



NAJWYŻSZA IZBA KONTROLI
Departament Administracji Publicznej

KAP – 4101-002-05/2014
P/14/004

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
Adres korespondencyjny: Skr. poczt. P-14, 00-950 Warszawa 1

I. Dane identyfikacyjne kontroli

<i>Numer i tytuł kontroli</i>	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
<i>Jednostka przeprowadzająca kontrolę</i>	Najwyższa Izba Kontroli Departament Administracji Publicznej
<i>Kontroler</i>	Agnieszka Klimowicz, specjalista k.p., upoważnienie do kontroli nr 89922 z dnia 10 czerwca 2014 r. (dowód: akta kontroli str. 1-2)
<i>Jednostka kontrolowana</i>	Urząd Miejski w Pruszkowie (zwany dalej Urzędem) ul. Kraszewskiego 14/16, 05-800 Pruszków
<i>Kierownik jednostki kontrolowanej</i>	Jan Starzyński, Prezydent Miasta Pruszkowa (dowód: akta kontroli str. 208)
<i>Okres objęty kontrolą</i>	Od 31 maja 2012 r. do 21 lipca 2014 r.

II. Ocena kontrolowanej działalności

Ocena ogólna

Prezydent Miasta Pruszkowa 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 teleinformatycznych¹ (zwanego dalej rozporządzeniem KRI):

- zapewnił współpracę wybranych do badania systemów informatycznych z innymi systemami Urzędu oraz systemami innych jednostek administracji publicznej, co spełniało minimalne wymogi interoperacyjności, o których mowa w § 5 ust. 3 pkt 3 rozporządzenia KRI,
- przeprowadził analizę zagrożeń występujących przy przetwarzaniu informacji i podjął działania w celu zminimalizowania stwierdzonego ryzyka, co było zgodne z § 20 ust. 2 pkt 3 rozporządzenia KRI,
- zapewnił, że pracownicy wykonujący zadania w wybranych do badania systemach informatycznych uczestniczyli w procesie przetwarzania informacji w stopniu adekwatnym do zadań wynikających z ich zakresów obowiązków, co było zgodne z § 20 ust. 2 pkt 4 rozporządzenia KRI,
- zorganizował szkolenia dla pracowników zaangażowanych w proces przetwarzania informacji, czym spełnił wymóg określony w § 20 ust. 2 pkt 6 rozporządzenia KRI.

W badanym okresie Urząd Miejski w Pruszkowie zwiększył z jednej do 15 liczbę świadczonych usług elektronicznych oraz wprowadził trzy usługi informacyjne.

¹ Dz. U. z 2012 r., poz. 526.

Ustalenia kontroli wykazały następujące nieprawidłowości przy realizacji zadań określonych w rozporządzeniu KRI:

- nie opracowano Polityki Bezpieczeństwa Informacji, która jest elementem systemu zarządzania bezpieczeństwem informacji. W myśl § 20 ust. 3 rozporządzenia KRI wymagania w zakresie systemu zarządzania bezpieczeństwem informacji uznaje się za spełnione jeżeli zostały opracowane na podstawie Polskiej Normy PN-ISO/IEC 27001:2007 *Technika informatyczna. Techniki bezpieczeństwa. Systemy zarządzania bezpieczeństwem informacji. Wymagania.* oraz powiązanej z nią Polskiej Normy PN-ISO/IEC 17799:2007 *Technika informatyczna. Techniki bezpieczeństwa. Praktyczne zasady zarządzania bezpieczeństwem informacji.* W pkt. 5.1 normy PN-ISO/IEC 17799:2007 wskazano opracowanie i stosowanie dokumentu polityki bezpieczeństwa informacji. W 2011 r. opracowano *Politykę bezpieczeństwa w Urzędzie Miejskim w Pruszkowie.* Nie dotyczyła ona jednak wszystkich danych jakie są przetwarzane w Urzędzie, lecz tylko danych osobowych,
- nie prowadzono inwentaryzacji zasobów informatycznych, która zawierałaby pełne i aktualne informacje w zakresie posiadanego sprzętu informatycznego oraz jego konfiguracji, co było niezgodne z § 20 ust. 2 pkt 2 rozporządzenia KRI,
- niezgodnie z wymaganiami określonymi w § 20 ust. 2 pkt 4 rozporządzenia KRI, w normie PN-ISO/IEC 27001, załącznik A, pkt. A.11.2.2 oraz w normie PN-ISO/IEC 17799 pkt. 11.2.2 b, 60% badanej grupy użytkowników systemów informatycznych niebędących pracownikami służb informatycznych miało przyznane uprawnienia administracyjne na użytkowanych przez nich komputerach,
- nie odebrano uprawnień do systemów informatycznych Urzędu dwóm z dziewięciu osób, które w badanym okresie zakończyły zatrudnienie, co było niezgodne z § 20 ust. 2 pkt 5 rozporządzenia KRI; nieprawidłowość została usunięta w trakcie kontroli,
- brak we wszystkich badanych umowach na zakup i serwis oprogramowania zapisów gwarantujących zabezpieczenie poufności informacji przetwarzanych w systemach informatycznych, co było niezgodne z § 20 ust. 2 pkt 10 rozporządzenia KRI,
- nie przeprowadzono okresowego audytu wewnętrznego w zakresie bezpieczeństwa informacji, mimo, że na podstawie § 20 ust. 2 pkt 14 rozporządzenia KRI powinien odbywać się nie rzadziej niż raz na rok,
- nie sporządzano z odpowiednią częstotliwością kopii zapasowych danych z systemu informatycznego KASA, przez co nie spełniono wymogu minimalizowania ryzyka utraty informacji w wyniku awarii, określonego w § 20 ust. 2 pkt 12 lit. b rozporządzenia KRI,
- niewłaściwie fizycznie zabezpieczano kopie zapasowe danych z systemów informatycznych KASA i OPLOK, przez co nie spełniono wymogu określonego w § 20 ust. 2 pkt 12 lit. e rozporządzenia KRI,
- nie testowano kopii zapasowych z systemów informatycznych KASA i OPLOK, czym nie spełniono wymogu określonego w § 20 ust. 2 pkt 12 lit. b rozporządzenia KRI.

III. Opis ustalonego stanu faktycznego

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

Opis stanu
faktycznego

Dokumenty strategiczne

W *Strategii Rozwoju Pruszkowa do roku 2020*² wskazano trzy cele strategiczne, w tym *Zrównoważony rozwój społeczny*, który ma być osiągnięty m.in. poprzez realizację celu operacyjnego *Stworzenie społeczeństwa informacyjnego (wdrożenie programu e-pruszków)*. W opisie powyższego celu operacyjnego podano, m.in. że *miasto udostępni mieszkańcom elektroniczną platformę (e-pruszków) umożliwiającą załatwienie jak największej liczby spraw w Urzędzie Miejskim poprzez kontakt elektroniczny. Ograniczenie do niezbędnego minimum formalności wymagających osobistego kontaktu pozwoli mieszkańcom oszczędzać czas, zniesie ograniczenie jakim są godziny pracy Urzędu Miejskiego, ograniczy obieg dokumentów papierowych. (...) Warunkiem właściwego wykorzystania programu e-pruszków, podobnie jak i obecnego internetowego serwisu internetowego Urzędu Miejskiego na stronie <http://www.pruszkow.pl/> jest powszechny dostęp do szerokopasmowego Internetu. Miasto podejmie działania zmierzające do jak najpełniejszego włączenia pruszkowian do tej sieci. Stopień realizacji ww. celu operacyjnego ma być wyrażony dwoma wskaźnikami: liczba spraw załatwianych przez mieszkańców Pruszkowa drogą elektroniczną (szt.) oraz liczba mieszkańców Pruszkowa z możliwością dostępu do szerokopasmowego Internetu (osoby). NIK zauważa, że w *Strategii Rozwoju Pruszkowa do roku 2020* nie podano docelowych wartości powyższych wskaźników, które określiłyby jaki rezultat planuje się osiągnąć.*

(dowód: akta kontroli str. 50-56)

W *Strategii Promocji Miasta Pruszkowa na lata 2013-2020*³, w jednym z pięciu programów tj. *Pruszków – tu żyję!*, przewidziano do realizacji projekt *Usprawnienie systemu obsługi mieszkańca*, w ramach którego wyodrębniono działanie *Rozbudowa systemu e-administracji*. W opisie działania wskazano, że polega ono *na stałym i kompleksowym zwiększaniu stopnia wykorzystania nowoczesnych technologii informatycznych i telekomunikacyjnych w funkcjonowaniu Urzędu Miejskiego w Pruszkowie, zarówno w obszarze komunikacji i kooperacji wewnętrznej między miejskimi Wydziałami, Biurami, Zespołami, itd. (back office) oraz komunikacji zewnętrznej (relacje między Urzędem a jego klientami – mieszkańcami oraz przedsiębiorcami). Stałe poszerzanie pakietu spraw i procedur, jakie klient Urzędu może załatwić w formie zdalnej. Dla powyższego działania nie określono wskaźników jego realizacji*⁴.

(dowód: akta kontroli str. 57-69)

² Przyjętej uchwałą nr XXIV/230/2008 Rady Miejskiej w Pruszkowie z dnia 28 sierpnia 2008 r. w sprawie Strategii Rozwoju Pruszkowa do roku 2020.

³ Przyjętej uchwałą nr XXXVI/329/2013 Rady Miejskiej w Pruszkowie z dnia 29 sierpnia 2013 r. w sprawie przyjęcia Strategii Promocji Miasta Pruszkowa na lata 2013-2020.

⁴ Działanie *Rozbudowa systemu e-administracji* jest skorelowane z działaniem *Budowa interaktywnego systemu reagowania na problemy mieszkańców*, dla którego określono dwa wskaźniki realizacji: 1) utworzenie interaktywnego systemu reagowania na problemy mieszkańców, 2) procent usterek zlokalizowanych na terenie będącym w zarządzie Urzędu Miejskiego w Pruszkowie naprawianych w terminie do 2 tygodni od zgłoszenia – 50%.

Promowanie komunikacji elektronicznej

W okresie objętym kontrolą Urząd Miejski w Pruszkowie nie prowadził działań promujących komunikację elektroniczną oraz działań w kierunku poznania potrzeb mieszkańców w zakresie korzystania z elektronicznej formy komunikacji z Urzędem. Zastępca Prezydenta Miasta Pruszkowa Pan Andrzej Kurzela poinformował, że *Strategia Promocji Miasta Pruszkowa na lata 2013-2020* przewiduje poszerzenie pakietu spraw i procedur, jakie mieszkańiec może załatwić w formie elektronicznej.

(dowód: akta kontroli str. 3-5, 164-166)

Współpraca z Ministrem Administracji i Cyfryzacji

Po wejściu w życie rozporządzenia KRI⁵, Prezydent Miasta Pruszkowa nie zwracał się do Ministra Administracji i Cyfryzacji z problemami lub prośbą o pomoc w zakresie dostosowania swoich systemów/rejestrów informatycznych do wymogów Krajowych Ram Interoperacyjności.

(dowód: akta kontroli str. 3-5, 164-166)

Obieg dokumentów

W Urzędzie Miejskim w Pruszkowie obowiązywała instrukcja kancelaryjna stanowiąca załącznik nr 1 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 zakładowych⁶. Na podstawie § 1 ust. 3 powyższej instrukcji kancelaryjnej, zarządzeniem Nr 81/2011 Prezydenta Miasta Pruszkowa z dnia 21 czerwca 2011 r. w sprawie wskazania podstawowego systemu wykonywania czynności kancelaryjnych w Urzędzie Miejskim w Pruszkowie, wskazany został system tradycyjny wykonywania czynności kancelaryjnych jako podstawowy sposób dokumentowania przebiegu załatwiania i rozstrzygania spraw w Urzędzie Miejskim w Pruszkowie.

(dowód: akta kontroli str. 3-5, 48-49)

Zastępca Prezydenta Miasta Pruszkowa Pan Andrzej Kurzela poinformował, że według stanu na dzień 23 czerwca 2014 r., w Urzędzie Miejskim w Pruszkowie nie działał elektroniczny obieg dokumentów i nie opracowano procedury obiegu dokumentów drogą elektroniczną. W trakcie kontroli ustalono, że dokumenty wpływające do Urzędu drogą elektroniczną na konto e-mail prezydent@miasto.pruszkow.pl oraz do *Składu dokumentów* na ePUAP były pobierane przez uprawnionych pracowników, drukowane i wpisywane w rejestr papierowy. W przypadku wysyłania dokumentów za pośrednictwem poczty elektronicznej lub ePUAP, dokumenty sporządzone w wersji papierowej były skanowane i wysyłane jako załączniki wiadomości (przy wysłaniu przez ePUAP przesyłka podpisywana była przez Prezydenta Miasta Pruszkowa profilem zaufanym).

W przypadku wysyłania za pośrednictwem ePUAP sprawozdań budżetowych sporządzonych w wersji elektronicznej, przed wysłaniem sprawozdania te były podpisywane przez Prezydenta i Skarbnika Miasta Pruszkowa kwalifikowanym podpisem elektronicznym (pliki .xls oraz .XAdES). Urzędowe potwierdzenie przedłożenia, automatycznie generowane przez Elektroniczną Skrzynkę Podawczą odbiorcy, było drukowane i przekazywane osobie, która przygotowała wysłane dokumenty.

(dowód: akta kontroli str. 3-5, 164-166, 317-325, 362)

⁵ 31 maja 2012 r.

⁶ Dz. U. Nr 14, poz. 67 ze zm.

Zastępca Prezydenta Miasta Pruszkowa Pan Andrzej Kurzela poinformował, że 5 sierpnia 2009 r. Urząd Miejski w Pruszkowie przystąpił do projektu Urzędu Marszałkowskiego Województwa Mazowieckiego *Rozwój elektronicznej administracji w samorządach województwa mazowieckiego wspomagającej niwelowanie dwudzielności potencjału województwa*, który przewiduje m.in. wdrożenie Elektronicznego Zarządzania Dokumentacją w ramach Systemu e-Urząd. Według stanu na dzień 23 czerwca 2014 r. Urząd przygotowywał się na rozpoczęcie wykorzystania oprogramowania dostarczonego w ramach powyższego projektu. Zainstalowane zostały wszystkie komponenty. System został zintegrowany z portalem www.wrotamazowska.pl (front-office Systemu e-Urząd) oraz platformą ePUAP. Wdrożenie Elektronicznego Zarządzania Dokumentacją w Urzędzie Miejskim w Pruszkowie przewidziane jest na 1 stycznia 2015 r.

(dowód: akta kontroli str. 164-200)

W okresie od 31 maja 2012 r. do 31 maja 2014 r. do Urzędu wpłynęło łącznie 128 295 dokumentów (85,4% w postaci papierowej i 14,6% w postaci elektronicznej), w tym:

- od obywateli 35 334 dokumenty (97,9%) w postaci papierowej oraz 745 dokumentów (2,1%) w postaci elektronicznej,
- od osób prawnych i innych podmiotów (m.in. prowadzących działalność gospodarczą, stowarzyszeń, fundacji) 25 472 dokumenty (92,8%) w postaci papierowej oraz 1 979 dokumentów (7,2%) w postaci elektronicznej,
- od innych urzędów 48 739 dokumentów (75,3%) w postaci papierowej oraz 16 026 dokumentów (24,7%) w postaci elektronicznej.

W tym samym okresie Urząd Miejski w Pruszkowie wysłał ogółem 139 162 dokumenty (73,7% w postaci papierowej i 26,3% w postaci elektronicznej), w tym:

- do obywateli 70 289 dokumentów (99,3%) w postaci papierowej oraz 489 dokumentów (0,7%) w postaci elektronicznej,
- do osób prawnych i innych podmiotów (m.in. prowadzących działalność gospodarczą, stowarzyszeń, fundacji) 10 913 dokumentów (92,4%) w postaci papierowej oraz 900 dokumentów (7,6%) w postaci elektronicznej,
- do innych urzędów 21 312 dokumentów (37,7%) w postaci papierowej oraz 35 259 dokumentów (62,3%) w postaci elektronicznej.

(dowód: akta kontroli str. 3-5, 201)

Usługi elektroniczne

Według stanu na dzień 31 maja 2012 r. Urząd świadczył jedną usługę elektroniczną tj. Elektroniczną Skrzynkę Podawczą na ePUAP, natomiast według stanu na dzień 23 czerwca 2014 r. Urząd udostępniał 15 usług elektronicznych na ePUAP⁷ oraz trzy usługi informacyjne na stronie internetowej Urzędu⁸.

⁷ 1) Skargi, wnioski, zapytania do urzędu, 2) Zawiadomienie o odkryciu w trakcie robót budowlanych lub ziemnych przedmiotu, co do którego istnieje przypuszczenie, iż jest on zabytkiem, 3) Zawiadomienie o przypadkowym znalezieniu przedmiotu, co do którego istnieje przypuszczenie, iż jest on zabytkiem archeologicznym, 4) Rozpatrywanie wniosków o wyrażenie zgody na używanie herbu miasta, 5) Przyjmowanie wniosków i uwag do sporządzonego studium uwarunkowań i kierunków zagospodarowania przestrzennego, 6) Przyjmowanie wniosków i uwag do sporządzanych miejscowych planów zagospodarowania przestrzennego, 7) Sporządzenie lub zmiana miejscowego planu zagospodarowania przestrzennego, 8) Wypisy i wyrysy ze studium uwarunkowań i kierunków zagospodarowania przestrzennego, 9) Bonifikata od opłat rocznych z tytułu użytkowania wieczystego nieruchomości gruntowych, 10) Zezwolenie na usunięcie drzew i krzewów, 11) Przyjmowanie zgłoszeń od wykonawców prac geologicznych zamierzających przystąpić do wykonywania robót geologicznych, 12) Wpis do ewidencji obiektów świadczących usługi hotelarskie, nie będących obiektami hotelarskimi, 13) Zaświadczenia o stanie majątkowym mieszkańców, 14) Przyjmowanie zawiadomień o organizacji zgromadzenia publicznego, 15) Deklaracje o wysokości opłaty za gospodarowanie odpadami komunalnymi.

⁸ Odbierz dowód – System informacji o terminie odbioru dowodu osobistego, System informacji o obwodach – dostępny w okresach przedwyborczych, System Informacji Przestrzennej e-mapa.

Szczegółowym badaniem objęto pięć usług elektronicznych świadczonych przez Urząd, tj.:

- Skargi, wnioski, zapytania do urzędu,
- Sporządzenie lub zmiana miejscowego planu zagospodarowania przestrzennego,
- Bonifikata od opłat rocznych z tytułu użytkowania wieczystego nieruchomości gruntowych,
- Zezwolenie na usunięcie drzew i krzewów,
- Deklaracje o wysokości opłaty za gospodarowanie odpadami komunalnymi.

Opisy badanych usług były zgodne z usługami faktycznie świadczonymi przez Urząd i aktualne w zakresie informacji dotyczących usługodawcy, możliwości jakie daje wybrana usługa, charakterystyki osób, dla których przeznaczona jest usługa, czasu realizacji, wymaganych dokumentów, opłat oraz trybu odwoławczego.

Według stanu na dzień 27 czerwca 2014 r. na stronie internetowej BIP Urzędu Miejskiego w Pruszkowie⁹, w zakładce ePUAP znajdowała się informacja o procedurze składania dokumentów przez skrzynkę podawczą na ePUAP oraz *Instrukcja wypełniania deklaracji śmieciowej*.

(dowód: akta kontroli str. 3-5, 164-166, 254, 259-311)

Centralne Repozytorium Dokumentów

Prezydent Miasta Pruszkowa nie przekazał 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 publiczne¹⁰, gdyż skorzystał z wzorów dokumentów dostępnych w katalogu usług na ePUAP.

(dowód: akta kontroli str. 226-228, 317-325)

Model Usługowy

Urząd Miejski w Pruszkowie w podstawowym zakresie wspierał model usługowy¹¹ w zakresie świadczenia usług elektronicznych. Urząd nie opracował procedury postępowania dotyczącej zarządzania usługami elektronicznymi. Zastępca Prezydenta Miasta Pruszkowa Pan Andrzej Kurzela poinformował m.in., że *w systemach usług elektronicznych świadczonych przez Urząd nie można automatycznie przyporządkować usługi do konkretnego pracownika, w opisie usługi znajdują się jedynie dane dotyczące nazwy wydziału i miejsca obsługi oraz numery telefonów. Istnieją karty opisu usługi i następuje ich aktualizacja. Nie zostały określone okresy niedostępności usług elektronicznych, sposób zgłaszania awarii, osoby odpowiedzialne za usuwanie awarii oraz techniczny właściciel usługi. Przewidziana jest aktywność przez cały czas.*

W trakcie kontroli ustalono, że dla wszystkich pięciu badanych usług elektronicznych sporządzono karty usług. Jedna karta¹² została zaktualizowana jeden raz, natomiast pozostałe cztery¹³ nie były aktualizowane od dnia utworzenia tj. od lutego 2013 r.

⁹ <http://umpruszkow.bip.org.pl>

¹⁰ Dz. U. z 2013 r., poz. 235 ze zm.

¹¹ 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.

¹² Karta usługi *Deklaracje o wysokości opłaty za gospodarowanie odpadami komunalnymi*.

¹³ Karty następujących usług: 1. Skargi, wnioski, zapytania do urzędu, 2. Sporządzenie lub zmiana miejscowego planu zagospodarowania przestrzennego, 3. Bonifikata od opłat rocznych z tytułu użytkowania wieczystego nieruchomości gruntowych, 4. Zezwolenie na usunięcie drzew i krzewów.

Należy zauważyć, że we wszystkich pięciu kartach aktualizacji wymagała informacja dotycząca podstawy prawnej świadczonej usługi. Stwierdzono, że w przypadku czterech z pięciu badanych usług podano wydział, który realizuje daną usługę. Nie został wskazany wydział odpowiedzialny za realizację usługi *Deklaracje o wysokości opłaty za gospodarowanie odpadami komunalnymi*. W kartach usług nie określono sposobu postępowania w przypadku awarii.

(dowód: akta kontroli str. 3-5, 164-166, 269-311)

Współpraca wybranych systemów informatycznych z innymi systemami

Zakres i sposób współpracy systemów informatycznych wewnątrz Urzędu oraz ich współpracy z systemami innych jednostek administracji publicznej zbadano na próbie trzech systemów zakupionych po 31 maja 2012 r., tj.:

1. OPLOK – Opłaty lokalne, firmy [...] ¹⁴,
2. KASA – System obsługi kasy, firmy [...] ¹⁵,
3. e-Gmina firmy [...] ¹⁶, z następującymi modułami:
 - iMPA VS (Internetowy Manager Punktów Adresowych),
 - iRMK (Internetowy Rejestr Mienia Komunalnego),
 - iGeoPlan.

W wyniku badania ustalono, że:

- **System OPLOK** wykorzystywany był m.in. do prowadzenia ewidencji oraz rozliczania należności z tytułu opłat za gospodarowanie odpadami komunalnymi. Dane wejściowe podatników (w tym imię i nazwisko, PESEL, adres) zostały zaimportowane z Systemu Gospodarki Odpadami, który wcześniej funkcjonował w Urzędzie Miejskim w Pruszkowie. System wymieniał dane w sposób transakcyjny ¹⁷ z systemem KSZOB – Księgowość podatków i opłat oraz z systemem KASA – System obsługi kasy. System OPLOK automatycznie przysyłał dane (np. dotyczące wysokości naliczonej opłaty za gospodarowanie odpadami komunalnymi) do systemów KSZOB i KASA oraz automatycznie pobierał dane (np. o wysokości zaksięgowanej wpłaty z tytułu opłaty za gospodarowanie odpadami komunalnymi) z systemów KSZOB i KASA. System nie wymieniał danych z systemami/rejestrami zewnętrznymi.
- **System KASA** wykorzystywany był m.in. do rejestracji wpłat z tytułu opłat za gospodarowanie odpadami komunalnymi. System wymieniał dane w sposób transakcyjny z systemem KSZOB – Księgowość podatków i opłat oraz z systemem OPLOK – Opłaty lokalne. System KASA automatycznie przysyłał dane (np. o wysokości zaksięgowanej wpłaty z tytułu opłaty za gospodarowanie odpadami komunalnymi) do systemów KSZOB i OPLOK oraz automatycznie pobierał z nich dane (np. dotyczące wysokości naliczonej opłaty za gospodarowanie odpadami komunalnymi). System nie wymieniał danych z systemami/rejestrami zewnętrznymi.
- **Moduł iMPA VS w systemie e-Gmina** służył do prowadzenia bazy punktów adresowych. Dostęp do modułu iMPA VS realizowany był z poziomu

¹⁴ Na podstawie art. 5 ust. 2 ustawy z dnia 6 września 2001 r. o dostępie do informacji publicznej (Dz. U. z 2014 r. poz. 782) i art. 11 ust. 4 ustawy z dnia 16 kwietnia 1993 r. o zwalczaniu nieuczciwej konkurencji (Dz. U. z 2003 r. Nr 153, poz. 1503 ze zm.) NIK wyłączyła jawność informacji w zakresie nazwy firmy. Wyłączenia tego dokonano w interesie przedsiębiorcy.

¹⁵ j.w.

¹⁶ j.w.

¹⁷ Transakcyjny sposób współpracy oznacza, że wymiana danych pomiędzy systemami odbywa się w sposób w pełni zautomatyzowany, bez jakiegokolwiek pośrednictwa pracownika.

przeglądarki internetowej. Dodanie nowego punktu i zmiana położenia istniejących punktów realizowana była poprzez wskazanie lokalizacji w powiązaniu z treścią mapy numerycznej (dane dotyczące nr działki ewidencyjnej i obrębu były automatycznie pobierane przez moduł iMPA VS z Systemu Informacji Przestrzennej Starostwa Powiatowego w Pruszkowie). Dane dotyczące właściciela działki wprowadzane były ręcznie z wniosku o ustalenie numeru porządkowego, po wcześniejszym sprawdzeniu przez pracownika Urzędu zgodności dostarczanych danych z bazą danych ewidencji gruntów (aktualizowaną przez Urząd Miejski w Pruszkowie na podstawie danych otrzymywanych raz w miesiącu od Starostwa Powiatowego w Pruszkowie) i działem II elektronicznych ksiąg wieczystych. Po dodaniu punktu adresowego, generowany był dokument – zawiadomienie o nadaniu numeru porządkowego, który po akceptacji Naczelnika Wydziału Geodezji i Gospodarki Nieruchomościami Urzędu Miejskiego w Pruszkowie przesyłany był przez operatora modułu iMPA VS w pliku .pdf do Urzędu Statystycznego w Warszawie i Starostwa Powiatowego w Pruszkowie. Punkty adresowe nadane w module iMPA VS były automatycznie widoczne w Systemie Informacji Przestrzennej Starostwa Powiatowego w Pruszkowie, a także w modułach iGeoPlan oraz iRMK systemu informatycznego e-Gmina.

- **Moduł iRMK w systemie e-Gmina** służył do zarządzania mieniem komunalnym miasta Pruszkowa. Obejmował informacje o działkach stanowiących mienie komunalne oraz rejestr użytkowników wieczystych, dzierżawców i podmiotów posiadających działki w trwałym zarządzie. Dostęp do modułu realizowany był z poziomu przeglądarki internetowej. Moduł iRMK automatycznie pobierał dane z innych modułów systemu e-Gmina tj. z iMPA VS informację o punktach adresowych, natomiast z iGeoPlan dane (warstwy) dotyczące np. planu zagospodarowania przestrzennego. Ponadto, moduł iRMK pobierał on-line dane z Systemu Informacji Przestrzennej Starostwa Powiatowego w Pruszkowie dotyczące geometrii (granic) działki stanowiącej mienie komunalne. Dane tekstowe opisujące daną działkę (m.in. nr działki, nr obrębu, nr księgi wieczystej, powierzchnia, położenie nieruchomości, informacje dotyczące właściciela, przeznaczenie w planie zagospodarowania przestrzennego, wartość nieruchomości, informacje czy działka jest w wieczystym użytkowaniu, w dzierżawie lub w trwałym zarządzie) wprowadzane były do modułu iRMK ręcznie przez pracownika Urzędu Miejskiego w Pruszkowie na podstawie dokumentów takich jak: akty notarialne, decyzje wojewody, decyzje Starosty Pruszkowskiego (tzw. ZRID), decyzje Prezydenta Miasta Pruszkowa. Wprowadzone dane nie były przekazywane do innych systemów informatycznych działających w Urzędzie, ani też do systemów informatycznych innych jednostek administracji publicznej.
- **Moduł iGeoPlan w systemie e-Gmina** wykorzystywany był do prowadzenia planu zagospodarowania przestrzennego, w szczególności generowania wypisów i wyrysów w wersji elektronicznej oraz prowadzenia rejestru decyzji o warunkach zabudowy. Oprogramowanie działało w środowisku przeglądarki internetowej. Współpracowało w sposób transakcyjny z innymi modułami systemu e-Gmina tj. iMPA VS oraz iRMK udostępniając wzajemnie w ramach modułów warstwy tematyczne poszerzające informacje z danego rejestru o dodatkowe dane.

Moduł iGeoPlan wymieniał dane w sposób transakcyjny z systemami zewnętrznymi tj. z centralnym systemem Geoportal.gov.pl oraz z Systemem Informacji Przestrzennej Starostwa Powiatowego w Pruszkowie. Wykorzystywał udostępnione on-line usługi sieciowe (WMS), które były dystrybuowane przez

Starostwo Powiatowe w Pruszkowie (za pośrednictwem Systemu Informacji Przestrzennej Starostwa Powiatowego), Generalną Dyрекcję Ochrony Środowiska oraz Główny Urząd Geodezji i Kartografii (za pośrednictwem centralnego systemu Geoportal.gov.pl), dotyczące warstw takich jak np. działki i budynki, ortofotomapa, obszary chronione. Z Systemu Informacji Przestrzennej Starostwa Powiatowego w Pruszkowie moduł iGeoPlan automatycznie pobierał zaktualizowaną mapę ewidencyjną, na którą Urząd Miejski w Pruszkowie nakładał dane związane z zagospodarowaniem przestrzennym w granicach administracyjnych miasta Pruszkowa.

W module iGeoPlan uprawnieni pracownicy Urzędu mieli dostęp do rozbudowanych warstw tematycznych obejmujących m.in. dane przestrzenne dotyczące planów zagospodarowania przestrzennego, rejestru miejscowych planów zagospodarowania przestrzennego, statystyk związanych z łączną powierzchnią miejscowych planów, rejestru decyzji administracyjnych wydanych przez Prezydenta Miasta Pruszkowa o warunkach zabudowy oraz o ustaleniu lokalizacji celu publicznego, statystyk związanych z liczbą i powierzchnią wydanych decyzji o warunkach zabudowy lub decyzji o ustaleniu lokalizacji celu publicznego wg statusu, jak również pod kątem rodzaju rozbudowy. Powyższe dane wprowadzane były do modułu iGeoPlan w systemie e-Gmina ręcznie przez pracowników Urzędu. Oprócz wymienionych warstw, uprawnieni pracownicy mieli podgląd do mapy zasadniczej Starostwa Powiatowego w Pruszkowie.

W przypadku uchwalenia przez Radę Miejską w Pruszkowie miejscowego planu zagospodarowania przestrzennego, Urząd Miejski w Pruszkowie zlecał firmie [...] ¹⁸ wprowadzenie danych przestrzennych w postaci cyfrowej do modułu iGeoPlan w systemie e-Gmina. Po odbiorze zlecenia Urząd udostępniał dane przestrzenne w systemie e-Gmina, które były automatycznie prezentowane w Systemie Informacji Przestrzennej Starostwa Powiatowego w Pruszkowie jak również w centralnym systemie Geoportal.gov.pl.

W ocenie NIK badane systemy informatyczne spełniały minimalne wymogi interoperacyjności ¹⁹ w zakresie współpracy z innymi systemami Urzędu lub systemami innych jednostek administracji publicznej, określone w § 5 ust. 3 pkt 3 rozporządzenia KRI ²⁰.

(dowód: akta kontroli str. 3-5, 164-166, 241-253)

Systemy informatyczne Urzędu Miejskiego w Pruszkowie wymieniały dane także z innymi systemami informatycznymi jednostek administracji publicznej, np. z CEIDG – Centralną Ewidencją i Informacją o Działalności Gospodarczej, z Rejestrem Wyborców Państwowej Komisji Wyborczej, z programu Płatnik wysyłane były do ZUS dane pracowników oraz dane z umów zlecenia, a za pośrednictwem programu Bestia do Regionalnej Izby Rozrachunkowej wysyłano sprawozdania finansowe. Zastępca Prezydenta Miasta Pruszkowa Pan Andrzej Kurzela poinformował, że w *większości przypadków nie ma opracowanych w pełni*

¹⁸ Na podstawie art. 5 ust. 2 ustawy z dnia 6 września 2001 r. o dostępie do informacji publicznej (Dz. U. z 2014 r. poz. 782) i art. 11 ust. 4 ustawy z dnia 16 kwietnia 1993 r. o zwalczaniu nieuczciwej konkurencji (Dz. U. z 2003 r. Nr 153, poz. 1503 ze zm.) NIK wyłączyła jawność informacji w zakresie nazwy firmy. Wyłączenia tego dokonano w interesie przedsiębiorcy.

¹⁹ Rozumianej jako zdolność różnych podmiotów oraz używanych przez nie systemów teleinformatycznych i rejestrów publicznych do współdziałania na rzecz osiągnięcia wzajemnie korzystnych i uzgodnionych celów, z uwzględnieniem współdzielenia informacji i wiedzy przez wspierane przez nie procesy biznesowe realizowane za pomocą wymiany danych za pośrednictwem wykorzystywanych przez te podmioty systemów teleinformatycznych.

²⁰ 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.

zautomatyzowanych mechanizmów integrujących programy obsługiwane przez poszczególne Wydziały Urzędu Miejskiego z systemami innych jednostek organów administracji publicznej. Dane wymieniane pomiędzy jednostkami przenoszone są na zewnętrznych nośnikach informacji jak np. w systemie SIO (System Informacji Oświatowej), Auta (dane zarejestrowanych i wyrejestrowanych pojazdów), EWOPIS (ewidencja gruntów).

Urząd prowadzi komunikację z innymi jednostkami administracji publicznej drogą tradycyjną oraz elektroniczną, i jak poinformował Prezydent Miasta Pruszkowa Pan Jan Starzyński, z żadną z tych jednostek nie komunikuje się wyłącznie elektronicznie. Urząd nie zwracał się do innych jednostek, ani nie otrzymał żadnego wniosku od innej jednostki administracji publicznej o prowadzenie wzajemnej wymiany korespondencji wyłącznie w formie elektronicznej.

(dowód: akta kontroli str. 317-325, 399-405)

Ustalone
nieprawidłowości

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

Uwagi dotyczące
badanej działalności

1. Opis pięciu badanych usług elektronicznych świadczonych przez Urząd za pośrednictwem ePUAP zawierał nieaktualne wskazania miejsca publikacji (dane promulgacyjne) podstawy prawnej świadczonej usługi. Ponadto, w przypadku jednej usługi pn. *Deklaracje o wysokości opłaty za gospodarowanie odpadami komunalnymi*, wskazano nieaktualną podstawę prawną tj. ustawę z dnia 11 maja 2001 r. o opakowaniach i odpadach opakowaniowych²¹, która została uchylona pół roku wcześniej²². Zastępca Prezydenta Miasta Pruszkowa Pan Andrzej Kurzela wyjaśnił m.in., że Urząd Miejski w Pruszkowie skorzystał z udostępnionego na ePUAP w dniu 9 czerwca 2010 r. pakietu usług dla jednostek samorządowych, i że opisy podstaw prawnych usług należących do ePUAP są niedostępne z poziomu Urzędu. NIK zauważa, że w trakcie kontroli Urząd podjął działania mające na celu aktualizację podstawy prawnej w opisach usług. Prezydent Miasta Pruszkowa Pan Jan Starzyński poinformował, że *Urząd Miejski przygotowuje korektę wszystkich usług na platformie ePUAP. Analizowana jest dokumentacja opublikowana przez platformę usług publicznych dotycząca modyfikacji kart usług. Wysłano zapytanie do pomocy ePUAP.*

(dowód: akta kontroli str. 254, 269-325, 399-409)

2. Na stronach internetowych Urzędu <http://www.pruszkow.pl> oraz <http://umpruszkow.bip.org.pl>, nie działały prawidłowo²³ odnośniki do usług elektronicznych świadczonych przez Urząd za pośrednictwem ePUAP²⁴. Usługi działały poprawnie po wejściu bezpośrednio na stronę ePUAP. Zastępca Prezydenta Miasta Pruszkowa Pan Andrzej Kurzela wyjaśnił m.in., że *linki przestały działać i zwracają błędy po zmianie systemu odwołań do wewnętrznych dokumentów na platformie ePUAP. Zastosowanie takiej technologii wyświetlania zawartości ePUAP uniemożliwia wygenerowanie jakiegokolwiek stałego linku odwołującego do usług udostępnionych przez Urząd. W związku z tym możemy jedynie linkować główną stronę ePUAP. Prace nad rozwiązaniem w/w problemu rozpoczęte zostały przed rozpoczęciem kontroli. Po zdiagnozowaniu problemu*

²¹ Dz. U. z 2001 r. Nr 63, poz. 638.

²² Z dniem 1 stycznia 2014 r.

²³ Wg stanu na dzień 26 i 27 czerwca 2014 r.

²⁴ Po kliknięciu w link następowało przekierowanie na stronę internetową ePUAP, na której wyświetlał się komunikat *Błędy. Źle przekazane parametry opisu* lub wyświetlała się grafika nagłówka strony ePUAP z wyszukiwarką (bez żadnej informacji dotyczącej usługi elektronicznej).

opracowaliśmy najkrótszą z możliwych drogę dostępu do naszych formularzy i w postaci instrukcji umieściliśmy na stronie BIP. Ponadto, Prezydent Miasta Pruszkowa Pan Jan Starzyński poinformował, że Urząd nie zgłaszał problemu nieprawidłowo działających linków (...). Wynikłe problemy są natury programistycznej natomiast Urząd jest tylko użytkownikiem korzystającym z narzędzi udostępnionych na Platformie ePUAP.

Z informacji uzyskanych z Centrum Projektów Informatycznych²⁵ wynika, że na platformie ePUAP nie został zmieniony system odwołań do wewnętrznych dokumentów, a zamieszczone na stronach internetowych Urzędu odnośniki do usług na platformie ePUAP nie działały ponieważ nie zostały utworzone poprawnie, zgodnie z instrukcją dotyczącą tworzenia odnośników do usług na platformie ePUAP.

NIK zauważa, że błędnie działające linki zostały usunięte w trakcie kontroli. Wprowadzona w zamian instrukcja korzystania z usług na ePUAP, zdaniem NIK, jest skomplikowana, gdyż wymaga od klienta Urzędu przeszukania kilku stron ePUAP w celu odnalezienia usługi elektronicznej świadczonej przez Urząd Miejski w Pruszkowie.

(dowód: akta kontroli str. 254-268, 317-325, 363-366, 399-405)

Ocena cząstkowa

Najwyższa Izba Kontroli ocenia pozytywnie działalność Urzędu w zakresie realizacji wymagań określonych w § 5 ust. 3 pkt 3 rozporządzenia KRI. Podjęto właściwe działania w celu dostosowania posiadanych systemów teleinformatycznych do współpracy z innymi systemami informatycznymi oraz systemami innych jednostek administracji publicznej, a także zwiększono liczbę świadczonych usług elektronicznych. NIK zauważa jednak, że możliwość skorzystania z tych usług jest utrudniona ze względu na brak na stronach internetowych Urzędu bezpośrednich odesłań do konkretnych usług świadczonych za pośrednictwem ePUAP.

2. Wdrożenie systemu zarządzania bezpieczeństwem systemów informatycznych

Opis stanu faktycznego

Dokumenty z zakresu bezpieczeństwa informacji

W Urzędzie obowiązywały następujące dokumenty wprowadzone zarządzeniem nr 30/11 Prezydenta Miasta Pruszkowa z dnia 10 marca 2011 r. w sprawie określenia i wdrożenia zasad bezpieczeństwa i ochrony danych osobowych przetwarzanych w Urzędzie Miejskim w Pruszkowie (zwanego dalej zarządzeniem nr 30/11):

- *Polityka bezpieczeństwa w Urzędzie Miejskim w Pruszkowie*, wprowadzająca reguły oraz zasady pozwalające na zapewnienie ochrony danych osobowych w Urzędzie Miejskim w Pruszkowie,
- *Instrukcja zarządzania systemami informatycznymi służącymi do przetwarzania danych osobowych w Urzędzie Miejskim w Pruszkowie*,
- *Instrukcja postępowania w przypadku naruszenia zasad ochrony danych osobowych*.

(dowód: akta kontroli str. 3-5, 71-144)

²⁵ W trybie art. 29 ust. 1 pkt 2 lit. f ustawy z dnia 23 grudnia 1994 r. o Najwyższej Izbie Kontroli (Dz.U. z 2012 r., poz. 82 ze zm.).

Uprawnienia pracowników na użytkowanych komputerach

W trakcie przeprowadzonych oględzin 10 komputerów w zakresie możliwości zainstalowania na nich dowolnego oprogramowania przez użytkowników niebędących pracownikami służb informatycznych w Urzędzie ustalono, że 4 z 10 badanych użytkowników systemów informatycznych miało ograniczone uprawnienia na użytkowanych przez nich komputerach, zgodnie z § 20 ust. 2 pkt 4 rozporządzenia KRI, z normą PN-ISO/IEC 27001, załącznik A, pkt. A.11.2.2 oraz normą PN-ISO/IEC 17799 pkt. 11.2.2 b.

(dowód: akta kontroli str. 396)

Analiza zagrożeń związanych z przetwarzaniem informacji

W Urzędzie sporządzono *Analizę zagrożeń i ryzyka przy przetwarzaniu danych osobowych w Urzędzie Miejskim w Pruszkowie*, która została zatwierdzona przez Prezydenta Miasta Pruszkowa Pana Jana Starzyńskiego w dniu 18 lutego 2013 r. Stosownie do wyników przeprowadzonej analizy, podjęto działania w celu wyeliminowania stwierdzonych ryzyk²⁶. Powyższe działania były zgodne z § 20 ust. 2 pkt 3 rozporządzenia KRI.

(dowód: akta kontroli str. 317-325, 342-354)

Zarządzanie uprawnieniami do pracy w systemach informatycznych

Zasady obowiązujące przy nadawaniu, modyfikowaniu i odbieraniu uprawnień użytkownikom systemów informatycznych określono w *Polityce bezpieczeństwa w Urzędzie Miejskim w Pruszkowie*, w rozdziale 5, pkt. 9 oraz w *Instrukcji zarządzania systemami informatycznymi służącymi do przetwarzania danych osobowych w Urzędzie Miejskim w Pruszkowie*, w rozdziale 2 *Nadawanie i cofanie uprawnień do przetwarzania danych i rejestrowania tych uprawnień w systemie informatycznym oraz wskazanie osoby odpowiedzialnej za te czynności*. W badaniu przeprowadzonym na próbie 15 pracowników wykonujących zadania w wybranych systemach informatycznych stwierdzono, że zgodnie z § 20 ust. 2 pkt 4 rozporządzenia KRI, osoby te uczestniczyły w procesie przetwarzania informacji w stopniu adekwatnym do zadań wynikających z ich zakresów obowiązków.

(dowód: akta kontroli str. 71-141, 367-372, 390)

Szkolenia pracowników zaangażowanych w proces przetwarzania informacji

Zastępca Prezydenta Miasta Pruszkowa Pan Andrzej Kurzela poinformował, że Urząd Miejski zapewnia szkolenia pracowników zaangażowanych w proces przetwarzania informacji. Każdy nowy pracownik w momencie przyjęcia, a także każdy pracownik, któremu przydzielono obowiązek przetwarzania informacji w danym systemie informatycznym zostaje przeszkolony m.in. w zakresie bezpieczeństwa informacji i sposobu postępowania z indywidualnie przydzielonym loginem do systemu. Szkolenia pracowników prowadzone były na bieżąco. Pracownicy zapoznali się z *Polityką bezpieczeństwa w Urzędzie Miejskim w Pruszkowie* oraz *Instrukcją zarządzania systemami informatycznymi służącymi do przetwarzania danych osobowych w Urzędzie Miejskim w Pruszkowie*, podpisali oświadczenia o zapoznaniu się z przepisami dotyczącymi ochrony danych osobowych i dokumentem *Zasady użytkowania sprzętu komputerowego przez pracowników Urzędu Miejskiego w Pruszkowie* oraz *obowiązki pracownicze*

²⁶ Założono instalację przeciwpożarową w całym budynku, przeniesiono UPS-y do nowej lokalizacji i zainstalowano dodatkową klimatyzację, rozbudowano serwerownię, wygospodarowano dodatkowe fundusze na wymianę sprzętu komputerowego z bezpieczniejszym systemem operacyjnym w związku z zaprzestaniem przez firmę Microsoft aktualizacji dotychczas zainstalowanego systemu Windows XP i oprogramowania serwerowego Windows 2003.

wynikające z ochrony danych osobowych i zobowiązali się do ich przestrzegania. Powyższe działanie było zgodne z § 20 ust. 2 pkt 6 rozporządzenia KRI.

(dowód: akta kontroli str. 317-332, 436-443)

Praca na odległość i mobilne przetwarzanie danych

W Urzędzie Miejskim w Pruszkowie nie ustanowiono procedur gwarantujących bezpieczną pracę na odległość, ponieważ, jak wyjaśnił Prezydent Miasta Pruszkowa Pan Jan Starzyński, *nie planuje się udostępniać pracy na odległość, ani też mobilnego przetwarzania danych. Urząd Miejski posiada na stanie komputery przenośne, ale wykorzystywane są one tylko do prezentacji multimedialnych lub obsługi sesji Rady Miejskiej bez dostępu do zasobów sieciowych Urzędu. Brak na tych komputerach konfiguracji do aplikacji dziedzinowych. Dostęp do firmowych kont internetowych znajduje się tylko na stacjonarnym stanowisku pracy.*

(dowód: akta kontroli str. 317-325, 399-405)

Serwis sprzętu informatycznego i oprogramowania

W dokumencie *Zasady użytkowania sprzętu komputerowego przez pracowników Urzędu Miejskiego w Pruszkowie oraz obowiązki pracownicze wynikające z ochrony danych osobowych*, stanowiącym załącznik do *Polityki bezpieczeństwa w Urzędzie Miejskim w Pruszkowie*, wskazano, że serwis sprzętowy i programowy wykonywany jest przez informatyka lub przez przedstawicieli firm serwisujących dane systemy informatyczne pod nadzorem informatyka. W rozdziale 9 *Instrukcji zarządzania systemami informatycznymi służącymi do przetwarzania danych osobowych w Urzędzie Miejskim w Pruszkowie*, określono, że w przypadku stwierdzenia uszkodzenia urządzenia, dyski i inne informatyczne nośniki danych zawierające dane osobowe przed ich przekazaniem w celu naprawy innemu podmiotowi są wymontowywane.

W okresie objętym kontrolą Urząd Miejski w Pruszkowie dokonał zakupu 20 zestawów komputerowych, z trzyletnim okresem gwarancji. W warunkach gwarancji wskazano, że komputery będą naprawiane w miejscu ich instalacji, a w przypadku awarii dysków twardych, dyski te pozostaną w Urzędzie.

(dowód: akta kontroli str. 71-136, 420-428)

Zgłaszanie incydentów naruszenia bezpieczeństwa informacji

W Urzędzie obowiązywała *Instrukcja postępowania w przypadku naruszenia zasad ochrony danych osobowych* wprowadzona zarządzeniem nr 30/11, która opisywała procedurę postępowania w przypadku uzasadnionego podejrzenia naruszenia zasad ochrony danych osobowych i zawierała wzór *Protokołu z postępowania w związku z naruszeniem bezpieczeństwa systemu informatycznego w Urzędzie Miejskim w Pruszkowie*. Wszyscy pracownicy przetwarzający dane osobowe podpisali oświadczenia, w których zobowiązali się do natychmiastowego zgłaszania przełożonemu i Administratorowi Bezpieczeństwa Informacji stwierdzenia na swoim stanowisku pracy próby lub faktu naruszenia zabezpieczenia fizycznego pomieszczenia, bezpieczeństwa zbioru lub systemu informatycznego, w którym przetwarzane są dane osobowe.

Prezydent Miasta Pruszkowa Pan Jan Starzyński poinformował, że w przypadku jakiegokolwiek sytuacji incydentalnej pracownik natychmiast informuje o tym fakcie swojego przełożonego i w zależności od sytuacji – odpowiednie osoby (...) oraz sporządza notatkę służbową.

(dowód: akta kontroli str. 71, 142-144, 399-405, 436-442)

Kopie zapasowe

Obowiązująca w Urzędzie procedura tworzenia kopii zapasowych zbiorów danych oraz sposób, miejsce i okres ich przechowywania zostały opisane w rozdziale 5 i 6 *Instrukcji zarządzania systemami informatycznymi służącymi do przetwarzania danych osobowych w Urzędzie Miejskim w Pruszkowie*. W trakcie kontroli ustalono, że kopie bezpieczeństwa z badanych systemów OPLOK i KASA robione były przez informatyków i przechowywane były poza miejscem wytwarzania danych. Prezydent Miasta Pruszkowa Pan Jan Starzyński poinformował, że kopie zapasowe baz danych dla modułów iGeoPlan, iRMK oraz iMPA systemu e-Gmina wykonywane były codziennie przez firmę [...]27 i przez nią przechowywane przez 30 dni.

(dowód: akta kontroli str. 124-141, 253, 436-442, 445-446)

Format danych udostępniany przez badane systemy informatyczne

Systemy informatyczne OPLOK, KASA, e-Gmina iMPA VS, iRMK, iGeoPlan, udostępniały zasoby informacyjne w co najmniej jednym formacie danych wymienionym w załączniku nr 2 do rozporządzenia KRI28.

(dowód: akta kontroli str. 241-253)

Ustalone
nieprawidłowości

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

1. W Urzędzie Miejskim w Pruszkowie nie opracowano i nie wdrożono Polityki Bezpieczeństwa Informacji, która jest elementem systemu zarządzania bezpieczeństwem informacji. Było to niezgodne z § 20 ust. 3 rozporządzenia KRI, który stanowi, że wymagania w zakresie systemu zarządzania bezpieczeństwem informacji uznaje się za spełnione, jeżeli system ten został opracowany na podstawie Polskiej Normy PN-ISO/IEC 27001:2007 *Technika informatyczna. Techniki bezpieczeństwa. Systemy zarządzania bezpieczeństwem informacji. Wymagania* oraz powiązanej z nią Polskiej Normy PN-ISO/IEC 17799:2007 *Technika informatyczna. Techniki bezpieczeństwa. Praktyczne zasady zarządzania bezpieczeństwem informacji*. W pkt 5.1 normy PN-ISO/IEC 17799:2007 wskazano opracowanie i stosowanie dokumentu polityki bezpieczeństwa informacji. W 2011 r. opracowano *Politykę bezpieczeństwa w Urzędzie Miejskim w Pruszkowie*. Nie dotyczyła ona jednak wszystkich danych jakie są przetwarzane w Urzędzie, lecz tylko danych osobowych.

Zastępca Prezydenta Miasta Pruszkowa Pan Andrzej Kurzela wyjaśnił m.in., że w Urzędzie funkcjonują elementy systemu zarządzania bezpieczeństwem informacji. (...) Na dzień dzisiejszy trwają prace związane z opracowywaniem Polityki Bezpieczeństwa Informacji na podstawie Polskiej Normy PN-ISO/IEC 27001. Sprawdzane są wytyczne dotyczące bezpieczeństwa informacji wg ISO/IEC 27001 i norm powiązanych wg dokumentu „Bezpieczeństwo informacji” opracowanego przez audytora. Zakończenie opracowywania dokumentu odbędzie się po przeprowadzeniu audytu związanego z bezpieczeństwem informacji, który odbędzie się w IV kwartale 2014 r. (uwzględniony w planie rocznym audytów zaakceptowanym przez Prezydenta Miasta).

(dowód: akta kontroli str. 3-5, 71-163, 317-325, 333-340)

²⁷ Na podstawie art. 5 ust. 2 ustawy z dnia 6 września 2001 r. o dostępie do informacji publicznej (Dz. U. z 2014 r. poz. 782) i art. 11 ust. 4 ustawy z dnia 16 kwietnia 1993 r. o zwalczaniu nieuczciwej konkurencji (Dz. U. z 2003 r. Nr 153, poz. 1503 ze zm.) NIK wyłączyła jawność informacji w zakresie nazwy firmy. Wyłączenia tego dokonano w interesie przedsiębiorcy.

²⁸ Systemy OPLOK i KASA udostępniały dane w formacie .rtf, moduł iMPA VS w formatach .pdf i .html, moduł iRMK w formatach .pdf i .csv, moduł iGeoPlan w formatach .pdf, .gml, .xls.

2. W Urzędzie Miejskim w Pruszkowie nie prowadzono inwentaryzacji zasobów informatycznych, rozumianej jako stałe posiadanie aktualnych informacji w zakresie posiadanego sprzętu informatycznego oraz jego konfiguracji. Było to niezgodne z § 20 ust. 2 pkt 2 rozporządzenia KRI, który stanowi, że zarządzanie bezpieczeństwem informacji realizowane jest w szczególności przez utrzymywanie aktualności inwentaryzacji sprzętu i oprogramowania służącego do przetwarzania informacji obejmującej ich rodzaj i konfigurację. Ponadto, zgodnie z pkt. 7.1.1 normy PN-ISO/IEC 17799, wszystkie aktywa informatyczne powinny być zidentyfikowane oraz powinien być sporządzany i aktualizowany ich spis. 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.

Prezydent Miasta Pruszkowa Pan Jan Starzyński wyjaśnił, że w Urzędzie *prowadzona jest inwentaryzacja zasobów elektronicznych w wersji papierowej. Na kartach wpisane są podstawowe parametry stanowiska komputerowego (licencje systemowe, oprogramowanie biurowe) wraz z informacjami do jakiego typu aplikacji jest komputer przeznaczony. Wszystkie aplikacje instalowane są na serwerach aplikacji. Stacje robocze posiadają jedynie skróty do tych aplikacji. Urząd Miejski planuje zakup i wdrożenie elektronicznego systemu służącego do przetwarzania informacji obejmującej rodzaj i konfigurację sprzętu i oprogramowania. Dotychczasowe systemy umożliwiały jedynie rejestr środków trwałych pod względem finansowo-księgowym. Stare komputery posiadają niewystarczające zasoby systemowe na pracę systemów aktualizujących sprzęt i oprogramowania spowalniając drastycznie wydajność starych komputerów. W przypadku zdarzeń losowych konfiguracje serwerów oraz danych są odtwarzane z kopii bezpieczeństwa.*

NIK zwraca uwagę, że prowadzona inwentaryzacja zasobów elektronicznych w wersji papierowej obejmowała zaledwie 16% używanego w Urzędzie sprzętu informatycznego, tylko w czterech przypadkach zawierała informacje do jakiego typu aplikacji dziedzicznych komputer był przeznaczony i nie zawierała żadnych informacji o rodzaju i konfiguracji serwerów. Taki zakres zgromadzonych informacji stanowi ryzyko, że w przypadku katastrofy lub innego zdarzenia losowego odtworzenie zasobów informatycznych Urzędu będzie znacznie utrudnione.

(dowód: akta kontroli str. 397-405)

3. Ustalono, że 6 z 10 badanych użytkowników systemów informatycznych niebędących pracownikami służb informatycznych w Urzędzie Miejskim w Pruszkowie posiadało uprawnienia administratora systemu na używanych przez nich komputerach, w związku z czym mogli samodzielnie instalować dowolne oprogramowanie. Było to niezgodne 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 i uczestniczą w tym procesie w stopniu adekwatnym do realizowanych przez nie zadań oraz obowiązków mających na celu zapewnienie bezpieczeństwa informacji. Zgodnie z normą PN-ISO/IEC 27001, załącznik A, pkt. A.11.2.2 oraz normą PN-ISO/IEC 17799 pkt. 11.2.2 b należy ograniczać i kontrolować przyznawanie i korzystanie z przywilejów w systemach informatycznych, które powinny być nadawane według minimalnych wymagań wynikających z przydzielonych pracownikom zadań i tylko wtedy, gdy jest to konieczne. Ponadto w § 15 *Instrukcji zarządzania systemami informatycznymi*

służącymi do przetwarzania danych osobowych w Urzędzie Miejskim w Pruszkowie, stanowiącej załącznik nr B do zarządzenia nr 30/11 wskazano, że w związku z tym, że system informatyczny narażony jest na działanie oprogramowania, którego celem jest uzyskanie nieuprawnionego dostępu do tego systemu, konieczne jest podjęcie odpowiednich środków ochronnych.

Prezydent Miasta Pruszkowa Pan Jan Starzyński wyjaśnił m.in., że posiadanie konta administratora części pracowników jest uwarunkowane wymaganiami niektórych programów, które nie działają prawidłowo przy kontach typu User (zdarzały się przypadki nie zapisania danych wprowadzanych przez pracownika). Wynika to przede wszystkim z przestarzałego oprogramowania dziedzicznego, których autorzy nie są często w stanie zaktualizować oprogramowania na poziomie uprawnień systemowych w związku z często zmienianymi systemami operacyjnymi tj. Windows XP, Vista, Windows 7 i braku dokumentacji do tych systemów (pracownicy muszą często pracować z jednym programem pod różnymi systemami operacyjnymi).

Pracownicy są informowani o tym, iż nie mogą instalować nieautoryzowanego oprogramowania, a jedynie aktualizacje systemowe oraz aktualizacje oprogramowania (odbywają się automatycznie, tj. aktualizacje Windows, pakietów biurowych MS Office, Adobe Acrobat, programów antywirusowych, systemu Bestia, Multicash), co potwierdzili własnoręcznym podpisem w składanych oświadczeniach.

Prezydent Miasta Pruszkowa Pan Jan Starzyński dodał, że uprawnienia administracyjne wymuszają systemy firm [...] ²⁹, [...] ³⁰, [...] ³¹, gdyż wymagają zapisywania danych w plikach konfiguracyjnych w środowiskach Windows XP, Windows Vista, Windows 7 i dostępu do bibliotek systemowych.

Z informacji uzyskanych ³² od ww. producentów systemów informatycznych wynika, że systemy informatyczne w wersjach używanych przez Urząd Miejski w Pruszkowie, do prawidłowego działania nie wymagają uprawnień administracyjnych użytkowników w systemach Windows XP, Vista i 7.

NIK zauważa, że zobowiązanie pracowników do nieinstalowania nieautoryzowanego oprogramowania na komputerach służbowych jest niewystarczające. Mogą oni nieświadomie zainstalować szkodliwe oprogramowanie na komputerze, a tym samym spowodować zagrożenie dla bezpieczeństwa informacji przetwarzanych na komputerach i w systemach informatycznych Urzędu.

(dowód: akta kontroli str. 124-141, 396, 436-442, 449-459)

4. Stwierdzono, że według stanu na dzień 9 lipca 2014 r. dwie spośród dziewięciu osób, które w okresie od 31 maja 2012 r. do 26 czerwca 2014 r. zakończyły zatrudnienie w Urzędzie Miejskim w Pruszkowie ³³, posiadały aktywne uprawnienia do systemów informatycznych Urzędu. Było to niezgodne 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

²⁹ Na podstawie art. 5 ust. 2 ustawy z dnia 6 września 2001 r. o dostępie do informacji publicznej (Dz. U. z 2014 r. poz. 782) i art. 11 ust. 4 ustawy z dnia 16 kwietnia 1993 r. o zwalczaniu nieuczciwej konkurencji (Dz. U. z 2003 r. Nr 153, poz. 1503 ze zm.) NIK wyłączyła jawność informacji w zakresie nazwy firmy. Wyłączenia tego dokonano w interesie przedsiębiorcy.

³⁰ J.w.

³¹ J.w.

³² W trybie art. 29 ust. 1 pkt 2 lit. f ustawy z dnia 23 grudnia 1994 r. o Najwyższej Izbie Kontroli.

³³ Tj. 30 listopada 2013 r. oraz 3 stycznia 2014 r.

przetwarzania informacji oraz z § 8 ust. 1 *Instrukcji zarządzania systemami informatycznymi służącymi do przetwarzania danych osobowych w Urzędzie Miejskim w Pruszkowie*, stanowiącym, że w przypadku gdy ustał stosunek pracy, indywidualne hasła i uprawnienia pracownika do pracy przy przetwarzaniu danych osobowych są wycofywane przez skasowanie aktywności konta użytkownika.

Powyższa nieprawidłowość została usunięta w trakcie kontroli NIK. Prezydent Miasta Pruszkowa Pan Jan Starzyński wyjaśnił m.in., że konta ww. byłych pracowników w systemach informatycznych zostały zablokowane po wpłynięciu wniosku Skarbnika Miasta Pruszkowa Pani Lidii Sadowskiej-Muchy z dnia 9 lipca 2014 r. o odebranie uprawnień do pracy w systemach informatycznych.

Zdaniem NIK konieczne jest usprawnienie w Urzędzie przepływu informacji dotyczących zakończenia zatrudnienia przez osoby, które miały dostęp do systemów informatycznych. W ocenie NIK, pozwoli to na niezwłoczne blokowanie dostępu tych pracowników do systemów informatycznych.

(dowód: akta kontroli str. 124-141, 206-207, 213, 376-395, 399-405, 410-415, 436-444)

5. We wszystkich czterech badanych umowach na zakup i serwis oprogramowania, tj.:

- nr ORA.133.1.2013 z dnia 21 stycznia 2013 r. oraz nr ORA.133.30.2013 z dnia 30 grudnia 2013 r. zawartych z [...] ³⁴, na przedłużenie aktualizacji licencji oraz okresu autorskiej opieki technicznej ³⁵ nad wdrożeniem oprogramowania e-Gmina iMPA VS, iRMK, iGeoPlan,
- nr 132.01.2013 z dnia 18 czerwca 2013 r. zawartej z firmą [...] ³⁶, na udzielenie prawa do używania oprogramowania OPLOK oraz serwisu tego oprogramowania,
- nr 132.02.2013 z dnia 15 lipca 2013 r. zawartej z firmą [...] ³⁷, na udzielenie prawa do używania oprogramowania KASA oraz serwisu tego oprogramowania,

nie zawarto zapisów gwarantujących odpowiedni poziom bezpieczeństwa informacji, co było niezgodne z § 20 ust. 2 pkt 10 rozporządzenia KRI. W szczególności:

- w umowach z [...] ³⁸ Urząd Miejski w Pruszkowie nie zawarł żadnych zapisów mówiących o zobowiązaniu wykonawcy do zachowania w tajemnicy informacji, do jakich może mieć dostęp w związku z realizacją umowy, pomimo tego, że firma ta ma dostęp do baz danych i kopii zapasowych z wykorzystywanego w Urzędzie oprogramowania e-Gmina iMPA VS, iRMK, iGeoPlan, w którym przetwarzane są m.in. dane osobowe,

³⁴ Na podstawie art. 5 ust. 2 ustawy z dnia 6 września 2001 r. o dostępie do informacji publicznej (Dz. U. z 2014 r. poz. 782) i art. 11 ust. 4 ustawy z dnia 16 kwietnia 1993 r. o zwalczaniu nieuczciwej konkurencji (Dz. U. z 2003 r. Nr 153, poz. 1503 ze zm.) NIK wyłączyła jawność informacji w zakresie nazwy firmy. Wyłączenia tego dokonano w interesie przedsiębiorcy.

³⁵ Na którą składa się m.in. dostarczanie najnowszych wersji programu e-Gmina, pomoc techniczna dla pracowników merytorycznych (zdalna i telefoniczna), dbanie o sprawne działanie i konfigurację programu, utrzymanie na serwerze dedykowanym oprogramowania wraz z bazami danych (kopie zapasowe przechowywane 30 dni), bieżący nadzór nad prawidłowym działaniem i pomoc w sytuacjach nietypowych.

³⁶ J.w.

³⁷ J.w.

³⁸ J.w.

- w umowach zawartych z firmą [...] ³⁹ zawarto tylko zapisy gwarantujące ochronę informacji niejawnych i danych osobowych.

Prezydent Miasta Pruszkowa Pan Jan Starzyński wyjaśnił, że w przypadku umowy z [...] ⁴⁰ brak zapisów mówiących o zachowaniu tajemnicy zostanie sprostowany aneksem do umowy, natomiast w umowach zawartych z firmą [...] ⁴¹ zawarte jest zobowiązanie firmy do ochrony informacji niejawnych i danych osobowych.

Zdaniem NIK, zobowiązanie do ochrony informacji niejawnych i danych osobowych jest niewystarczające. Urząd Miejski w Pruszkowie powinien zapewnić w zawieranych umowach zachowanie w tajemnicy wszelkich informacji (z wyjątkiem informacji, których podanie wymagane jest obowiązującymi przepisami) do jakich wykonawca może mieć dostęp w związku z realizowaniem umowy.

(dowód: akta kontroli str. 429-442, 445-446, 448)

6. W Urzędzie Miejskim w Pruszkowie w okresie od 31 maja 2012 r. do 16 lipca 2014 r. nie przeprowadzono okresowego audytu wewnętrznego z zakresu bezpieczeństwa informacji. Było to niezgodne z § 20 ust. 2 pkt 14 rozporządzenia KRI, który stanowi, że zarządzanie bezpieczeństwem informacji realizowane jest w szczególności poprzez zapewnienie okresowego audytu wewnętrznego w zakresie bezpieczeństwa informacji, nie rzadziej niż raz na rok.

Prezydent Miasta Pruszkowa Pan Jan Starzyński wyjaśnił, m.in. że *zostały zakupione normy, o których wspomina rozporządzenie KRI. Na ich podstawie przygotowano Wytyczne i w roku bieżącym, zgodnie z planem audytów na 2014 r., ma być przeprowadzony audyt bezpieczeństwa informacji zgodnie z zapisami normy.*

(dowód: akta kontroli str. 355-360, 399-405)

7. W trakcie oględzin przeprowadzonych w dniu 16 lipca 2014 r. ustalono, że kopia zapasowa danych z systemu KASA została ostatnio sporządzona w dniu 11 lipca 2014 r. Było to niezgodne z obowiązującą w Urzędzie procedurą tworzenia kopii zapasowych zbiorów danych, zawartą w § 13 *Instrukcji zarządzania systemami informatycznymi służącymi do przetwarzania danych osobowych w Urzędzie Miejskim w Pruszkowie*, według której kopie programów finansowo-księgowych i budżetowych wykonuje się codziennie (oprócz niedziel). Ponadto działanie takie nie spełniało wymagania określonego w § 20 ust. 2 pkt 12 lit. b rozporządzenia KRI, tj. minimalizowania ryzyka utraty informacji w wyniku awarii.

Prezydent Miasta Pruszkowa Pan Jan Starzyński wyjaśnił, że *system KASA jest jednym z systemów firmy [...] ⁴², które pracują na jednym serwerze. W wyniku obecności 11 lipca 2014 r. pracowników firmy wdrażającej oprogramowanie Dzierżawy i Wieczyste użytkowanie została wyłączona możliwość automatycznego backupu. Po oględzinach w dniu 16 lipca 2014 r. konfiguracja została przywrócona.*

NIK zauważa, że w trakcie przeprowadzonych oględzin tworzenia kopii zapasowych danych z systemu KASA ustalono, że kopie te wykonywano ręcznie, zatem wyłączenie automatycznego sporządzania kopii zapasowych (backupu)

³⁹ J.w.

⁴⁰ J.w.

⁴¹ J.w.

⁴² J.w.

w dniu 11 lipca 2014 r. nie mogło mieć wpływu na częstotliwość sporządzania kopii bezpieczeństwa z systemu KASA.

(dowód: akta kontroli str. 124-141, 253, 436-442, 447)

8. Stwierdzono, że fizyczny sposób przechowywania kopii zapasowych danych z systemów OPLOK i KASA nie gwarantował, że dostęp do nich posiadać będą jedynie uprawnione osoby. Było to niezgodne z wymogami określonymi w § 20 ust. 2 pkt 12 lit. e rozporządzenia KRI, który stanowi, że zarządzanie bezpieczeństwem informacji realizowane jest w szczególności przez zapewnienie przez kierownictwo podmiotu publicznego warunków umożliwiających realizację i egzekwowanie m.in. zapewnienia odpowiedniego poziomu bezpieczeństwa w systemach informatycznych, polegającego w szczególności na zapewnieniu bezpieczeństwa plików systemowych. Było to również niezgodne z postanowieniami rozdziału X *Polityki bezpieczeństwa w Urzędzie Miejskim w Pruszkowie*, stanowiącymi, że miejsca przechowywania kopii zapasowych wyposaża się w system kontroli dostępu oraz zabezpiecza drzwi i okna, adekwatnie do poziomu ryzyka. Zauważyć należy również, że zgodnie z pkt. 10.5.1 normy PN-ISO/IEC 17799 kopie zapasowe powinny być odpowiednio zabezpieczone fizycznie.

Zdaniem NIK, podane w wyjaśnieniach Prezydenta Miasta Pruszkowa Pana Jana Starzyńskiego stosowane metody fizycznego zabezpieczenia kopii zapasowych, nie zapewniały wystarczającej ochrony przed dostępem osób nieupoważnionych.

(dowód: akta kontroli str. 71-80, 253, 436-442)

9. Ustalono, że kopie bezpieczeństwa z systemów OPLOK i KASA nie były testowane. Było to niezgodne z obowiązującą w Urzędzie procedurą tworzenia kopii zapasowych zbiorów danych, zawartą w § 13 *Instrukcji zarządzania systemami informatycznymi służącymi do przetwarzania danych osobowych w Urzędzie Miejskim w Pruszkowie*, według której kopie bezpieczeństwa powinny być automatycznie sprawdzane pod względem poprawności zapisu danych oraz okresowo sprawdzane pod kątem ich przydatności do odtworzenia danych w przypadku awarii systemu. Ponadto działanie takie nie spełniało wymagania określonego w § 20 ust. 2 pkt 12 lit. b rozporządzenia KRI, tj. minimalizowania ryzyka utraty informacji w wyniku awarii.

Prezydent Miasta Pruszkowa Pan Jan Starzyński wyjaśnił, że *integralność danych jest sprawdzana okresowo przez firmę [...] ⁴³ podczas częstych aktualizacji oprogramowania. Jest to konieczne, gdyż aktualizacje mogłyby spowodować niezgodności w pracy oprogramowania zakupionego przez Urząd Miejski w Pruszkowie.*

Zdaniem NIK powyższe działanie jest niewystarczające, gdyż aktualizacje oprogramowania nie występują w stałych okresach czasowych. Może więc wystąpić sytuacja, że przez dłuższe okresy czasu sporządzona kopia zapasowa nie będzie testowana pod względem prawidłowości jej wykonania. Ustalenie stałych okresów czasowych w jakich należy testować sporządzone kopie zapasowe wpłynie na zmniejszenie ryzyka utraty informacji w wyniku awarii.

(dowód: akta kontroli str. 124-141, 253, 436-442)

⁴³ Na podstawie art. 5 ust. 2 ustawy z dnia 6 września 2001 r. o dostępie do informacji publicznej (Dz. U. z 2014 r. poz. 782) i art. 11 ust. 4 ustawy z dnia 16 kwietnia 1993 r. o zwalczaniu nieuczciwej konkurencji (Dz. U. z 2003 r. Nr 153, poz. 1503 ze zm.) NIK wyłączyła jawność informacji w zakresie nazwy firmy. Wyłączenia tego dokonano w interesie przedsiębiorcy.

NIK zauważa, że w Urzędzie Miejskim w Pruszkowie nie opracowano i nie wdrożono do stosowania procedury bezzwłocznego zgłaszania incydentów naruszenia bezpieczeństwa wszelkich informacji. Obowiązująca w Urzędzie *Instrukcja postępowania w przypadku naruszenia zasad ochrony danych osobowych*, wprowadzona zarządzeniem nr 30/11, nie dotyczyła bowiem innych niż dane osobowe informacji przetwarzanych w Urzędzie. Zgodnie z § 20 ust. 2 pkt 13 rozporządzenia KRI, w ramach zarządzania bezpieczeństwem informacji, bezzwłoczne zgłaszanie incydentów naruszenia bezpieczeństwa informacji (nie tylko z zakresu danych osobowych) powinno odbywać się w określony i z góry ustalony sposób, umożliwiając szybkie podjęcie działań korygujących.

(dowód: akta kontroli str. 142-144, 399-405, 436-442)

Ocena częściowa

Najwyższa Izba Kontroli ocenia negatywnie działalność Urzędu Miejskiego w Pruszkowie w zakresie wdrażania systemu zarządzania bezpieczeństwem systemów informatycznych. Powyższą ocenę uzasadnia skala stwierdzonych nieprawidłowości. W Urzędzie nie opracowano Polityki Bezpieczeństwa Informacji, brak było kompletnej i aktualnej inwentaryzacji sprzętu komputerowego i posiadanego oprogramowania wraz z jego konfiguracją, byłym pracownikom nie odbierano bezzwłocznie uprawnień do systemów informatycznych Urzędu, użytkownicy niebędący pracownikami służb informatycznych posiadali możliwość instalacji dowolnego oprogramowania, w badanych umowach dotyczących zakupu i serwisu oprogramowania (zawartych przez Urząd w 2013 r.) brak było zapisów gwarantujących odpowiedni poziom bezpieczeństwa informacji, nie zrealizowano wewnętrznego audytu w zakresie bezpieczeństwa informacji, kopie bezpieczeństwa z systemu KASA nie były sporządzane z odpowiednią częstotliwością oraz nie były testowane i właściwie przechowywane, podobnie jak kopie zapasowe z systemu OPLOK.

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

Opis stanu
faktycznego

W toku kontroli zweryfikowano zgodność stron internetowych Urzędu Miejskiego w Pruszkowie <http://www.pruszkow.pl> oraz <http://umpruszkow.bip.org.pl>, ze standardem WCAG 2.0⁴⁴ w zakresie Zasady 4 – Kompatybilność. W badaniu z wykorzystaniem narzędzia dostępnego na stronie <http://validator.w3.org> stwierdzono 407 błędów i 110 ostrzeżeń na stronie <http://www.pruszkow.pl> oraz 24 błędy i 1 ostrzeżenie na stronie <http://umpruszkow.bip.org.pl>. W badaniu z wykorzystaniem narzędzia dostępnego na stronie <http://jigsaw.w3.org/css-validator> stwierdzono 17 błędów i 1 ostrzeżenie na stronie <http://www.pruszkow.pl> oraz 7 błędów na stronie <http://umpruszkow.bip.org.pl>. Strony internetowe Urzędu nie posiadały funkcjonalności pozwalającej na dostosowanie wyświetlanej treści do potrzeb osób niedowidzących (np. z powiększoną czcionką, obrazem, kontrastem).

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.

⁴⁴ WCAG jest standardem służącym dostosowaniu wyświetlanej treści na stronie internetowej do potrzeb osób niedowidzących. Rozwiązanie to ma na celu zapewnienie prezentacji treści w sposób ułatwiający osobom niepełnosprawnym zapoznanie się z wiadomościami. Ułatwienia te koncentrują się na sposobie wyświetlania i komunikatach głosowych.

Urząd Miejski w Pruszkowie podjął prace na rzecz realizacji obowiązku wynikającego z § 19 rozporządzenia KRI, stanowiącego, że w systemie teleinformatycznym podmiotu realizującego zadania publiczne służące prezentacji zasobów informacji należy zapewnić spełnienie przez ten system wymagań WCAG 2.0, z uwzględnieniem poziomu AA, określonych w załączniku nr 4 do rozporządzenia. W dniu 17 stycznia 2014 r. Urząd zawarł umowę z firmą [...] ⁴⁵ m.in. na wykonanie i dostarczenie serwisu internetowego Urzędu zgodnie ze specyfikacją funkcjonalną stanowiącą załącznik nr 1 do umowy, w której znajduje się zapis „Spełnienie wymogów dostępności zgodnie z wytycznymi WCAG 2.0 AA dla administracji publicznej m.in. poprzez stworzenie wersji kontrastowej serwisu”. Zastępca Prezydenta Miasta Pruszkowa Pan Andrzej Kurzela poinformował, że *w chwili obecnej zainstalowana jest wersja beta serwisu i odbyły się pierwsze szkolenia z funkcjonalności działania. Uruchomienie serwisu jest przewidziane na wrzesień 2014 r. Drugim serwisem internetowym Urzędu Miejskiego w Pruszkowie jest Biuletyn Informacji Publicznej, który również planujemy wymienić aby dostosować system do potrzeb osób niepełnosprawnych. Jesteśmy aktualnie na etapie prezentacji systemów BIP.*

(dowód: akta kontroli str. 222-225, 229-240, 317-325)

IV. Wnioski

Wnioski pokontrolne

Przedstawiając powyższe oceny i uwagi wynikające z ustaleń kontroli, Najwyższa Izba Kontroli, na podstawie art. 53 ust. 1 pkt 5 ustawy z dnia 23 grudnia 1994 r. o Najwyższej Izbie Kontroli ⁴⁶, wnosi o:

1. Opracowanie i wdrożenie Polityki Bezpieczeństwa Informacji, określającej zasady bezpieczeństwa informacji, zgodnej z normą PN-ISO/IEC 27001 oraz wykonywanie audytów w tym zakresie nie rzadziej niż raz na rok.
2. Prowadzenie aktualnej i kompletnej inwentaryzacji sprzętu informatycznego, obejmującej jego rodzaj i konfigurację.
3. Odebranie użytkownikom systemów informatycznych niebędących pracownikami służb informatycznych uprawnień umożliwiających instalowanie oprogramowania.
4. Przechowywanie kopii zapasowych danych z systemów informatycznych OPLOK i KASA w miejscu właściwie zabezpieczonym przed dostępem osób nieupoważnionych.
5. Ustalenie okresów w jakich powinno następować testowanie kopii zapasowych sporządzanych z systemów informatycznych.

⁴⁵ Na podstawie art. 5 ust. 2 ustawy z dnia 6 września 2001 r. o dostępie do informacji publicznej (Dz. U. z 2014 r. poz. 782) i art. 11 ust. 4 ustawy z dnia 16 kwietnia 1993 r. o zwalczaniu nieuczciwej konkurencji (Dz. U. z 2003 r. Nr 153, poz. 1503 ze zm.) NIK wyłączyła jawność informacji w zakresie nazwy firmy. Wyłączenia tego dokonano w interesie przedsiębiorcy.

⁴⁶ Dz.U. z 2012 r., poz. 82 ze zm.

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 Departamentu Administracji Publicznej Najwyższej Izby Kontroli.

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.

Warszawa, dnia 12 września 2014 r.

Najwyższa Izba Kontroli
Departament Administracji Publicznej

Kontroler
Agnieszka Klimowicz
specjalista k.p.

Dyrektor
Bogdan Skwarka

.....
podpis

.....
podpis