NAJWYŻSZA IZBA KONTROLI
Delegatura w Poznaniu

LPO-4101-012-03/2014
P/14/004

WYSTĄPIENIE POKONTROLNE

NAJWYŻSZA IZBA KONTROLI
Delegatura w Poznaniu
ul. Dożynkowa 9H, 61-662 Poznań
T +48 61 655 62 00, F +48 61 655 62 01
lpo@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 Poznaniu

Kontroler

Piotr Białka, główny specjalista k.p., upoważnienie do kontroli nr 90970 z dnia 24 czerwca 2014 r.

(dowód: akta kontroli str. 1-2)

Jednostka kontrolowana

Urząd Miasta Leszna, ul. K. Karasia 15, 64-100 Leszno (dalej: Urząd)

Kierownik jednostki kontrolowanej

Tomasz Malepszy, Prezydent Miasta Leszna (dalej: Prezydent)

(dowód: akta kontroli str. 3-4)

II. Ocena kontrolowanej działalności

Ocena ogólna

Prezydent Miasta Leszna[1] w okresie od 31 maja 2012 r. do 6 sierpnia 2014 r., 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[2] (dalej: rozporządzenie w sprawie KRI):

− zapewnił współpracę wybranych do badania systemów informatycznych z innymi systemami Urzędu zgodnie z wymaganiami określonymi w § 5 ust. 3 pkt 3 rozporządzenia w sprawie KRI,

− inwentaryzował posiadany sprzęt informatyczny, zgodnie z § 20 ust. 2 pkt 2 rozporządzenia w sprawie KRI,

− właściwie tworzył, przechowywał i zabezpieczał kopie zapasowe danych, zgodnie z § 20 ust. 2 pkt 12 lit. b i e rozporządzenia w sprawie KRI,

− zapewnił szkolenia osób zaangażowanych w proces przetwarzania informacji, zgodnie z § 20 ust. 2 pkt 6 rozporządzenia w sprawie KRI.

Ustalenia kontroli wykazały także m.in. następujące nieprawidłowości przy realizacji zadań określonych w rozporządzeniu w sprawie KRI:

− nienależycie zrealizowano wymagania określone w § 20 ust. 3, gdyż nie aktualizowano wewnętrznych regulacji dotyczących systemu zarządzania bezpieczeństwem informacji,

− nie przeprowadzano okresowych audytów wewnętrznych w zakresie bezpieczeństwa informacji, co było niezgodne z treścią § 20 ust. 2 pkt 14,

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

[2] Dz. U. z 2012 r. poz. 526.

− nie przeprowadzano okresowych analiz ryzyka utraty integralności, poufności lub dostępności informacji, których obowiązek przeprowadzania wynika z § 20 ust. 2 pkt 3.

III. Opis ustalonego stanu faktycznego

1. Działania w zakresie dostosowania posiadanych systemów teleinformatycznych do współpracy z systemami/rejestrami używanymi przez inne podmioty administracji publicznej

Opis stanu faktycznego

1.1. W Strategii rozwoju Leszna zawarto założenia programu „Przyjazny Urząd", którego elementem było wprowadzenie elektronicznego obiegu dokumentów, ułatwienie mieszkańcom dostępu do informacji oraz umożliwienie mieszkańcom elektronicznego załatwienia spraw poprzez internet. W Strategii zawarto także założenia programu „Rozwój infrastruktury społeczeństwa informacyjnego", którego celem było ułatwienie klientom Urzędu dostępu do internetu.

(dowód: akta kontroli str. 183-187)

W okresie objętym kontrolą, miasto Leszno (wspólnie z miastem Konin) przystąpiło (w ramach Programu Operacyjnego Kapitał Ludzki 2007-2013) do realizacji projektu „E-urząd dla e-obywatela, wdrożenie elektronicznych usług publicznych w Koninie i Lesznie". Głównymi celami projektu były: podniesienie świadomości obywateli oraz promocja wzrostu wykorzystania elektronicznych usług publicznych świadczonych przez Leszno i Konin; podniesienie wiedzy i umiejętności pracowników samorządowych w zakresie stosowania nowoczesnych rozwiązań IT w procesie świadczenia elektronicznych usług publicznych; wzrost wymiany korespondencji elektronicznej wysłanej przez urzędy jednostek samorządu terytorialnego; wzrost liczby elektronicznych usług publicznych świadczonych za pośrednictwem ePUAP lub platformy regionalnej kompatybilnej z ePUAP.

W ramach działań dotyczących przygotowania projektu zidentyfikowano potrzeby oraz wskazano do jakich grup skierowane miały być działania.

Projekt ten nie uzyskał wsparcia finansowego.

Zgodnie z wyjaśnieniami Macieja Dziamskiego Sekretarza Miasta Leszna uzyskana przy jego pisaniu wiedza (grupy docelowe i narzędzia promocji) zostanie wykorzystana przy pozyskiwaniu pieniędzy na realizację powyższego zadania z innych źródeł finansowania, a w roku bieżącym, z pieniędzy własnych zostanie zrealizowana część powyższego projektu - opracowanie i wdrożenie Systemu Zarządzania Bezpieczeństwem Informacji oraz systemu zarządzania usługami IT.

(dowód: akta kontroli str. 183-187, 239-247, 342-350)

1.2. Urząd podejmował akcje informacyjno-promocyjne zachęcające mieszkańców do wykorzystywania elektronicznych form komunikacji z Urzędem.

Wykorzystywał do tego celu m.in.:

- publikacje danych kontaktowych (adresy mailowe) w nagłówkach i stopkach dokumentów oraz w materiałach medialnych dotyczących Miasta;
- zamieszczanie na stronie internetowej www.leszno.pl informacji dotyczących funkcjonowania miasta i Urzędu;
- zamieszczanie na stronie internetowej www.leszno.pl interaktywnego formularza „Zadaj pytanie Prezydentowi";
- corocznie opracowywaną broszurę informacyjną „Leszno w liczbach", która wskazywała do kontaktu również pocztę elektroniczną. Broszura ta była rozsyłana do wszystkich mieszkańców miasta;

- informowanie mieszkańców w wydawnictwie tradycyjnym „Wiadomości Miasta Leszna", o sprawach, które można załatwiać przez internet (np.: konsultacje społeczne, nabór do szkół);
- promowanie wiadomości o Urzędzie za pośrednictwem portali społecznościowych. Prezentowane tam informacje odsyłały do miejskich stron internetowych.

(dowód: akta kontroli str. 255-259, 294-299, 342-350)

1.3. Urząd nie przeprowadzał osobnych ankiet dotyczących potrzeb korzystania z elektronicznych form komunikacji z Urzędem. Miasto prowadziło badania dotyczące jakości życia w mieście - badania realizowano w latach: 1995, 1999, 2005, 2009 i 2013. Pytania dotyczące komunikacji elektronicznej zawarto w trzech ostatnich kwestionariuszach.

(dowód: akta kontroli str. 137-156)

1.4. Po wejściu w życie rozporządzenia w sprawie KRI[3], Prezydent nie zwracał się do Ministra Administracji i Cyfryzacji z problemami/prośbą o pomoc w zakresie dostosowania swoich systemów/rejestrów informatycznych do wymogów ww. rozporządzenia.

(dowód: akta kontroli str. 342-350)

1.5. W Urzędzie, w celu zarządzania obiegiem dokumentów i dokumentacją, stosowane były procedury i zasady postępowania z dokumentami wpływającymi do Urzędu, zawarte w Instrukcji Kancelaryjnej stanowiącej załącznik do rozporządzenia Prezesa Rady Ministrów z dnia 18 stycznia 2011 r. w sprawie instrukcji kancelaryjnej, jednolitych rzeczowych wykazów akt oraz instrukcji w sprawie organizacji i zakresu działania archiwów zakładowych[4].

Zgodnie z § 1 zarządzenia nr 165/2011 Prezydenta w sprawie sposobu dokumentowania przebiegu załatwiania i rozstrzygania spraw z dnia 7 czerwca 2011 r., jako podstawowy sposób dokumentowania przebiegu załatwiania i rozstrzygania spraw wskazano tradycyjny system wykonywania czynności kancelaryjnych.

Urząd nie korzystał z systemu elektronicznego obiegu dokumentów, w związku z powyższym nie zostały opracowane w nim procedury regulujące komunikację elektroniczną.

(dowód: akta kontroli str. 27)

Zgodnie z regulaminem organizacyjnym Urzędu[5] do zakresu zadań wszystkich komórek organizacyjnych należało stosowanie zasad dotyczących obiegu dokumentów.

(dowód: akta kontroli str. 5-26)

Urząd realizował usługę „Skargi, wnioski, zapytania do urzędu", za pośrednictwem Elektronicznej Skrzynki Podawczej (dalej: ESP) na platformie ePUAP[6]. Dostęp do ESP na ePUAP posiadało sześciu pracowników: dwie osoby z Referatu ds. Informatyzacji Wydziału Organizacyjnego Urzędu, które obsługiwały korespondencję wchodząca i wychodzącą za jej pośrednictwem i cztery osoby z Wydziału Spraw Obywatelskich, które wysyłały do Wielkopolskiego Urzędu Wojewódzkiego pliki aktualizacyjne zawierające zmiany w lokalnej Ewidencji Ludności i odbierały pliki odpowiedzi przesyłane przez Wielkopolski Urząd Wojewódzki.

Ustalono, że przyjętą praktyką w Urzędzie dotyczącą ESP było, że poczta wchodząca była odbierana przez pracowników Referatu ds. Informatyzacji Urzędu, następnie drukowana i przekazywana do kancelarii w celu rejestracji i dekretacji do

[3] Z dniem 31 maja 2012 r.

[4] Dz. U. z 2011 r. Nr 14, poz. 67, ze zm.

[5] § 22 pkt 24 Zarządzenia Prezydenta Nr 486/2013 z dnia 30 grudnia 2013 r.

[6] Elektroniczna Platforma Usług Administracji Publicznej.

właściwej komórki. Dalszy obieg dokumentu następował w formie papierowej. Również korespondencja wychodząca wysyłana była przez pracowników Referatu ds. Informatyzacji Urzędu.

(dowód: akta kontroli str. 342-350)

1.6. W kontrolowanym okresie złożono w Urzędzie łącznie 303.131 dokumentów (wniosków, podań) w formie papierowej. Na przykładzie miesiąca kwietnia 2014 r. ustalono, że spośród złożonych łącznie 11.592 dokumentów w formie papierowej, obywatele złożyli 6.199, podmioty gospodarcze 1.906, a urzędy 3.487.
Urząd w tym samym okresie, w formie papierowej, wysłał 122.367 dokumentów.
W kontrolowanym okresie złożono w Urzędzie łącznie 436 dokumentów w formie elektronicznej. Obywatele złożyli łącznie 12 dokumentów, podmioty gospodarcze 5, a inne urzędy 419 dokumentów w tej postaci.
Urząd w tym samym okresie, w formie elektronicznej, wysłał 422 dokumenty, z czego 13 do obywateli, a 5 do podmiotów gospodarczych.

(dowód: akta kontroli str. 248-254)

1.7. Według stanu na dzień 31 maja 2012 r. i 31 maja 2014 r. Urząd świadczył jedną usługę elektroniczną („Skargi, wnioski, zapytania do urzędu"), która realizowana była za pośrednictwem platformy ePUAP. Informacje dot. ww. usługi, zawarte na portalu ePUAP, były zgodne i aktualne z usługą faktycznie świadczoną przez Urząd.
Dodatkowo Urząd świadczył w okresie objętym kontrolą:

- usługę informacyjną - na stronie www.leszno.pl - formularz „Zadaj pytanie Prezydentowi", który umożliwiał elektroniczne zadawanie pytań;
- usługę informacyjną - na stronie http://www.konsultacje.leszno.pl - usługa dotyczyła wyrażenia opinii na temat projektów aktów prawa miejscowego, strategii, programów współpracy i innych spraw dotyczących Miasta Leszna;
- usługę informacyjną - na stronie www.leszno.pl - elektroniczny nabór do szkół ponadgimnazjalnych, stanowiącą bazę informacji o przebiegu rekrutacji do szkół ponadgimnazjalnych;
- usługę dedykowaną - na stronie Geoportal Miasta Leszna - usługa iKerg (obsługa geodetów online) - dedykowana dla geodetów w zakresie przygotowania materiałów do prac geodezyjnych (zgłoszenie robót - po zgłoszeniu system generuje dokumenty, które geodeci mogą pobrać).

Były to usługi nie przeznaczone do wnoszenia podań i wniosków.

(dowód: akta kontroli str. 255-259, 294-301, 342-350)

1.8. Urząd opublikował na stronie Biuletynu Informacji Publicznej Miasta Leszna (dalej: BIP) informacje o usłudze świadczonej za pomocą platformy ePUAP. Dane tam zawarte nie obejmowały: podstawy prawnej świadczenia usługi i komórki odpowiedzialnej za załatwienie sprawy.

(dowód: akta kontroli str. 255-259)

1.9. Zgodnie z art. 19b ust. 3 ustawy z dnia 17 lutego 2005 r. o informatyzacji działalności podmiotów realizujących zadania publiczne[7] organy administracji publicznej przekazują do centralnego repozytorium oraz udostępniają w Biuletynie Informacji Publicznej wzory dokumentów elektronicznych.
W odniesieniu do usługi „Skargi, wnioski, zapytania do urzędu" Urząd nie przekazał wzoru dokumentu elektronicznego do Centralnego Repozytorium Dokumentów (dalej: CRD) ponieważ do świadczenia tej usługi wykorzystano wzór formularza zamieszczony wcześniej w CRD.

(dowód: akta kontroli str. 342-350)

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

1.10. W przypadku usługi „Skargi, wnioski, zapytania do Urzędu" nie stworzono karty opisu usługi elektronicznej.

(dowód: akta kontroli str. 255-259, 294-299, 342-350)

1.11. Zakres współpracy systemów IT działających wewnątrz Urzędu zbadano na przykładzie trzech systemów, których zakup miał miejsce po 31 maja 2012 r., tj.:

- Geo-Info iAdres; służący do prowadzenia bazy danych Ewidencji Miejscowości, Ulic i Adresów; zakup w dniu 21 grudnia 2012 r. - program wdrożony;
- Geo-Info iZamówienie; aplikacja przeznaczona do sprzedaży map przez internet; zakup w dniu 21 grudnia 2012 r. - planowane pełne wdrożenie we wrześniu 2014 r.;
- iDotacje; aplikacja internetowa wraz z hostingiem, służąca do gromadzenia i przechowywania danych na temat podległych jednostek oświatowe danych oraz naliczania przysługujących im dotacji; zakup w dniu 29 listopada 2013 r. - planowane pełne wdrożenie we wrześniu 2014 r.

Program Geo-Info iAdres stanowi moduł aplikacji Geo-Info Integra. Aplikacja iAdres zawiera bazę adresową Miasta Leszna. Dane z modułu iAdres przekazywane są automatycznie do innego modułu aplikacji Geo-Info Integra - Mapa. W module tym pojawia się informacja o zaimportowaniu danych i na mapie pojawia się punkt adresowy (ulica i numer). Inne systemy nie korzystają z danych wprowadzanych w programie Geo-Info iAdres. Moduł iAdres jako część składowa Geo-Info umożliwiał także zapis danych wyjściowych w formacie *.pdf, *.swde i *.xls.

Aplikacja iZamówienie stanowi także moduł aplikacji Geo-Info Integra, z której to może pobierać dane na poziomie dwustronnej komunikacji[8]. Program iDotacje jest programem autonomicznym, nie odwołującym się do innych rejestrów danych (pozwala na generowania raportów zewnętrznych w postaci plików *.xls).

W ocenie NIK wdrożony system informatyczny Geo-Info iAdres spełniał minimalne wymogi interoperacyjności w zakresie współpracy z innymi systemami Urzędu, określone w § 5 ust. 3 pkt 1 i 2 rozporządzenia w sprawie KRI. Pozostałe dwa systemy, ze względu na brak pełnego wdrożenia (Geo-Info iZamówienie; iDotacje), nie mogły podlegać ocenie w zakresie współpracy, o której mowa w § 5 ust. 3 pkt 1 i 2 rozporządzenia w sprawie KRI.

(dowód: akta kontroli str. 200-203, 205-228, 255-259, 339)

1.12. W Urzędzie nie wprowadzono procedur dotyczących współpracy z innymi jednostkami administracji publicznej. Dokumenty w formie elektronicznej do innych instytucji publicznych przesyłane były:

- za pośrednictwem platformy ePUAP:
  - jako odpowiedzi do spraw wpływających za pośrednictwem Elektronicznej Skrzynki Podawczej,
  - sprawozdania Rb-27ZZ, Rb-50 i Rb-ZN do Wielkopolskiego Urzędu Wojewódzkiego, przesyłane były w formie arkusza kalkulacyjnego (*.xlsx),
  - pliki aktualizacyjne z lokalnej Ewidencji Ludności - do Wielkopolskiego Urzędu Wojewódzkiego - generowane z programu do obsługi Ewidencji Ludności i przekazywane w formacie tekstowym. W takim samym formacie przekazywane były odpowiedzi z Wielkopolskiego Urzędu Wojewódzkiego, które następnie importowane były do programu do obsługi Ewidencji Ludności (jednostronna komunikacja).
- za pośrednictwem aplikacji Legislator - przekazywano akty normatywne do Dzienników Urzędowych Województwa Wielkopolskiego. Dane te przekazywane były w formacie *.xml.

[8] Dane z jednego systemu informatycznego przekazywane są do innego systemu.

Urząd nie zwracał się do innych jednostek z wnioskiem o prowadzenie komunikacji wyłącznie w formie elektronicznej. Również do Urzędu nie zwrócił się inny organ administracji publicznej z wnioskiem o prowadzenie komunikacji wyłącznie w formie elektronicznej.

(dowód: akta kontroli str. 255-259, 342-350)

Uwagi dotyczące badanej działalności

1. W przypadku usługi „Skargi, wnioski, zapytania do urzędu" Urząd opublikował na stronie BIP niepełne informacje o ww. usłudze. Dane te nie obejmowały m.in.: podstawy prawnej świadczenia usługi oraz komórki odpowiedzialnej za załatwienie sprawy. Zdaniem NIK, zamieszczenie powyższych danych, dotyczących usługi elektronicznej świadczonej za pomocą ePUAP na stronie BIP, niewątpliwie ułatwiłoby obywatelom korzystanie z tej usługi elektronicznej i mogłoby zwiększyć jej wykorzystanie.

2. Ustalenia kontroli NIK wykazały, że usługa „Skargi, wnioski, zapytania do urzędu" wspierała model usługowy[9] w podstawowym zakresie, o którym mowa w § 2 pkt 8 rozporządzenia w sprawie KRI.

Nie stworzono karty opisu usługi elektronicznej świadczonej drogą elektroniczną. Brak było wskazania maksymalnego czasu niedostępności usługi, sposobu zgłaszania awarii, wskazania osób (komórki) odpowiedzialnej za usuwanie awarii, technicznego właściciela usługi, nie określono również dopuszczalnych okresów niedostępności usługi elektronicznej. Zdaniem NIK dla zapewnienia sprawnego zarządzania usługą, celowym jest aby opracować taką kartę, zawierającą wskazane wyżej dane. (dowód: akta kontroli str. 255-259, 294-299, 342-350)

3. Zdaniem NIK udostępnienie tylko jednej pełnej usługi za pośrednictwem systemu teleinformatycznego świadczy o niedostatecznym poziomie rozwoju w Urzędzie e-administracji. NIK zwraca uwagę na potrzebę zintensyfikowanie działań w tym zakresie, tak aby w miarę możliwości zwiększać liczbę świadczonych usług elektronicznych, w szczególności takich, które wynikają z potrzeb mieszkańców np. wniosku o dopisanie do spisu wyborców.

4. NIK zwraca uwagę na długi okres wdrożenia do pełnej funkcjonalności programu Geo-Info iZamówienie. Zakupu dokonano w grudniu 2012 r., a pełne wdrożenie wszystkich jego funkcjonalności nastąpi dopiero we wrześniu 2014 r.

Jak wyjaśnił Sekretarz Miasta, ze względu na równoległe wdrażanie modułu iAdres programu Geo-Info, moduł iZamówienie w 2013 r. był testowany, a dla użytkowników zewnętrznych udostępniony w ograniczonej funkcjonalności. Po wprowadzeniu płatności elektronicznych proces zamówienia będzie odbywał się w całości za pośrednictwem aplikacji. Dodatkowo Sekretarz Miasta wyjaśnił, że oba moduły były zakupione w ramach jednego postępowania, co zmniejszyło koszty związane z zakupem i późniejszym wdrożeniem.

W toku kontroli, dnia 11 lipca 2014 r., Urząd podpisał umowę dotyczącą realizacji płatności elektronicznych.

(dowód: akta kontroli str. 203-210, 229-238)

[9]Zgodnie z definicją zawartą w § 2 pkt 8 rozporządzenia KRI, model usługowy jest modelem architektury systemu teleinformatycznego, w którym dla użytkowników zdefiniowano stanowiące odrębną całość funkcje systemu teleinformatycznego (usługi sieciowe) oraz opisano sposób korzystania z tych funkcji. Na potrzeby niniejszej kontroli przyjęto, że model usługowy powinien spełniać do najmniej poniższe warunki: a) można zidentyfikować właściciela poszczególnych usług świadczonych przez Urząd (jednostkę organizacyjną i konkretną osobę oraz ewentualnie osoby odpowiedzialne za realizację poszczególnych elementów świadczonej usługi), b) istnieją karty opisu usługi oraz następuje ich aktualizacja, c) w opisie usługi wskazany jest maksymalny czas jej niedostępności, sposób zgłaszania awarii, osoby/komórki/podmioty odpowiedzialne za usuwanie awarii, techniczny właściciel usługi, d) określone zostały dopuszczalne okresy niedostępności usługi elektronicznej.

Ocena cząstkowa

W ocenie NIK, w Urzędzie podjęto właściwe działania w zakresie wprowadzania systemów teleinformatycznych gotowych do współpracy z innymi systemami wewnątrz jednostki. Rozszerzany był zakres prowadzenia komunikacji w formie elektronicznej m.in. z Wielkopolskim Urzędem Wojewódzkim. Promowano także elektroniczną komunikację z Urzędem. Ustalenia kontroli dały jednak podstawę do sformułowania przedstawionych wyżej uwag dot. kontrolowanej działalności.

2. Wdrożenie systemu zarządzania bezpieczeństwem systemów informatycznych

Opis stanu faktycznego

2.1. Urząd posiadał opracowaną i wdrożoną do stosowania Politykę Bezpieczeństwa Informacji w zakresie przetwarzania danych osobowych (dalej: PBI), Instrukcję Zarządzania Systemami Informatycznymi w zakresie wymogów bezpieczeństwa przetwarzania danych osobowych (dalej: IZSI) oraz Instrukcję Postępowania w sytuacji naruszenia systemu ochrony danych osobowych (dalej: IPNDO), ustanowione i zatwierdzone przez Prezydenta[10]. Z § 6 PBI wynikało, że zakresy określone przez dokumenty PBI mają zastosowanie do całego systemu informacyjnego Urzędu, w tym systemów informatycznych, w których przetwarzane są informacje podlegające ochronie. Polityka ta posiadała ustalonego właściciela. Wymienione regulacje zostały wdrożone w związku z ustawą z dnia 29 sierpnia 1997 r. o ochronie danych osobowych[11] oraz rozporządzeniem Ministra Spraw Wewnętrznych i Administracji z dnia 29 kwietnia 2004 r. w sprawie dokumentacji przetwarzania danych osobowych oraz warunków technicznych i organizacyjnych, jakim powinny odpowiadać urządzenia i systemy informatyczne służące do przetwarzania danych osobowych[12]. Od daty wejścia w życie PBI, IZSI i IPNDO tj. 1 września 2006 r. nie były one aktualizowane**.**

(dowód: akta kontroli str. 28-72, 342-350)

2.2. Zgodnie z § 20 ust. 2 pkt 14 rozporządzenia w sprawie KRI, zarządzanie bezpieczeństwem informacji realizowane jest m.in. poprzez zapewnienie przez kierownictwo podmiotu publicznego warunków umożliwiających realizację i egzekwowanie działania polegającego na okresowym audycie wewnętrznym w zakresie bezpieczeństwa informacji, nie rzadziej niż raz na rok. W Urzędzie nie przeprowadzono okresowego audytu wewnętrznego i zewnętrznego z zakresu bezpieczeństwa informacji. Nie przeprowadzono także okresowych analiz ryzyka utraty integralności, poufności lub dostępności informacji.

(dowód: akta kontroli str. 28-72, 342-350)

2.3. Urząd posiadał pełną wiedzę o konfiguracji sprzętowej oraz zainstalowanym oprogramowaniu na badanych urządzeniach. Inwentaryzacja[13] zasobów informatycznych Urzędu była realizowana bez wykorzystywania specjalistycznego oprogramowania komputerowego. Karty sprzętu informatycznego (prowadzone w Referacie ds. informatyzacji Urzędu) zawierały informację o jego rodzaju, konfiguracji i użytkownikach.

W trakcie oględzin (na 10 komputerach Urzędu oraz pięciu komputerach, które Urząd otrzymał z Ministerstwa Spraw Wewnętrznych i Administracji w ramach projektu „pl.ID - Polska ID karta") stwierdzono, że nie było możliwości zainstalowania na ww. komputerach dowolnego oprogramowania przez

[10] Stanowiące załączniki odpowiednio nr 1-3 do Zarządzenia Prezydenta Nr 297/2006 z dnia 26 sierpnia 2006 r.

[11] Dz. U. z 2002 r. Nr 101 poz. 926 ze zm.

[12] Dz. U. z 2004 r. Nr 100 poz. 1024 ze zm.

[13] W rozumieniu posiadania aktualnych informacji w zakresie posiadanego sprzętu informatycznego, oprogramowania, konfiguracji i miejsca użytkowania.

użytkowników tych komputerów niebędących pracownikami służb informatycznych Urzędu.
Ponadto, zgodnie z § 71 IZSI, zabroniono pracownikom Urzędu samodzielnego instalowania jakiegokolwiek oprogramowania.
(dowód: akta kontroli str. 28-79, 255-259, 302-312, 324-327)
W trakcie kontroli dokonano przeglądu uprawnień do systemów i zasobów informatycznych dla 15 losowo wybranych pracowników Urzędu. Stwierdzono, że posiadali oni stosowne uprawnienia adekwatne do realizowanych zadań, co było zgodne z § 20 ust. 2 pkt 4 rozporządzenia w sprawie KRI. W Urzędzie wprowadzono procedurę regulującą zarządzanie uprawnieniami w systemach informatycznych, co spełniało wymogi § 20 ust. 2 pkt 4 i 5 tego rozporządzenia. W trakcie kontroli NIK dokonano sprawdzenia zablokowania dostępu do systemów IT Urzędu dla 10 byłych pracowników, którzy zakończyli pracę w Urzędzie w kontrolowanym okresie oraz dodatkowo mających aktualnie dostęp do aplikacji iDotacje oraz Geo-Info.
W jednym przypadku konto użytkownika systemu Geo-Info do dnia 5 sierpnia 2014 r. nie zostało zablokowane, pomimo, że konto zostało przypisane do osoby nie będącej pracownikiem Urzędu od dnia 13 lipca 2013 r.
(dowód: akta kontroli str. 28-72, 157-182, 255-259, 328-336)
2.4. W kontrolowanym okresie, stosownie do § 20 ust. 2 pkt 6 rozporządzenia w sprawie KRI, Urząd zapewnił szkolenia wszystkich osób zaangażowanych w proces przetwarzania informacji. Zakres tematyczny tych szkoleń obejmował politykę bezpieczeństwa informacji stosowaną w Urzędzie (tj. zagrożenia bezpieczeństwa informacji) i obowiązujące w Urzędzie regulaminy i procedury (obowiązujące na danym stanowisku).
(dowód: akta kontroli str. 157-171, 340-341)
2.5. Procedura dotycząca korzystania z urządzeń mobilnych zawarta została w IZSI, co było zgodne § 20 ust. 2 pkt 8 rozporządzenia w sprawie KRI. Użytkownicy zostali zapoznani z tą instrukcją i zobowiązani do jej stosowania.
(dowód: akta kontroli str. 28-72)
2.6. W stosunku do badanych systemów IT: w umowie nadzoru z dnia 10 kwietnia 2014 r. dotyczącej aplikacji Geo-Info (aplikacje iZamówienie oraz iAdres) oraz umowie na usługę hostingu oraz licencji na korzystanie z aplikacji internetowej iDotacje z 29 listopada 2013 r. zawarto zapisy mówiące o zobowiązaniu firm zewnętrznych do zachowania wymogów ustawy o ochronie danych osobowych oraz wcześniej przywołanego rozporządzenia Ministra Spraw Wewnętrznych i Administracji z dnia 29 kwietnia 2004 r.
Urząd po 31 maja 2012 r. (tj. po wejściu w życie rozporządzenia w sprawie KRI) zawarł dwie umowy dotyczące zakupu komputerów. W umowach lub stanowiących ich integralną część załącznikach zawarto zapisy, że dyski twarde lub inne nośniki danych nie podlegają wydaniu na zewnątrz, a uszkodzone będą wymieniane na nowe bez konieczności zwrotu uszkodzonych.
(dowód: akta kontroli str. 82-136, 205-228)
2.7. W Urzędzie w 2006 r. opracowano i wdrożono IPNDO. Z dokumentem zostali zapoznani pracownicy Urzędu. W okresie objętym kontrolą nie wystąpiły przypadki zgłaszania incydentów naruszenia bezpieczeństwa informacji.
Zgodnie z wyjaśnieniami Sekretarza Miasta, instrukcja będzie aktualizowana w ramach wdrożenia w 2014 r. Systemu Zarządzania Bezpieczeństwem Informacji.
(dowód: akta kontroli str. 342-350)
2.8. Obowiązek tworzenia i przechowywania kopii zapasowych baz danych, a także częstotliwość ich wykonywania określono w IZSI. Kopie zapasowe były sporządzane raz dziennie (w dni robocze). Kopie zapasowe danych były jednocześnie zapisywane i przechowywane na odrębnych nośnikach, zainstalowanych w czterech serwerowniach. Kopie te były testowane. Przynajmniej jedna kopia danych była

przechowywana poza miejscem wytworzenia danych. Pomieszczenia serwerowni zlokalizowane były w dwóch odrębnych budynkach Urzędu, co minimalizowało ryzyko utraty informacji w wyniku awarii. Pomieszczenia te były prawidłowo zabezpieczone, zgodnie z § 20 ust. 2 pkt 12 lit. b rozporządzenia w sprawie KRI.

(dowód: akta kontroli str. 255-259, 313-323)

2.9. Badane systemy informatyczne umożliwiały zapis danych wyjściowych w następujących formatach:

- program iDotacje umożliwiał zapis danych wyjściowych w formacie *.xls;
- program iZamówienie umożliwiał zapis danych wyjściowych w formacie *.pdf;
- program iAdres jako część składowa Geo-Info umożliwiał zapis danych wyjściowych w formacie *.pdf, *.swde i *.xls.

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

(dowód: akta kontroli str. 339)

Ustalone nieprawidłowości

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

1. W Urzędzie nie aktualizowano PBI, IZSI i IPNDO od momentu ich wejścia w życie tj. dnia 1 września 2006 r. Tylko z § 6 PBI wynikało, że zakresy określone przez dokumenty PBI mają zastosowanie do całego systemu informacyjnego Urzędu, w tym systemów informatycznych. Zauważyć należy, że w myśl § 20 ust. 3 ww. rozporządzenia, wymagania w zakresie systemu zarządzania bezpieczeństwem informacji uznaje się za spełnione jeżeli został on opracowany na podstawie Polskiej Normy: PN-ISO/IEC 27001:2007 *Technika informatyczna. Techniki bezpieczeństwa. Systemy zarządzania bezpieczeństwem informacji* oraz powiązanej z nią Polskiej Normy PN-ISO/IEC 17799:2007 *Technika informatyczna. Techniki bezpieczeństwa. Praktyczne zasady zarządzania bezpieczeństwem informacji.* Wspomniane wyżej normy zostały opublikowane w 2007 r., a więc nie mogły stanowić podstawy opracowania PBI, IZSI i IPNDO.
2. Zgodnie z § 20 ust. 2 pkt 14 rozporządzenia w sprawie KRI, zarządzanie bezpieczeństwem informacji realizowane jest m.in. poprzez zapewnienie przez kierownictwo podmiotu publicznego warunków umożliwiających realizację i egzekwowanie działania polegającego na okresowym audycie wewnętrznym w zakresie bezpieczeństwa informacji, nie rzadziej niż raz na rok[14]. W Urzędzie takich audytów nie przeprowadzano.
3. Zgodnie z § 20 ust. 2 pkt 3 rozporządzenia w sprawie KRI podmiot realizujący zadania publiczne ma obowiązek przeprowadzania okresowych analiz ryzyka utraty integralności, dostępności lub poufności informacji oraz podejmowania działań minimalizujących to ryzyko, stosownie do wyników przeprowadzonych analiz. W Urzędzie nie przeprowadzano tych analiz.

Jak wyjaśnił Sekretarz Miasta Leszna, aktualizacja Polityki Bezpieczeństwa Informacji, audyt oraz wymienione wyżej analizy zostaną wykonane w roku bieżącym. W Urzędzie zaplanowane jest bowiem wykonanie zadania „Opracowania i wdrożenie Systemu Zarządzania Bezpieczeństwem Informacji oraz systemu

[14] Zgodnie ze wspólnym stanowiskiem Departamentu Informatyzacji Ministerstwa Administracji i Cyfryzacji oraz Departamentu Audytu Sektora Finansów Publicznych Ministerstwa Finansów odnośnie zapewnienia audytu wewnętrznego w zakresie bezpieczeństwa informacji (dostępnym na stronie http://www.mf.gov.pl/ministerstwo-finansow/wiadomosci/aktualnosci/-asset_publisher/M1vU/content/id/3812517) obowiązek ten dotyczy jednostek, które nie wdrożyły SZBI, zgodnie z normami wskazanymi w § 20 ust. 3 rozporządzenia w sprawie KRI, a audyt wewnętrzny nie musi być wykonywany przez audytora wewnętrznego, lecz przez osobę/komórkę charakteryzującą się odpowiednimi kwalifikacjami, doświadczeniem, znajomością metodyki audytu w zakresie bezpieczeństwa informacji, a także niezależnością od obszaru audytowanego.

zarządzania usługami IT w Urzędzie Miasta Leszna." Wdrożenie zostanie wykonane do dnia 14 listopada 2014 r. i zakłada dostosowanie systemów i procedur Urzędu do wymagań stawianych w rozporządzeniu w sprawie KRI.
W toku kontroli, w dniu 31 lipca 2014 r., wysłano zapytanie ofertowe do potencjalnych wykonawców, dotyczące wymienionych wyżej zadań. Elementy zapytania obejmowały aktualizację dokumentacji dotyczącej przetwarzania danych, w tym Polityki Bezpieczeństwa Informacji, audyt z zakresu bezpieczeństwa informacji oraz analizę ryzyka utraty integralności, poufności lub dostępności informacji.

(dowód: akta kontroli str. 28-72, 188-199, 342-350)

4. W umowie nadzoru z dnia 10 kwietnia 2014 r. dotyczącej aplikacji Geo-Info (aplikacje iZamówienie oraz iAdres) nie zawarto zapisów gwarantujących odpowiedni poziom bezpieczeństwa informacji, o czym mowa w § 20 ust. 2 pkt 10 rozporządzenia w sprawie KRI. W umowie tej zagwarantowano wyłącznie ochronę danych osobowych, ale nie zagwarantowano bezpieczeństwa wszystkich innych ogólnie niedostępnych informacji przetwarzanych w tych systemach (np. danych uzyskanych z systemów komputerowych Urzędu zarówno w czasie trwania umowy, jak również po jej wygaśnięciu) oraz nieudostępniania ich osobom trzecim.

(dowód: akta kontroli str. 82-136, 205-228)

5. W jednym przypadku konto użytkownika systemu Geo-Info do dnia 5 sierpnia 2014 r. nie zostało zablokowane, pomimo, że konto zostało przypisane do osoby nie będącej pracownikiem Urzędu od dnia 13 lipca 2013 r. Było to niezgodne z § 20 ust. 2 pkt 5 rozporządzenia KRI, w myśl którego zarządzanie bezpieczeństwem informacji realizowane jest w szczególności poprzez bezzwłoczną zmianę uprawnień w przypadku zmiany zadań pracowników. Jak podał Kierownik referatu ds. informatyzacji przyczyną powyższego był brak dostarczenia do referatu *Karty obiegowej rozliczenia pracownika w związku z ustaniem stosunku pracy*, spowodowany jego zgonem.

(dowód: akta kontroli str. 28-72, 157-182, 255-259, 328-336)

Ocena cząstkowa

Najwyższa Izba Kontroli ocenia, że Prezydent wywiązał się z realizacji przepisów rozporządzenia w sprawie KRI w części. Właściwie przechowywano i zabezpieczono kopie zapasowe danych, zinwentaryzowano posiadany sprzęt informatyczny oraz wykluczono możliwość nadawania uprawnień administracyjnych pracownikom Urzędu. Naruszenie obowiązujących przepisów stanowiło jednak niezaktualizowanie PBI, IZSI i IPNDO oraz niedokonywanie audytu bezpieczeństwa informacji.

3. Zapewnienie dostępności informacji dla osób niepełnosprawnych

Opis stanu faktycznego

W toku kontroli dokonano weryfikacji zgodności strony internetowej Urzędu[15] oraz strony BIP Urzędu[16] ze standardem WCAG 2.0. Ustalono, iż żadna ze stron Urzędu nie spełniała jeszcze w pełni wymagań określonych w § 19 rozporządzenia w sprawie KRI dotyczących dostosowania systemów prezentujących treści do wymagań WCAG 2.0[17].
Strona internetowa www.leszno.pl posiadała funkcję powiększania czcionek umożliwiającą zapoznanie się z zawartością strony osobom słabowidzącym.

[15] www.leszno.pl

[16] www.bip.leszno.pl

[17] Co powinno nastąpić nie później niż w terminie 3 lat od wejścia w życie tego rozporządzenia, tj. do dnia 31 maja 2015 r.

Dodatkowo możliwe było odsłuchanie zamieszczanych tam wiadomości. Strona www.bip.leszno.pl nie posiadała funkcji ułatwiających korzystanie ze strony osobom niepełnosprawnym.

(dowód: akta kontroli str. 260-299)

W wyniku ww. weryfikacji ustalono, że na stronie internetowej Urzędu wystąpiło 26 błędów stwierdzonych przy badaniu z wykorzystaniem narzędzia dostępnego na stronie http://jigsaw.w3.org/css-validator/ oraz 13 błędów stwierdzonych z wykorzystaniem narzędzia dostępnego na stronie http://validator.w3.org/. Na stronie bip.leszno.pl wystąpiły 4 błędy stwierdzone przy badaniu z wykorzystaniem narzędzia dostępnego na stronie http://jigsaw.w3.org/css-validator/ oraz 29 błędów stwierdzonych z wykorzystaniem narzędzia dostępnego na stronie http://validator.w3.org/.

(dowód: akta kontroli str. 260-293)

Zgodnie z treścią wyjaśnień Sekretarza Miasta, w roku 2015 planowana jest wymiana stron Biuletynu Informacji Publicznej i w konsekwencji wprowadzenie udogodnień dla osób niepełnosprawnych.

(dowód: akta kontroli str. 342-350)

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[18], wnosi o podjęcie działań mających na celu:

1. Aktualizację regulacji wewnętrznych dotyczących systemu zarządzania bezpieczeństwem informacji, przeprowadzenie audytu z zakresu bezpieczeństwa informacji oraz analiz ryzyka utraty integralności, poufności lub dostępności informacji.
2. Zapewnienie w treściach umów podpisywanych przez Miasto Leszno zapisów gwarantujących bezpieczeństwo wszystkich informacji przetwarzanych w systemach komputerowych Urzędu.

V. Pozostałe informacje i pouczenia

Prawo zgłoszenia zastrzeżeń

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

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

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.

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

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.

Poznań, dnia 5 września 2014 r.

Najwyższa Izba Kontroli
Delegatura w Poznaniu

Kontroler Piotr Białka gł. specjalista k. p.	Dyrektor z up. Tomasz Nowiński Wicedyrektor
.....	.....
Podpis	*podpis*