NAJWYŻSZA IZBA KONTROLI
Delegatura w Poznaniu

LPO – 4101-012-01/2014
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

Maria Wojcińska, starszy inspektor kontroli państwowej, upoważnienie do kontroli nr 90971 z 25 czerwca 2014 r.

(dowód: akta kontroli str. 1-2)

Jednostka kontrolowana

Urząd Miasta w Luboniu, pl. Edmunda Bojanowskiego 2, 62-030 Luboń (dalej: Urząd)

Kierownik jednostki kontrolowanej

Dariusz Szmyt, Burmistrz Miasta Lubonia (dalej: Burmistrz)

(dowód: akta kontroli str. 3)

II. Ocena kontrolowanej działalności

Ocena ogólna

Burmistrz Miasta Luboń[1] w okresie od 31 maja 2012 r. do 25 lipca 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):

- zapewniał 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,
- zapewniał regularne tworzenie kopii zapasowych danych.

Stwierdzono również, że w badanym okresie zwiększyła się liczba spraw możliwych do załatwienia drogą elektroniczną z wykorzystaniem elektronicznej platformy usług administracji publicznej (dalej: ePUAP).

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

- nienależycie zrealizowano wymagania określone w § 20 ust. 3 rozporządzenia w sprawie KRI, gdyż nie opracowano i nie wdrożono Polityki Bezpieczeństwa Informacji (dalej: PBI),

[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.

- niewłaściwie przechowywano i zabezpieczano kopie zapasowe danych, czym naruszono przepisy § 20 ust. 2 pkt 12 lit. b i e rozporządzenia w sprawie KRI,
- nie zapewniono szkoleń osób zaangażowanych w proces przetwarzania informacji, co było niezgodne z § 20 ust. 2 pkt 6 rozporządzenia w sprawie KRI,
- nadano uprawnienia administracyjne pracownikom Urzędu, niebędącym pracownikami służb informatycznych, w związku z czym mogli oni samodzielnie instalować oprogramowanie na komputerach służbowych, co stało w sprzeczności z zapisami normy PN-ISO/IEC 27001:2007, załącznik A, punkt A.11.2.2 pkt b[3],
- nie zamieszczono w centralnym repozytorium wzorów formularzy dotyczących trzech usług świadczonych przez portal ePUAP.

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

W Strategii Rozwoju Miasta Luboń na lata 2007-2018[4] w rozdziale dotyczącym programów i projektów strategicznych wskazano, że władze samorządowe planują organizację projektu pod roboczą nazwą e-Luboń. Jego realizacja miała opierać się na zapewnieniu powszechnego bezprzewodowego dostępu do Internetu na terenie miasta oraz kompleksowej informatyzacji instytucji publicznych. W zaktualizowanej Strategii[5] w części dotyczącej monitoringu wykonania zadań wskazano, że nie dokonano opracowania koncepcji informatyzacji miasta Lubonia i instytucji publicznych. Burmistrz wyjaśnił, że nie znalazła ona uzasadnienia technicznego i finansowego. Zapisano natomiast nowe zadanie, tj. poprawę jakości obsługi mieszkańców przez administrację publiczną - realizowane m.in. poprzez rozwijanie i propagowanie możliwości załatwienia sprawy przez internet.

(dowód: akta kontroli str. 5-13, 295, 297)

W Urzędzie nie opracowano programu promocji komunikacji elektronicznej, jednakże Burmistrz podejmował działania w tym kierunku, m.in. zobowiązując pracowników do uzyskania profilu zaufanego na portalu ePUAP, udostępniając na nim 17 usług świadczonych przez Urząd drogą elektroniczną, a także publikując adresy elektroniczne pracowników Urzędu na stronie internetowej miasta i BIP. Burmistrz uruchomił także na stronie internetowej Urzędu zakładkę[6], gdzie można było zadać mu pytanie dotyczące sprawy związanej z funkcjonowaniem miasta.

(dowód: akta kontroli str. 295, 297-298)

W Urzędzie nie rozpoznawano potrzeb korzystania przez mieszkańców gminy z elektronicznej formy komunikacji przy załatwianiu spraw. Ankiety badania satysfakcji interesanta wskazywały natomiast pośrednio na korzystanie przez

[3] Wymagania w zakresie zarządzania bezpieczeństwem informacji uznaje się za spełnione, jeżeli system zarządzania bezpieczeństwem informacji został opracowany na podstawie Polskiej Normy PN-ISO/IEC 27001 (§ 20 ust. 3 rozporządzenia w sprawie KRI).

[4] Uchwała nr XXIV/132/2008 Rady Miasta Luboń z 15 października 2008 r. w sprawie przyjęcia Strategii Rozwoju Miasta Luboń na lata 2008-2017.

[5] Uchwała nr XXXI/190/2013 Rady Miasta Luboń z 25 kwietnia 2013 r. w sprawie przyjęcia „Strategii Rozwoju Miasta Luboń na lata 2008-2017".

[6] Zakładka pod nazwą: MASZ SPRAWĘ – ZADAJ PYTANIE BURMISTRZOWI.

mieszkańców ze stron internetowych miasta (np. przy zapoznawaniu się z materiałami informacyjnymi dotyczącymi załatwianej sprawy).

(dowód: akta kontroli str. 295, 298)

Po wejściu w życie rozporządzenia w sprawie KRI[7], Burmistrz 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. 295-296, 298)

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[8].

Zgodnie z § 1 Zarządzenia Burmistrza Miasta Luboń z 20 stycznia 2011 r. w sprawie podstawowego sposobu dokumentowania spraw w Urzędzie Miasta Luboń, powołania koordynatora czynności kancelaryjnych oraz określenia listy rodzajów przesyłek wpływających, które nie są otwierane przez punkt kancelaryjny[9], podstawowym sposobem dokumentowania przebiegu załatwiania i rozstrzygania spraw w Urzędzie był system tradycyjny. W związku z powyższym nie opracowano procedur dotyczących obiegu i zarządzania dokumentami regulujących komunikację elektroniczną w Urzędzie.

(dowód: akta kontroli str. 14-15, 164)

W Urzędzie był wykorzystywany system obsługi spraw i korespondencji e-SOS. Wpływające do jednostki dokumenty (za wyjątkiem faktur) nie były jednak skanowane i nie następował ich obieg elektroniczny. W przypadku wniesienia sprawy drogą tradycyjną następowało procedowanie sprawy w formie dokumentów papierowych, a system e-SOS służył pomocniczo do zamieszczania w nim dokumentów wytwarzanych przez pracowników (z możliwością podglądu i edycji przez przełożonych).

W przypadku wniesienia sprawy przez interesanta poprzez portal ePUAP bądź skrzynkę mailową - jeżeli sprawa nie wymagała rozpatrzenia w trybie przepisów ustawy z dnia 14 czerwca 1960 r. Kodeks postępowania administracyjnego[10] (dalej: KPA) - dokumentacja była drukowana i sprawę rozpatrywano tak, jak gdyby nastąpił wpływ pisma drogą tradycyjną. Odpowiedź udzielana była – w zależności od charakteru sprawy - poprzez użycie opcji „odpowiedz” (w systemie ePUAP lub poprzez skrzynkę mailową) bądź przez zeskanowanie odpowiedzi podpisanej przez uprawnioną osobę i wysłanie jej przez portal ePUAP lub jako wiadomość elektroniczną. W przypadku wniesienia sprawy poprzez skrzynkę mailową i konieczność jej procedowania w trybie przepisów KPA, sprawę rozpatrywano po otrzymaniu wniosku w wersji tradycyjnej lub poprzez portal ePUAP.

W Urzędzie testowano w maju i czerwcu 2014 r. dołączanie do systemu e-SOS wszystkich zeskanowanych pism i dokumentów, jednak wprowadzenie tej

[7] Z dniem 31 maja 2012 r.

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

[9] Nr 120.02.2011.

[10] Dz. U. z 2013 r., poz. 267, ze zm.

funkcjonalności będzie możliwe po wdrożeniu odpowiednich rozwiązań organizacyjnych.

(dowód: akta kontroli str. 165-166)

W okresie od 31 maja 2012 r. do 31 maja 2014 r. do Urzędu wpłynęło łącznie (tj. papierowo i elektronicznie) 75 927 dokumentów, z czego 42,13% zostało wniesionych przez obywateli, 27,62% przez podmioty gospodarcze i 30,25% przez inne urzędy. Najwięcej dokumentów drogą elektroniczną zostało złożonych przez inne urzędy[11]. W Urzędzie nie wydano drogą elektroniczną żadnej decyzji lub zaświadczenia; rozpatrzono w ten sposób trzy skargi i wnioski.

(dowód: akta kontroli str. 349)

Usługi elektroniczne Urzędu były świadczone z wykorzystaniem platformy ePUAP. Na stronie internetowej BIP Urzędu znajdowała się ogólna instrukcja dotycząca korzystania z Elektronicznej Skrzynki Podawczej, bez podziału na poszczególne usługi świadczone drogą elektroniczną. Szczegółowe informacje dotyczące miejsca świadczenia usług, sposobu ich realizacji (wymaganych dokumentów, opłat, terminów rozpatrzenia spraw, trybu odwoławczego) oraz podstawy prawnej były dostępne na stronie www.epuap.gov.pl.

(dowód: akta kontroli str. 294)

Na dzień 30 maja 2012 r. Urząd świadczył osiem, a na dzień rozpoczęcia czynności kontrolnych[12] – 17 usług elektronicznych. Szczegółowym badaniem w zakresie zgodności świadczonych przez Urząd usług z ich opisem zamieszczonym na stronie internetowej www.epuap.gov.pl objęto pięć usług, tj.:
- składanie deklaracji o wysokości opłaty za gospodarowanie odpadami komunalnymi,
- dopisanie do spisu wyborców,
- dokonanie wpisu żłobka lub klubu dziecięcego do rejestru żłobków i klubów dziecięcych,
- wydawanie zezwoleń na sprzedaż napojów alkoholowych,
- przyjmowanie wniosków i uwag do sporządzonego studium uwarunkowań i kierunków zagospodarowania przestrzennego.

Opisy wszystkich ww. usług (tj. miejsce i sposób realizacji) były zgodne z faktycznie świadczonymi. Stwierdzono podanie jednej nieaktualnej podstawy prawnej w przypadku usługi składania deklaracji o wysokości opłaty za gospodarowanie odpadami komunalnymi.

(dowód: akta kontroli str. 167-172, 178-197)

Zarządzanie usługami elektronicznymi nie odbywało się w oparciu o udokumentowane procedury. Działania jednostki w podstawowym zakresie wspierały model usługowy[13] w procesie świadczenia usług elektronicznych. W Urzędzie było możliwe zidentyfikowanie właścicieli świadczonych usług (tj. komórek organizacyjnych i konkretnego pracownika/pracowników odpowiedzialnych za realizację usług). W czterech na pięć badanych usług sporządzono wewnętrzne karty opisu usług, które były aktualizowane. W opisie wszystkich pięciu badanych usług nie wskazano maksymalnego ani dopuszczalnego czasu ich niedostępności, sposobu zgłaszania awarii oraz osób/komórek/podmiotów

[11] 91,17% wszystkich dokumentów, które wpłynęły do Urzędu drogą elektroniczną.

[12] Tj. 25 czerwca 2014 r.

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

odpowiedzialnych za usuwanie awarii, ze względu na fakt, że usługi są realizowane przez portal ePUAP, a Urząd nie ma możliwości technicznej ingerencji w jego funkcjonowanie.

(dowód: akta kontroli str. 178-197, 308, 312-313)

Stwierdzono, że w 14 na 17 przypadków Urząd do świadczenia własnych usług elektronicznych wykorzystał wzory usług zamieszczonych wcześniej w repozytorium ePUAP bądź udostępnionych na portalu Pojedynczy Punkt Kontaktowy.

(dowód: akta kontroli str. 175, 307, 310, 334-343)

Zakres współpracy[14] systemów informatycznych wewnątrz Urzędu zbadano w oparciu o dobór celowy czterech systemów, zakupionych lub zmodernizowanych po dacie wejścia w życie rozporządzenia w sprawie KRI. Ustalono, że:

- system POST+ (system naliczania podatków od środków transportu) – umożliwiał m.in. prowadzenie ewidencji podatników oraz naliczania dla nich podatków, rejestrację kart podatkowych pojazdów oraz deklaracji w zakresie podatku od środków transportu, jak również automatyczne naliczanie wysokości należnego podatku. System miał możliwość pobierania danych z systemu ELUD (System Ewidencji Ludności przeznaczony do obsługi lokalnego banku danych PESEL) oraz współpracował z systemem WIP+ (służącym księgowaniu i egzekwowaniu należności). Użytkownik systemu wprowadzając dane interesanta poprzez wpisanie numeru PESEL, automatycznie uzyskiwał podpowiedź w zakresie jego pozostałych danych,

- system ALK+ (obsługa zezwoleń na sprzedaż napojów alkoholowych) – umożliwiał m.in. prowadzenie ewidencji zezwoleń na sprzedaż napojów alkoholowych, rejestrację wniosków i zezwoleń, naliczanie opłat oraz drukowanie dokumentów związanych z prowadzoną ewidencją zezwoleń. System miał możliwość pobierania danych z systemu ELUD. Użytkownik systemu wprowadzając dane interesanta poprzez wpisanie numeru PESEL, automatycznie uzyskiwał podpowiedź w zakresie jego pozostałych danych,

- system GOK+ (obsługa gospodarki odpadami) – zawierał m.in. dane o nieruchomościach i ich właścicielach, kartoteki deklaracji i decyzji dotyczących opłat za gospodarowanie odpadami komunalnymi oraz informacje o przedsiębiorstwach prowadzących działalność w zakresie ich odbierania. System dzięki pobieraniu danych z systemów: ELUD i POGRUN + (System Naliczania Podatków od Gruntów i Nieruchomości) umożliwiał automatyczną rejestrację deklaracji i opłat na podstawie danych dotyczących mieszkańców i nieruchomości.

Powyższe systemy należy sklasyfikować jako działające na zasadzie jednostronnej komunikacji, tj. mające możliwość pobierania danych z innego systemu informatycznego z udziałem użytkowników systemu.

Kontrolą objęto również **system NABÓR**, wspomagający rekrutację do przedszkoli. Umożliwiał on rodzicom wypełnianie w wersji elektronicznej wniosku o przyjęcie

[14] Przyjęto możliwość wystąpienia jednego z pięciu poziomów współpracy: brak współpracy (interoperacyjności), informacyjny (użytkownicy systemu wiedzą, że są gromadzone dane i w razie potrzeby mogą z nich skorzystać), jednostronnej komunikacji, dwustronnej komunikacji oraz transakcyjny (wymiana danych pomiędzy systemami bez jakiegokolwiek pośrednictwa pracownika - przekazywanie danych odbywa się w sposób w pełni zautomatyzowany).

dziecka do przedszkola. Następnie należało go wydrukować i złożyć w wybranej placówce. Po zakończeniu rekrutacji, rodzice mogli sprawdzić w systemie (korzystając z nadanego indywidualnego numeru PIN), czy ich dziecko dostało się do wybranej jednostki.

System ten działał na zasadzie usługi informatycznej zakupionej od zewnętrznego podmiotu, w związku z tym nie był zainstalowany w środowisku informatycznym Urzędu. Gromadził on dane, z których pracownicy w razie potrzeby mogli skorzystać (np. poprzez wygenerowanie danych do pliku). Należy go więc sklasyfikować jako system informacyjny.

W ocenie NIK, badane systemy informatyczne POST+, ALK+ oraz GOK+ osiągnęły interoperacyjność[15] w zakresie współpracy z innymi systemami Urzędu, o której mowa w § 5 ust. 3 pkt 3 rozporządzenia w sprawie KRI.

(dowód: akta kontroli str. 173-174, 176-177, 217-220)

W zakresie współpracy systemów informatycznych Urzędu z systemami/rejestrami zewnętrznymi ustalono, że systemy Urzędu nie pobierają danych z innych systemów/rejestrów informatycznych np. PESEL, CEIDG. Burmistrz nie zwracał się do innych jednostek administracji publicznej z wnioskiem o prowadzenie wzajemnej korespondencji wyłącznie w formie elektronicznej. Z prośbą o zwiększenie wymiany informacji poprzez system ePUAP występował natomiast do gmin Wojewoda Wielkopolski (Urząd komunikuje się z Wojewodą zarówno papierowo, jak i przez portal ePUAP).

(dowód: akta kontroli str. 296, 298-299, 308, 313)

Ustalone nieprawidłowości

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

Zgodnie z art. 19b ust. 3 ustawy z 17 lutego 2005 r. o informatyzacji działalności podmiotów realizujących zadania publiczne[16], organy administracji publicznej przekazują do centralnego repozytorium znajdującego się na stronie www.crd.gov.pl wzory dokumentów elektronicznych. Stwierdzono, że Urząd nie przekazał wzorów dokumentów związanych ze świadczeniem trzech usług (tj. wpisaniem żłobka lub klubu dziecięcego do rejestru żłobków i klubów dziecięcych, zmianą danych w rejestrze żłobków i klubów dziecięcych, wykreśleniem z rejestru żłobków i klubów dziecięcych). Burmistrz wyjaśnił, że stało się tak z powodu trudności technicznych.

(dowód: akta kontroli str. 175, 307, 310, 334-344)

Uwagi dotyczące badanej działalności

1. W opinii NIK, wykorzystywanie w szerszym zakresie, w komunikacji elektronicznej wewnątrz i na zewnątrz jednostki, systemu e-SOS usprawni i przyśpieszy obieg dokumentów, zwłaszcza, że brak jest ku temu przeszkód technicznych.

2. W opisie usługi składania deklaracji o wysokości opłaty za gospodarowanie odpadami komunalnymi na portalu ePUAP wskazana jest nieaktualna podstawa prawna, tj. ustawa z 11 maja 2001 r. o opakowaniach i odpadach opakowaniowych[17]. Ten akt prawny został uchylony i obecnie obowiązuje ustawa z 13 czerwca 2013 r. o gospodarce opakowaniami i odpadami opakowaniowymi[18].

[15] Rozumianą 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.

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

[17] Dz. U. z 2001 r. Nr 63, poz. 638, ze zm.

[18] Ustawa obowiązująca od 1 stycznia 2014 r., Dz. U. z 2013 r., poz. 888.

Burmistrz wyjaśnił, że opis usługi został przygotowany przez zarządcę portalu, jednakże Urząd nie zwracał się o aktualizację opisu.

(dowód: akta kontroli str. 169-172, 321, 325)

3. NIK zwraca uwagę na brak karty usługi dotyczącej przyjmowania wniosków i uwag do sporządzonego studium uwarunkowań i kierunków zagospodarowania przestrzennego. Ponadto, wybrane do badania karty opisu pięciu usług zamieszczone na stronie internetowej Urzędu nie wskazywały na możliwość załatwienia sprawy także drogą elektroniczną. W opinii NIK, uzupełnienie karty usług świadczonych poprzez platformę ePUAP o informacje dotyczące możliwości załatwienia takich spraw również drogą elektroniczną, wpłynie na usprawnienie świadczenia tych usług.

(dowód: akta kontroli str. 178-197)

4. Na portalu ePUAP udostępniono w okresie od 26 sierpnia 2013 r. do 23 lipca 2014 r. elektroniczną usługę wydzierżawienia gruntu rolnego lub działki ogrodowej. Usługa nie była jednak nigdy realizowana przez Urząd. Burmistrz wyjaśnił, że została ona zamieszczona przez pracownika w ramach ćwiczeń warsztatowych, ale nie została przez niego usunięta. Błąd naprawiono w trakcie trwania czynności kontrolnych. W opinii NIK, sytuacja taka wskazuje na potrzebę zwracania większej uwagi na aktualność danych udostępnianych na portalu.

(dowód: akta kontroli str. 167-168, 345)

Ocena cząstkowa

W Urzędzie podjęto właściwe, choć w ocenie NIK mogące zostać zintensyfikowane, działania dotyczące dostosowania posiadanych systemów teleinformatycznych do współpracy z innymi systemami wewnątrz jednostki, a także na przestrzeni dwóch lat rozszerzano katalog usług świadczonych drogą elektroniczną poprzez system ePUAP. Ustalona nieprawidłowość nie miała istotnego wpływu na działalność w zbadanym zakresie.

2. Wdrożenie systemu zarządzania bezpieczeństwem systemów informatycznych

Opis stanu faktycznego

Dokumentami obowiązującymi w Urzędzie były: Polityka bezpieczeństwa z 1 października 2008 r. oraz Instrukcja zarządzania systemem informatycznym Ochrony Danych Osobowych z 15 marca 2010 r. (dalej: Instrukcja Ochrony Danych Osobowych). Wdrożenie Polityki bezpieczeństwa miało na celu zabezpieczenie danych osobowych przetwarzanych przez administratora danych, zgodnie z wymogami ustawy z 29 sierpnia 1997 r. o ochronie danych osobowych[19]. W Urzędzie trwały prace nad przygotowaniem PBI, która, jak podał Burmistrz, zostanie opracowana na podstawie normy PN-ISO/IEC 27001:2007 oraz w oparciu o przepisy rozporządzenia w sprawie KRI.

(dowód: akta kontroli str.16-163)

Stwierdzono, że inwentaryzacja była prowadzona przy użyciu specjalistycznego oprogramowania zawierającego szczegółowe informacje o danym urządzeniu informatycznym i jego konfiguracji (w przypadku komputerów – m.in. dane dotyczące systemu operacyjnego, płyty głównej, procesora, pamięci RAM, karty graficznej, dysku twardego), co było zgodne z § 20 ust. 2 pkt 2 rozporządzenia w sprawie KRI.

(dowód: akta kontroli str. 290-291)

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

W Urzędzie przeprowadzono w 2012 r. (od 15 października do 15 listopada) badanie bezpieczeństwa informacji (odnoszące się do ryzyka utraty integralności, dostępności lub poufności informacji), co było zgodne z § 20 ust. 2 pkt 3 rozporządzenia w sprawie KRI. W wyniku przeprowadzonego badania zrealizowano wydane zalecenia.

(dowód: akta kontroli str. 296, 299-306, 322, 325, 330-333)

Zgodnie z § 20 ust. 2 pkt 4 i 5 rozporządzenia w sprawie KRI, zarządzanie bezpieczeństwem informacji realizowane jest m.in. przez podejmowanie 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, a w przypadku zmiany zadań następuje również zmiana uprawnień. Na próbie 15 pracowników wykonujących zadania w wybranych systemach informatycznych potwierdzono, że osoby te uczestniczyły w procesie przetwarzania informacji w stopniu adekwatnym do zadań wynikających z zakresu obowiązków. Ponadto, w Instrukcji Ochrony Danych Osobowych opisano procedurę nadawania uprawnień do przetwarzania danych osobowych.

(dowód: akta kontroli str. 225-236, 321, 324-325, 347-348)

Na próbie dziewięciu pracowników, którzy zakończyli pracę w Urzędzie w okresie objętym kontrolą stwierdzono, że nastąpiła blokada uprawnień do użytkowanego przez nich systemu informatycznego[20], co było zgodne z § 20 ust. 2 pkt 5 rozporządzenia w sprawie KRI.

(dowód: akta kontroli str. 177, 225-231)

W § 20 ust. 2 pkt 8 rozporządzenia w sprawie KRI wskazano na konieczność ustanowienia podstawowych zasad gwarantujących bezpieczną pracę przy przetwarzaniu mobilnym i pracy na odległość. Ustalono, że podstawowe wymagania w zakresie zachowania się pracowników Urzędu w zakresie przetwarzania mobilnego zawarte zostały w Polityce bezpieczeństwa.

(dowód: akta kontroli str. 52-53, 272, 308, 311, 346)

Naprawy gwarancyjne sprzętu odbywały się w Urzędzie na zasadach ustalonych w umowach lub warunkach gwarancyjnych producenta sprzętu. Wszystkie naprawy pogwarancyjne sprzętu komputerowego były wykonywane przez informatyka Urzędu.

(dowód: akta kontroli str. 322, 325)

Ustalono, że Burmistrz zawarł dwie umowy na dostawę sprzętu komputerowego. Zapisano w nich, że przekazanie sprzętu komputerowego do naprawy poza miejsce użytkowania może nastąpić jedynie po wymontowaniu dysku twardego oraz – w przypadku umowy z 16 października 2013 r. – że dyski twarde nie podlegają zwrotowi dostawcy lub producentowi w przypadku konieczności ich wymiany. Ponadto, w przypadku umowy dotyczącej udzielenia licencji na korzystanie z systemu informatycznego NABÓR stwierdzono, że w jej treści zawarto m.in. zobowiązanie wykonawcy do ochrony danych związanych z wykonywaniem umowy oraz ich nieudostępniania osobom trzecim.

[20] Sprawdzono dostęp użytkowników do systemu e-SOS. Żaden z byłych pracowników nie posiadał dostępu do systemów objętych szczegółowym badaniem, tj. ALK+, POST+, GOK+ i NABÓR.

Przekazywanie baz danych między serwisem producenta oprogramowania ALK+, POST+ oraz GOK+ i użytkownikiem odbywało się w ten sposób, że istniała możliwość szyfrowania danych oraz kodowania baz danych systemów z brakiem możliwości zamiany danych osobowych. Działania Burmistrza należy uznać za zgodne z § 20 ust. 2 pkt 10 rozporządzenia w sprawie KRI, który stanowi, że zarządzanie bezpieczeństwem informacji realizowane jest m.in. poprzez zawieranie w umowach serwisowych podpisanych ze stronami trzecimi zapisów gwarantujących odpowiedni poziom bezpieczeństwa informacji.

(dowód: akta kontroli str. 198-224, 321, 326-329)

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[21]. W Urzędzie przeprowadzono w lutym 2013 r. audyt wstępny z zakresu Systemu Zarządzania Bezpieczeństwem Informacji (dalej: SZBI), będący audytem zgodności z normą PN-ISO/IEC 27001:2007. W wyniku audytu wskazano działania korygujące i doskonalące, które były w trakcie realizacji.

(dowód: akta kontroli str. 264-271, 281-288, 320)

Kopie zapasowe programów wykonywane były na nośnikach zewnętrznych (nośniki optyczne jednokrotnego użytku, np. CD-R) w cyklu miesięcznym, półrocznym i rocznym. Kopie bezpieczeństwa baz danych oraz katalogów na serwerach plików wykonywane były w cyklu dziennym (na taśmach DDS), tygodniowym, miesięcznym, półrocznym i rocznym (na płytach DVD). Nośniki były przechowywane w serwerowni[22]. Informatyk dokonywał m.in. comiesięcznego testowania danych zapisanych na taśmie DDS.

(dowód: akta kontroli str. 238-244, 322, 325)

Zapis danych wyjściowych z systemów POST+, GOK+, ALK+ oraz NABÓR był zgodny z listą formatów danych zapewniających dostęp do zasobów informacji udostępnianych za pomocą systemów teleinformatycznych używanych do realizacji zadań publicznych, opublikowaną w załączniku nr 2 do rozporządzenia w sprawie KRI.

(dowód: akta kontroli str. 176-177)

Ustalone nieprawidłowości

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

1. Ustalono, że do czasu zakończenia czynności kontrolnych (25 lipca 2014 r.) w Urzędzie nie opracowano i nie wdrożono PBI, która jest elementem systemu zarządzania bezpieczeństwem informacji. Zauważyć należy, że w myśl § 20 ust. 3 rozporządzenia w sprawie KRI, wymagania w zakresie SZBI uznaje się za

[21] 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.

[22] Obowiązek i częstotliwość wykonywania kopii zapasowych oraz procedury dotyczące ich przechowywania wynikały z Instrukcji Ochrony Danych Osobowych, jednakże miały zastosowanie do wszystkich danych, nie tylko osobowych.

spełnione, jeżeli zostały opracowane na podstawie Polskiej Normy: PN-ISO/IEC 27001:2007 *Technika informatyczna. Techniki bezpieczeństwa. Systemy zarządzania bezpieczeństwem informacji* oraz norm z nią związanych, m.in. PN-ISO/IEC 17799:2007 *Technika informatyczna. Techniki bezpieczeństwa. Praktyczne zasady zarządzania bezpieczeństwem informacji.* W pkt 5.1.1. normy PN-ISO/IEC 17799 wskazuje się, aby opracowano i stosowano w Urzędzie dokument polityki bezpieczeństwa informacji. Stwierdzono, że PBI była w trakcie przygotowania. Burmistrz wyjaśnił, że opracowanie dokumentu powinno zakończyć się do 30 września 2014 r., a opóźnienie wdrożenia przepisów rozporządzenia wynikało głównie z małej obsady kadrowej działu informatycznego Urzędu i braku dokładnego harmonogramu działań.

(dowód: akta kontroli str. 296, 299, 320, 323-324, 347-348)

2. Stwierdzono, że użytkownicy systemów informatycznych niebędący pracownikami służb informatycznych posiadali uprawnienia administracyjne w związku z czym mogli samodzielnie instalować oprogramowanie na komputerach służbowych[23]. Zgodnie z zapisami normy PN-ISO/IEC 27001:2007, załącznik A, punkt A.11.2.2 pkt b należy ograniczyć i kontrolować przyznawanie oraz korzystanie z przywilejów w systemach informatycznych według minimalnych wymagań wynikających z przydzielonych pracownikom zadań służbowych. Burmistrz wyjaśnił m.in., że przyjęte rozwiązanie wynikało z braków kadrowych (w Urzędzie zatrudniony był jeden informatyk oraz jedna osoba na stanowisku pomocy administracyjnej posiadająca wiedzę informatyczną); każdy z pracowników podpisał oświadczenie o niepodejmowaniu prób instalacji oprogramowania innego niż pochodzącego od pracodawcy; Urząd posiadał oprogramowanie, które umożliwiało bieżący monitoring aplikacji instalowanych przez użytkownika, a ponadto na każdej stacji roboczej zainstalowany był program antywirusowy reagujący w przypadku instalacji oprogramowania mogącego zagrozić bezpieczeństwu komputera. W ocenie NIK, wskazane przez Burmistrza działania nie gwarantowały bezpiecznej pracy w systemie informatycznym (oprogramowanie antywirusowe nie zawsze jest skuteczne). Ponadto, potrzeba ograniczenia uprawnień związana jest z minimalizowaniem ryzyka polegającego na możliwości nieświadomego zainstalowania przez użytkownika złośliwego oprogramowania (dokonanego np. w trakcie przeglądania stron internetowych).

(dowód: akta kontroli str. 290-292, 308, 311-312, 347-348)

3. Zgodnie z § 20 ust. 2 pkt 6 rozporządzenia w sprawie KRI zarządzanie bezpieczeństwem informacji realizowane jest w szczególności przez zapewnienie przez kierownictwo podmiotu publicznego warunków umożliwiających realizację i egzekwowanie szkolenia osób zaangażowanych w proces przetwarzania informacji. Stwierdzono, że w Urzędzie nie organizowano szkoleń w zakresie, o którym mowa w rozporządzeniu w sprawie KRI. Burmistrz wyjaśnił m.in., że większość pracowników Urzędu została przeszkolona w zakresie ochrony danych osobowych (ostatnie grupowe szkolenie miało miejsce w 2011 r.), a wszyscy złożyli oświadczenia, w których potwierdzili zapoznanie się z treścią Instrukcji Ochrony Danych Osobowych, a także zobowiązali się do przestrzegania postanowień Regulaminu ochrony danych osobowych. Zdaniem NIK powyższe argumenty nie mogą uzasadniać niewywiązania się przez Burmistrza z obowiązku nałożonego przez przepisy rozporządzenia w sprawie KRI, gdyż przeprowadzone szkolenie dotyczyło

[23] Sprawdzono na próbie 10 z 71 komputerów.

wyłącznie bezpieczeństwa przetwarzania danych osobowych, a nie wszystkich danych, jakie są przetwarzane w Urzędzie[24].

(dowód: akta kontroli str. 245-263, 309, 313-319, 347-348)

4. Kopie zapasowe badanych systemów informatycznych przechowywane były w serwerowni, czyli w miejscu wytwarzania danych. Pomieszczenie to nie było właściwie zabezpieczone, a sposób przechowywania kopii zapasowych nie gwarantował, że dostęp do nich posiadać będą jedynie uprawnione osoby. Było to niezgodne z wymogami określonymi w § 20 ust. 2 pkt 12 lit. b i e rozporządzenia w sprawie 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 teleinformatycznych, polegającego w szczególności na: minimalizowaniu ryzyka utraty informacji w wyniku awarii i zapewnieniu bezpieczeństwa plików systemowych. Zauważyć należy również, że zgodnie z pkt 10.5.1 pkt d i e normy PN -ISO/IEC 17799 kopie zapasowe powinny być przechowywane w innej lokalizacji niż miejsce ich tworzenia oraz powinny być odpowiednio zabezpieczone fizycznie i przed wpływem środowiska. Burmistrz wyjaśnił, że zalecił przechowywanie kopii zapasowych poza miejscem wytwarzania danych i zostaną one tam przeniesione.

(dowód: akta kontroli str. 289, 321, 325, 347-348)

Uwagi dotyczące badanej działalności

1. NIK zwraca uwagę, że w przypadku utraty uprawnień do korzystania z systemów informatycznych służących do przetwarzania danych osobowych, spowodowanych np. zakończeniem zatrudnienia, nie sporządzano w Urzędzie odwołań upoważnień. Burmistrz wyjaśnił, że upoważnienia wydawane są na czas zatrudnienia na stanowisku związanym z danym zakresem spraw i z tego względu nie sporządza się ich odwołań. Stwierdzono jednak, że w siedmiu przypadkach były one ważne do odwołania.

(dowód: akta kontroli str. 237, 273-280)

2. Zgodnie z § 20 ust. 2 pkt 13 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 bezzwłocznym zgłaszaniu incydentów naruszenia bezpieczeństwa informacji w określony i z góry ustalony sposób, umożliwiający szybkie podjęcie działań korygujących. Stwierdzono, że w Urzędzie nie wprowadzono stosownej procedury. Kwestia ta zostanie uregulowana w tworzonej dokumentacji SZBI[25].

(dowód: akta kontroli str. 149-157, 308, 312)

Ocena cząstkowa

Najwyższa Izba Kontroli ocenia, że Burmistrz w znacznym stopniu zrealizował obowiązki wynikające z przepisów rozporządzenia w sprawie KRI. Pozytywnie należy odnieść się m.in. do przeprowadzania właściwej inwentaryzacji posiadanego sprzętu, zapewnienia audytu wewnętrznego w zakresie bezpieczeństwa informacji, blokowania uprawnień do systemów informatycznych byłym pracownikom Urzędu oraz zawierania w umowach serwisowych postanowień mających gwarantować

[24] Zgodnie z rozporządzeniem w sprawie KRI, szkolenia powinny uwzględniać w szczególności takie zagadnienia jak:

a) zagrożenia bezpieczeństwa informacji,

b) skutki naruszenia zasad bezpieczeństwa informacji, w tym odpowiedzialność prawna,

c) stosowanie środków zapewniających bezpieczeństwo informacji, w tym urządzenia i oprogramowanie minimalizujące ryzyko błędów ludzkich.

[25] Potwierdzono, że przygotowywana jest procedura „Działania korygujące i zapobiegawcze".

odpowiedni poziom bezpieczeństwa informacji. Negatywnie należy ocenić brak opracowania PBI, nadanie uprawnień administracyjnych wszystkim pracownikom Urzędu, brak odpowiedniego przeszkolenia pracowników w zakresie bezpieczeństwa informacji oraz niewłaściwy sposób przechowywania i zabezpieczenia kopii zapasowych danych.

3. Zapewnienie dostępności informacji dla osób niepełnosprawnych

Opis stanu faktycznego

Na stronie internetowej BIP Luboń (www.bip.lubon.pl) zamieszczono informację o możliwości otwarcia strony w wersji dla osób niedowidzących. Stwierdzono, że możliwe jest zapoznanie się z treścią ww. strony z wykorzystaniem powiększonej czcionki. Ułatwieniem dla odbiorców była również możliwość odtwarzania zapisów dźwiękowych z posiedzeń sesji Rady Miasta. Nie istniała natomiast możliwość posłużenia się wersją dla osób niedowidzących przy korzystaniu ze strony internetowej miasta (www.lubon.pl). W Urzędzie trwały prace nad przygotowaniem nowej strony internetowej miasta, która będzie posiadała udogodnienia dla osób niedowidzących[26].

(dowód: akta kontroli str. 293, 307, 311)

Zweryfikowano zgodność strony internetowej Urzędu (www.lubon.pl) i strony BIP Urzędu (www.bip.lubon.pl) ze standardem WCAG 2.0[27], który służy dostosowaniu wyświetlanej treści na stronie internetowej do potrzeb osób niedowidzących. Stwierdzono, że strona BIP Urzędu nie zawierała żadnych błędów. Na stronie internetowej Urzędu wystąpił jeden błąd stwierdzony w badaniu z wykorzystaniem narzędzia dostępnego na stronie http://validator.w3.org oraz 193 błędy stwierdzone w badaniu z wykorzystaniem narzędzia dostępnego na stronie http://jigsaw.w3.org/css-validator.

(dowód: akta kontroli str. 293, 307, 311)

Informacja o możliwości otwarcia strony BIP Luboń w wersji dla osób niedowidzących pisana była bardzo małą czcionką, potencjalnie więc mogła być ona niezauważona przez osoby zainteresowane. Ponadto, pomimo dostępności Biuletynu dla osób niedowidzących, błędy techniczne powodowały ograniczenie dostępności do niektórych treści, np.:

- po otwarciu zakładki *Rejestry*, interesant był przekierowywany na kolejny poziom, z którego miał możliwość wglądu w interesujący go rejestr lub ewidencję. Z pięciu dostępnych rejestrów otwierały się: rejestr żłobków i klubów dziecięcych, księga rejestrowa instytucji kultury oraz rejestr punktów adresowych, a brak było możliwości wyświetlenia ewidencji szkół niepublicznych oraz rejestru instytucji kultury,

- po otwarciu zakładki *Sprawozdania z wykonania budżetu miasta*, interesant był przekierowywany na kolejny poziom, z którego mógł wybrać interesujący go rok. W przypadku lat 2008, 2010 i 2013 „nie podpięto" sprawozdania; podobna sytuacja miała miejsce w przypadku informacji Burmistrza o przebiegu wykonania budżetu Miasta Luboń za I półrocze 2009 i 2011 roku, informacji o stanie realizacji zadań oświatowych miasta Luboń za rok szkolny 2008/2009 oraz informacji rocznej instytucji kultury za rok 2006.

[26] Strona dostępna pod roboczym adresem http://lubon.test.lo.pl.

[27] Systemy teleinformatyczne podmiotów realizujących zadania publiczne funkcjonujące w dniu wejścia w życie rozporządzenia w sprawie KRI należy dostosować do wymagań określonych w § 19, nie później niż w terminie 3 lat od dnia wejścia w życie rozporządzenia, tj. do 31 maja 2015 r.

Burmistrz wyjaśnił, że wersja strony dla osób niedowidzących istnieje od początku 2014 r. Treści zawarte w BIP (gromadzone przez wiele lat) zostały przeniesione ze starej wersji do aktualnej w sposób automatyczny. Z technicznego punktu widzenia nie ma możliwości odtworzenia pełnej zawartości stron w wersji dla niedowidzących, co wynika z niepełnej kompatybilności struktur obu wersji BIP. W wielu miejscach wymagana jest ręczna modyfikacja działów, stron, podstron lub pojedynczych wpisów. Jest to proces czasochłonny, wykonywany stopniowo w miarę możliwości.

(dowód: akta kontroli str. 293, 307-308, 311)

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[28], wnosi o:

1. Przekazanie do centralnego repozytorium brakujących wzorów dokumentów elektronicznych dotyczących usług świadczonych przez Urząd.
2. Odebranie użytkownikom systemów informatycznych niebędącym pracownikami służb informatycznych uprawnień umożliwiających instalowanie oprogramowania.
3. Podjęcie działań w celu przeszkolenia osób zaangażowanych w proces przetwarzania informacji w zakresie, o którym mowa w § 20 ust. 2 pkt 6 rozporządzenia w sprawie KRI.
4. Przechowywanie i zabezpieczenie kopii zapasowych systemów informatycznych i danych w nich zawartych w innym pomieszczeniu niż są one wytwarzane.

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.

[28] 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 **1** sierpnia 2014 r.

Najwyższa Izba Kontroli
Delegatura w Poznaniu

Kontroler
Maria Wojcińska
starszy inspektor kontroli państwowej

.....
podpis

Dyrektor
z up. Tomasz Nowiński
Wicedyrektor

.....
podpis