarządzania Jakością stwierdzono, że w 2013 roku w stosunku do 2012 roku - udział osób które korzystały z materiałów informacyjnych opracowanych i udostępnionych przez Urząd w Wirtualnym Biurze Mieszkańców (WBM) nie zmienił się i wynosił 38 %. Preferencje załatwiania sprawy elektronicznie zmniejszyły się z 29 % do 24%.

[Dowód: akta kontroli str. 28÷34]

Korespondencja z Ministrem Administracji i Cyfryzacji

Po wejściu w życie rozporządzenia KRI, Prezydent Miasta nie zwracał się do Ministra Administracji i Cyfryzacji z problemami ani z prośbą o pomoc w zakresie dostosowania swoich systemów / rejestrów informatycznych do wymogów Krajowych Ram Interoperacyjności.

[Dowód: akta kontroli str. 35÷40]

Obieg dokumentów

Obieg dokumentów w Urzędzie regulowały:

- rozporządzenie 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[5],
- zarządzenie Prezydenta Miasta Mysłowice nr 134/11 z dnia 14 marca 2011 r. w sprawie realizacji wymagań wynikających z ww. rozporządzenia Prezesa Rady Ministrów. Zarządzeniem tym wskazano system tradycyjny jako podstawowy sposób dokumentowania przebiegu załatwiania i rozstrzygania spraw,
- zarządzenie Prezydenta Miasta Mysłowic nr 431/13 z dnia 19 sierpnia 2013 r. w sprawie wprowadzenia Procedury obiegu dokumentów i spraw w Urzędzie. Zarządzeniem tym wskazano system tradycyjny jako podstawowy sposób dokumentowania przebiegu załatwiania i rozstrzygania spraw.

[5] Dz. U. nr 14 poz. 67

Procedura wprowadzona ostatnim z wymienionych zarządzeń Prezydenta Miasta przewidywała (z wyjątkami wyszczególnionymi w Zarządzeniu), że korespondencja podlega rejestracji w Elektronicznym Systemie Obiegu Dokumentów (e-SOD) lub w innym oprogramowaniu umożliwiającym rejestrację korespondencji poza e-SOD (np. Komputerowy System Obsługi Urzędu Stanu Cywilnego, Rejestr Wniosków i Decyzji dla Głównego Urzędu Nadzoru Budowlanego).

Korespondencję przychodzącą, w tym - drogą elektroniczną przy wykorzystaniu SEKAP, ePUAP lub wpływającą na główny adres e-mail Urzędu, przyjmuje i rejestruje Kancelaria Urzędu, natomiast przesyłki telefaksowe i pocztę elektroniczną wpływającą na adresy skrzynek wydziałowych lub służbowych imiennych - pracownik komórki organizacyjnej. Przesyłki takie po rejestracji i ewentualnym wykonaniu odwzorowania cyfrowego, przekazywane są do właściwej komórki organizacyjnej Urzędu za pośrednictwem e-SOD. Dla dokumentów papierowych, dodatkowo, przekazaniu za potwierdzeniem podlega także oryginał dokumentu, po oznaczeniu go numerem z e-SOD.

Przekazywanie korespondencji wychodzącej odbywa się: przesyłką listową, telefaksem, na nośniku informatycznym wysyłanym przesyłką listową, pocztą elektroniczną i przy wykorzystaniu platform SEKAP lub ePUAP. W ostatnim z przypadków korespondencja tworzona na odpowiednich stanowiskach przekazywana jest bezpośrednio adresatowi. W pozostałych przypadkach - za pośrednictwem Kancelarii.

[Dowód: akta kontroli str. 41÷63]

W okresie od 31 maja 2012 r. do 31 maja 2014 r. do Urzędu wpłynęło ogółem 326 101 dokumentów, w tym:

- 204 142 dokumentów od obywateli, w tym 1 728 — elektronicznych;
- 70 469 z innych urzędów, w tym 21 573 — w formie elektronicznej;
- 51 490 od pozostałych podmiotów, w tym 3 408 dokumentów elektronicznych.

Wysłano ogółem 361 157 dokumentów, w tym:

- 258 404 do obywateli, z tego 401 w formie elektronicznej;
- 58 568 do innych urzędów, w tym 22 132 elektronicznie;
- 44 185 do pozostałych podmiotów w tym 6074 w formie elektronicznej.

[Dowód: akta kontroli str. 64]

Usługi elektroniczne

Liczba usług elektronicznych udostępnionych na platformie SEKAP wyniosła: 217 w 2012 r., 153 w 2013 r. i 150 według stanu na 6 sierpnia 2014 r.

Aktualnie[6] Urząd świadczy 150 usług poprzez platformę SEKAP, w tym:

- w przypadku 111 usług użytkownik mógł wnieść sprawę i złożyć wniosek w formie elektronicznej,
- w przypadku 39 usług wniosek składany był w formacie pdf.

[Dowód: akta kontroli str. 76÷95]

[6] Według stanu na 6 sierpnia 2014 r.

Szczegółowym badaniem objęto pięć usług, tj.: Udostępnienie informacji publicznej, Uzyskanie karty dużej rodziny / wydanie duplikatu karty dużej rodziny, Zameldowanie na pobyt stały lub czasowy trwający ponad 3 miesiące, Nadanie numeru porządkowego oraz Uzyskanie decyzji ustalającej podatek od nieruchomości, rolny, leśny na dany rok podatkowy. Stwierdzono, że załatwianie ww. spraw przebiegało zgodnie z ich opisem zamieszczonym na platformie SEKAP i na stronie podmiotowej BIP Urzędu.

Opisy badanych pięciu usług były zgodne z usługami faktycznie świadczonymi przez Urząd i aktualne w zakresie informacji dotyczących usługodawcy, możliwości jakie daje dana usługa, terminu załatwienia sprawy, wymaganych dokumentów, podstawy prawnej i trybu odwoławczego.

Urząd publikował w BIP opisy procedur stosowanych przy załatwianiu spraw z zakresu jego właściwości drogą elektroniczną, w http://myslowice.pl/ » Wirtualny Urząd » Biuro Obsługi Mieszkańca » Katalog usług.

W procedurze systemu ISO pn. „Nadzór nad Kartami usług publicznych" określono zasady weryfikacji Kart pod względem spełniania oczekiwań klientów i wymagań formalno-prawnych.

[Dowód: akta kontroli str. 96÷196]

Centralne Repozytorium Dokumentów

Prezydent Miasta nie przekazywał do centralnego repozytorium na ePUAP wzorów dokumentów elektronicznych, o których mowa w art. 19b ust. 3 ustawy z dnia 17 lutego 2005 r. o informatyzacji działalności podmiotów realizujących zadania publiczne[7], gdyż wykorzystywane były wzory dokumentów dostępnych w katalogu usług SEKAP.

[Dowód: akta kontroli str. 197÷200]

Model usługowy

Urząd w podstawowym zakresie stosował rozwiązania informacyjne oparte na modelu usługowym[8] przy świadczeniu usług elektronicznych. Na podstawie pięciu objętych badaniem usług ustalono, że było możliwe zidentyfikowanie właściciela świadczonej usługi, tj. komórki organizacyjnej zajmującej się jej obsługą. W opisie usługi nie wskazano parametrów organizacyjno-technicznych jak maksymalny lub dopuszczalny czas ich niedostępności, sposobu zgłaszania awarii ani osób / komórek / podmiotów odpowiedzialnych za usuwanie awarii, ze względu na fakt, że usługi nie są świadczone elektronicznie na platformie SEKAP, której administratorem jest Śląskie Centrum Społeczeństwa Informacyjnego.

[Dowód: akta kontroli str. 197÷200]

Współpraca wybranych systemów informatycznych z innymi systemami

Zakres współpracy systemów informatycznych wewnątrz Urzędu został zbadany w oparciu o dobór celowy czterech aplikacji komputerowych zakupionych po 31 maja 2012 r., (tj. po wejściu w życie rozporządzenia KRI) od producentów był następujący:

Aplikacje firmy Rekord SI, tj.:

---

[7] Dz. U. z 2013 r., poz. 235 ze zm.

[8] Zgodnie z definicją zawartą w § 2 pkt 8 rozporządzenia KRI, model usługowy to model architektury systemu informatycznego, w którym dla użytkowników zdefiniowano stanowiące odrębną całość funkcje systemu teleinformatycznego (usługi sieciowe) oraz opisano sposób korzystania z tych funkcji.

- Zintegrowany System Zarządzania Dochodami,
- Dodatek Energetyczny,
- Ewidencja licencji transportu drogowego (eLTD)

Aplikacje te współpracują w ramach pakietu zintegrowanego w zakresie uznanym przez producenta oprogramowania za niezbędny. Ponadto jest możliwe pobieranie danych na poziomie jednostronnej komunikacji np. aktualizacja danymi z gminnej ewidencji ludności, import wpłat z systemu bankowego w zakresie obsługi płatności masowych. Pozwalają również na wymianę danych (np. proces generowania przelewów bankowych, które następnie są importowane do systemu bankowego) oraz na zapis raportów w formie arkuszy kalkulacyjnych i innych popularnych formatach.

Aplikacja firmy (CADexpert) System Informacji o Terenie Miasta Mysłowic pobiera (jednostronnie) dane z serwera Urzędu. Jest ona przeznaczona do prezentacji wcześniej zgromadzonych danych.

Objęte kontrolą oprogramowanie nie było przewidziane do tworzenia zasobów udostępnianych publicznie, o którym mowa w § 18. ust. 1 rozporządzenia KRI.

W ocenie NIK, objęte kontrolą systemy informatyczne spełniają minimalne wymogi interoperacyjności w zakresie współpracy z innymi systemami Urzędu określone w § 5 ust. 3 pkt 3 rozporządzenia KRI.

[Dowód: akta kontroli str. 201÷220]

Urząd korzysta z możliwości prowadzenia korespondencji w formie elektronicznej z innymi jednostkami administracji publicznej gdy istnieją możliwości prawne i techniczne, a jednostka oczekuje odpowiedzi w tej formie. Odpowiedź na korespondencję otrzymaną drogą elektroniczną udzielana była także tą drogą. Korespondencję w formie elektronicznej w zakresie wybranego katalogu spraw, Urząd prowadzi z Urzędem Wojewódzkim, który zwrócił się w tej sprawie do Urzędu. Korespondencja ta odbywa się za pośrednictwem platformy ePUAP. Urząd nie zwracał się do innych jednostek administracji publicznej o prowadzenie wzajemnej korespondencji w formie elektronicznej.

[Dowód: akta kontroli str. 241÷256]

Ocena cząstkowa

Najwyższa Izba Kontroli ocenia pozytywnie działania Urzędu w zakresie realizacji dostosowania posiadanych systemów teleinformatycznych do współpracy z innymi systemami, stosownie do wymogów wynikających z § 5 ust. 3 pkt 3 rozporządzenia KRI. Urząd zapewnił wymianę danych pomiędzy badanymi systemami informatycznymi z innymi systemami wewnątrz jednostki. Urząd świadczył 111 Usług w formie elektronicznej. Ponadto prowadzono komunikację elektroniczną ze Śląskim Urzędem Wojewódzkim w Katowicach.

2 Wdrożenie systemu zarządzania bezpieczeństwem systemów informatycznych

Opis stanu faktycznego

Dokumenty z zakresu bezpieczeństwa informacji

W Urzędzie opracowano i wdrożono do stosowania Politykę Bezpieczeństwa Urzędu - stanowiącą załącznik nr 1 do zarządzenia z dnia 23 lipca 2014 r. Prezydenta Miasta[9]. Jako podstawę prawną w zarządzeniu powołano m.in. rozporządzenie KRI. Poprzednio obowiązywały: zarządzenie Prezydenta Miasta z 6 maja 2005 r. w sprawie ochrony danych osobowych w Urzędzie Miasta Mysłowice oraz zarządzenie z 13 maja 2004 r. w sprawie wprowadzenia Regulaminu określającego zasady używania oprogramowania komputerów przez pracowników Urzędu Miasta Mysłowice.

[Dowód: akta kontroli str. 261÷298]

Posiadanie zinwentaryzowanego sprzętu informatycznego oraz zapobieganie możliwości instalacji nieautoryzowanego oprogramowania

Urząd ma zinwentaryzowany sprzęt informatyczny, którego szczegółowa ewidencja ilościowa prowadzona była w Wydziale Informatyki (WI) według numerów inwentarzowych nadanych przez Księgowość. Ewidencja zawiera dane techniczne w zakresie konfiguracji sprzętu i zainstalowanego oprogramowania (np. użytkownik, rodzaj komputera, urządzenia zewnętrzne i oprogramowanie), co spełniało wymogi określone w § 20 ust. 2 pkt 2 rozporządzenia KRI.

[Dowód: akta kontroli str. 299÷313]

Urząd otrzymał z Ministerstwa Spraw Wewnętrznych i Administracji (MSWiA) 16 stacji roboczych, serwer, router, 6 skanerów, 13 drukarek oraz 22 czytniki kart kryptograficznych. Sprzęt użytkowany jest w wydziałach w których miał pracować ZMOKU i został zaewidencjonowany w grupie środków obcych.

[Dowód: akta kontroli str. 341÷375]

Zbadano 26 komputerów, w tym 16 otrzymanych z MSWiA w zakresie możliwości zainstalowania na nich dowolnego oprogramowania przez użytkowników niebędących pracownikami służb informatycznych w Urzędzie i stwierdzono, że pracownicy nie mogli samodzielnie instalować oprogramowania na komputerach służbowych. Było to zgodne z § 20 ust. 2 pkt 4 rozporządzenia KRI, stanowiącym, że zarządzanie bezpieczeństwem informacji realizowane jest w szczególności przez podjęcie działań zapewniających, że osoby zaangażowane w proces przetwarzania informacji posiadają stosowne uprawnienia do realizowanych przez nie zadań oraz obowiązków mających na celu zapewnienie bezpieczeństwa informacji,.

[Dowód: akta kontroli str. 376,377, 421÷480]

Analizy utraty integralności, poufności lub dostępności informacji

Elementem Systemu zarządzania jakością wg PN-EN ISO 9001:2009 (System ISO) była Karta podprocesu nr 41, którego celem jest gwarancja jakości świadczonych usług i realizacja zadań poprzez: utrzymywanie i rozwój systemów informatycznych oraz zapewnienie poprawności i ciągłości działania struktury teleinformatycznej.

[9] w sprawie wyznaczenia administratora Bezpieczeństwa Informacji i Administratora Systemów Informatycznych oraz aktualizacji Polityki Bezpieczeństwa i Instrukcji Zarządzania Systemem Informatycznym służącym do przetwarzania danych osobowych w Urzędzie Miasta Mysłowice, zwane dalej „Zarządzeniem w sprawie bezpieczeństwa".

Karta przewiduje formularze własne, kontrolki pomocnicze: poprawności wykonania i archiwizacji kopii zapasowej, poprawności odczytu / odtworzenia danych / bazy danych / systemu z kopii, Listę kontroli antywirusowych oraz kontrolkę niedostępności systemów IT będącą wynikiem awarii krytycznych. Dokument wyszczególniał ryzyka, a w tym m.in.: skomplikowany i długotrwały proces migracji zgromadzonych danych, awarię sprzętu i oprogramowania spowodowaną czynnikami zewnętrznymi. Wykazane zostały także reakcje na ryzyko.

W Urzędzie wykonywano okresowe analizy utraty integralności, poufności lub dostępności informacji, o których mowa w § 20 ust. 2 pkt 3 rozporządzenia KRI oraz podejmowano dalsze działania związane z wynikami tych analiz. Przeprowadzano w tym zakresie audyty podatności serwerowej (wykrywanie luk) przy wykorzystaniu narzędzia informatycznego np. 2 lipca 2014 r.

[Dowód: akta kontroli str. 378÷417]

Zarządzanie uprawnieniami do pracy w systemach informatycznych

Obowiązki pracowników Urzędu i użytkowników zewnętrznych ujęto w § 7 Polityki bezpieczeństwa Urzędu, a nadawanie uprawnień do przetwarzania danych osobowych oraz ich rejestracja w systemie informatycznym w § 3 Instrukcji zarządzania systemem informatycznym.

Procedury nadawania upoważnień do przetwarzania danych osobowych i rejestrowania tych uprawnień w systemie informatycznym określała też Karta podprocesu nr 42 Systemu ISO, którego celem była ochrona danych osobowych i bezpieczeństwo informacji. Przewidziano siedem Formularzy własnych, a w tym: Wniosek o nadanie odebranie i modyfikację upoważnień i uprawnień do przetwarzania danych osobowych, Oświadczenie pracownika o przeszkoleniu, Ewidencja przeprowadzonych szkoleń z zakresu ochrony danych osobowych i osób w nich uczestniczących, Raport z naruszenia bezpieczeństwa. Dokument wyszczególniał ryzyka i reakcje na ryzyko.

Na podstawie przeglądu uprawnień dla 15 pracowników będących użytkownikami wybranych do badania systemów informatycznych, stwierdzono, że pracownicy Urzędu zaangażowani w proces przetwarzania informacji mieli stosowne upoważnienia i uczestniczyli w tym procesie w stopniu odpowiednim do realizowanych przez nich zadań oraz obowiązków mających na celu zapewnienie bezpieczeństwa informacji.

Ponadto, badaniem objęto zablokowanie dostępu do systemów informatycznych dziesięciu pracowników, z którymi rozwiązano stosunek pracy po 31 maja 2012 r. Stwierdzono, że osoby te miały zablokowany dostęp wszystkich do systemów informatycznych, uprawnienia do pracy w systemach komputerowych tych pracowników były kasowane. Było to zgodne z § 20 ust. 2 pkt 5 rozporządzenia KRI stanowiącym, że zarządzanie bezpieczeństwem informacji realizowane jest w szczególności poprzez bezzwłoczną zmianę uprawnień w przypadku zmiany zadań osób zaangażowanych w proces przetwarzania informacji.

[Dowód: akta kontroli str. 418÷480]

Szkolenia pracowników przetwarzających informacje

Zgodnie z § 20 ust. 2 pkt 6 rozporządzenia KRI, zarządzanie bezpieczeństwem informacji realizowane było w szczególności przez zapewnienie przez kierownictwo podmiotu publicznego warunków umożliwiających realizację i egzekwowanie szkolenia osób zaangażowanych w procesie przetwarzania informacji. Urząd zapewnił szkolenia pracowników zaangażowanych w proces przetwarzania informacji, które prowadzone były przez Administratora Bezpieczeństwa Informacji Urzędu. Zakres tematyczny szkoleń obejmował: zagrożenia bezpieczeństwa informacji, skutki naruszenia zasad bezpieczeństwa informacji, w tym odpowiedzialność prawną, stosowanie środków zapewniających bezpieczeństwo informacji, w tym urządzenia i oprogramowanie minimalizujące ryzyko błędów ludzkich. Szkolenia prowadzone były także przez firmy zewnętrzne i dotyczyły przykładowo: ochrony danych osobowych i ich legalnego przetwarzania oraz analizy ryzyka w audycie bezpieczeństwa informacji. W latach 2013-2014 w sześciu tego typu szkoleniach zewnętrznych wzięło ośmiu pracowników, zarówno informatycy, jak również pracownicy innych wydziałów Urzędu.

[Dowód: akta kontroli str. 481÷510]

Praca na odległość i mobilne przetwarzanie danych

W Urzędzie ustanowiono procedury gwarantujące bezpieczną pracę przy przetwarzaniu mobilnym i pracy na odległość, o których mowa w § 20 ust. 2 pkt 8 rozporządzenia KRI. Zagadnienia te ujęto w § 13 – *Dostęp zdalny i praca na odległość* ww. Instrukcji zarządzania systemem informatycznym Urzędu. Użytkownik przetwarzający dane na komputerze przenośnym, w myśl § 13 Instrukcji Zarządzania Systemem Informatycznym ma obowiązek w sposób szczególny chronić je przed nieuprawnionym dostępem, co najmniej zabezpieczając materiał silnymi hasłami dostępu, zwłaszcza podczas transportu, przechowywania i użytkowania komputera poza wyznaczonymi miejscami, o których mowa w Polityce Bezpieczeństwa. Pracownicy byli zapoznawani z ww. uregulowaniami.

[Dowód: akta kontroli str. 314÷340, 481-484, 489-491, 511]

Umowy serwisowe

W umowach zakupu licencji oprogramowania i umowach serwisowych czterech objętych kontrolą aplikacji, zgodnie z wymogami § 20 ust. 2 pkt 10 rozporządzenia KRI, zawarto zapisy dotyczące bezpieczeństwa informacji i tak:

- W umowach zawartych z Rekord SI sp. z o.o. w Bielsku-Białej obejmujących systemy informatyczne należące do pakietu zintegrowanego *Ratusz*: Zintegrowany System Zarządzania Dochodami, Dodatek Energetyczny oraz Ewidencja licencji transportu drogowego (eLTD) strony zobowiązały się m.in. do zachowania poufności i nieujawniania informacji uzyskanych w związku z wykonywaniem tej umowy, także po zakończeniu jej realizacji.

  Dodatkowo zawarta została z ww. podmiotem umowa z dnia 5 maja 2014 r. w przedmiocie serwisu i nadzoru autorskiego i asysty technicznej dla środowiska Linux / Firebird oprogramowania pakietu Ratusz zainstalowanego w Urzędzie. W umowie tej Wykonawca zobowiązał się do zachowania wszystkich danych pozyskanych przy wykonywaniu tej umowy, a także innych informacji mogących mieć charakter poufny w tajemnicy, także po jej zakończeniu.

- W umowie dotyczącej Systemu Informacji o Terenie Miasta Mysłowic, Wykonawca zobowiązał się wykorzystywać dane Systemu wyłącznie do celów realizacji umowy, a po jej zakończeniu — do wykasowania tych danych ze

swoich nośników komputerowych. Zastrzeżono również, że Wykonawca nie może kopiować danych, przetwarzać ich ani udostępniać osobom trzecim.

Według informacji Prezesa Zarządu dostawcy Systemu Informacji o Terenie - oprogramowanie nie przetwarzało danych osobowych.

W umowach zakupu i serwisu sprzętu komputerowego zawierano zapisy dotyczące postępowania w przypadku uszkodzenia dysku twardego, np. w umowie z dnia 4 lipca 2013 r. w § 6 zastrzeżono, że w przypadku konieczności wymiany dysku twardego uszkodzony dysk pozostawał w posiadaniu Urzędu.

Uszkodzone nośniki danych były przechowywane w zamkniętej szafie metalowej w pomieszczeniu WI. Nie były jeszcze niszczone.

[Dowód: akta kontroli str. 204÷228, 377, 521, 622-623]

Zgłaszanie incydentów naruszenia bezpieczeństwa informacji

Obowiązek określony w § 20 ust. 2 pkt 13 rozporządzenia KRI dotyczący bezzwłocznego zgłaszania incydentów naruszenia bezpieczeństwa informacji został ujęty w § 11 – *Postępowanie i podstawowe wytyczne w przypadku naruszenia ochrony danych osobowych* Instrukcji zarządzania systemem informatycznym. Załącznikiem nr 7 do Instrukcji był druk Raportu z naruszenia bezpieczeństwa. Druki te były wypełniane i ujęto w nich m.in.: awarie zasilaczy UPS, problem z wykonaniem kopii zapasowej bazy danych, podejrzenie kompromitacji certyfikatu. W raportach odnotowywano także przyczyny naruszenia bezpieczeństwa, postępowanie wyjaśniające i podjęte działania.

[Dowód: akta kontroli str. 314÷340]

Audyt wewnętrzny z zakresu bezpieczeństwa informacji

W Urzędzie przeprowadzono okresowy audyt wewnętrzny z zakresu bezpieczeństwa informacji, i tak:

- w 2012 - audyt dotyczył zakresu i jakości obsługi zadań wykonywanych przez wybrane systemy informatyczne. Zarekomendowano zaktualizowanie Polityki bezpieczeństwa Urzędu, co zrealizowano oraz - zakupienie oprogramowania biurowego dla administratora systemu e-SOD,
- w 2013 - audyt objął uprawnienia do pracy w dziedzinowym systemie teleinformatycznym. Rekomendacji z zakresu objętego kontrolą NIK nie było,
- w 2014 - w planie audytu przewidziano przeprowadzenie czynności sprawdzających w zakresie jakości obsługi zadań wykonywanych przez wybrane systemy informatyczne.

[Dowód: akta kontroli str. 528÷551]

Kopie zapasowe

W Urzędzie regularnie tworzono i testowano kopie zapasowe danych i oprogramowania aplikacyjnego, w którym przetwarzane są dane, stosownie do § 20 ust. 2 pkt 12 lit. b rozporządzenia KRI. Prowadzone są: kontrolka poprawności wykonania i archiwizacji dziennej kopii zapasowej, kontrolka poprawności odczytu / odtworzenia danych / bazy danych / systemu z kopii (taśma, płyta CD, DVD, BLU-RAY, dysk RDX), lista kontroli antywirusowych, lista instalacji lub aktualizacji oprogramowania i inne przewidziane w Instrukcji. Sporządzane były Protokoły zniszczenia nośnika zawierającego dane osobowe. Przeprowadzone oględziny Serwerowni wykazały, że zapewniono bezpieczne warunki pracy urządzeń zarówno w zakresie zasilania, jak i warunków klimatycznych.

[Dowód: akta kontroli str. 583÷592]

Przez pomieszczenie serwerowni głównej przebiegały instalacje wodociągowe i kanalizacyjne obudowane płytami kartonowo-gipsowymi, co w przypadku ich awarii mogłoby zakłócić pracę systemów informatycznych. Podczas kontroli, Prezydent Miasta podjął decyzję o:

- uzupełnieniu instalacji monitorujących o czujnik wycieku wody,
- dodatkowym zabezpieczeniu pomieszczenia na poziomach kanalizacji sanitarnej przed zalaniem urządzeń serwerowni,
- opracowaniu instrukcji dotyczącej zasad nadzoru i ochrony fizycznej w budynkach Urzędu,
- doposażeniu portierni w telefon komórkowy (do systemu powiadamiania przy wykorzystaniu SMS).

[Dowód: akta kontroli str. 552÷582, 593÷606]

Format danych udostępniany przez badane systemy informatyczne

Objęte kontrolą oprogramowanie:

- Zintegrowany System Zarządzania Dochodami,
- Dodatek Energetyczny,
- Ewidencja Licencji Transportu drogowego (eLTD),

współpracuje w ramach pakietu zintegrowanego Ratusz i ma możliwość udostępniania zasobów w formatach określonych w załączniku 2 do rozporządzenia KRI, tj.: xls, .rtf, .pdf, .txt.

- System Informacji o Terenie Miasta Mysłowic - nie jest przeznaczony do udostępniania danych w formie innej niż graficzna (dostosowana do przeglądarki internetowej).

Tym samym spełniony został warunek określony w § 18 ust. 1 rozporządzenia KRI o udostępnianiu zasobów informacyjnych w co najmniej jednym z formatów wymienionych w załączniku nr 2 do tego rozporządzenia KRI.

[Dowód: akta kontroli str. 607÷611]

Ocena cząstkowa

Najwyższa Izba Kontroli ocenia pozytywnie działalność Prezydenta Miasta w zakresie wdrożenia systemu zarządzania bezpieczeństwem systemów informatycznych. W Urzędzie zapewniono bieżącą inwentaryzacje sprzętu i oprogramowania służącego do przetwarzania informacji. Zabezpieczono komputery wykorzystywane w Urzędzie przed możliwością zainstalowania

nieautoryzowanego oprogramowania. Przeprowadzono szkolenia pracowników zaangażowanych w proces przetwarzania informacji.

3 Zapewnienie dostępności informacji dla osób niepełnosprawnych

Opis stanu faktycznego

W Strategii zrównoważonego rozwoju Mysłowice 2020+, wśród słabych stron w Obszarze instytucjonalnym wykazano niedostateczne przystosowanie budynków i stron internetowych dla osób niepełnosprawnych w Urzędzie Miasta i jednostkach miejskich.

Urząd, w umowach dotyczących systemów teleinformatycznych, ujmował zapisy o obowiązku ich dostosowywania do obowiązujących przepisów prawa. W odniesieniu do stron internetowych, miejski Pełnomocnik ds. Osób Niepełnosprawnych zwracał się do Kierownika Kancelarii Prezydenta Miasta o dostosowanie oficjalnej strony Mysłowic do możliwości osób z dysfunkcjami ograniczającymi dostęp do informacji, poprzez wprowadzenia zaleceń Web Content Accessibility Guidelines (WCAG).

Zarówno oficjalna strona Miasta jak i strona podmiotowa BIP umożliwiają wyświetlenie ich wersji kontrastowej (tekstowej).

W toku kontroli zweryfikowano strony internetowe Urzędu za pomocą następujących narzędzi:

a) walidacja narzędziem spod adresu http://validator.w3.org/:
   - strony Urzędu http://www.myslowice.pl/ wykazała 0 błędów i jedno ostrzeżenie,
   - strony podmiotowej BIP Urzędu http://www.bip.myslowice.pl/ - nie wykazała błędów i wykazała 1 ostrzeżenie,

b) walidacja przy pomocy walidatora arkuszy stylu spod adresu [http://jigsaw.w3.org/css-validator/] dla ww. stron internetowych Urzędu nie wykazała ostrzeżeń, a jeden błąd stwierdzono tylko na stronie podmiotowej BIP Urzędu.

Według wyjaśnień Naczelnika WI - błąd walidacji strony BIP wynika z użytych elementów na stronie i właściwości niezbędnej do kompatybilności ze starszymi przeglądarkami Microsoft Internet Explorer.

[Dowód: akta kontroli str. 612÷621]

Ocena cząstkowa

Najwyższa Izba Kontroli nie formułuje oceny cząstkowej w tym obszarze, gdyż zgodnie z § 22 rozporządzenia KRI systemy teleinformatyczne podmiotów realizujących zadania publiczne należy dostosować do wymagań określonych w § 19 ww. rozporządzenia, nie później niż w terminie 3 lat od dnia jego wejścia w życie, czyli do dnia 30 maja 2015 r.

IV 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 z dnia 23 grudnia 1994 r. o Najwyższej Izbie Kontroli[10] kierownikowi jednostki kontrolowanej przysługuje prawo zgłoszenia na piśmie

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

umotywowanych zastrzeżeń do wystąpienia pokontrolnego, w terminie 21 dni od dnia jego przekazania. Zastrzeżenia zgłasza się do dyrektora Delegatury NIK w Katowicach.

Katowice, dnia 30 października 2014 r.

Najwyższa Izba Kontroli

Delegatura w Katowicach

Kontrolerzy

Jerzy Horodecki
gł. spec. kontroli państwowej

… … … … … …

Arkadiusz Przytulski

spec. kontroli państwowej

… … … … … …