NAJWYŻSZA IZBA KONTROLI
Delegatura w Szczecinie

LSZ - 4101-011-02/2014
P/14/004

WYSTĄPIENIE POKONTROLNE

NAJWYŻSZA IZBA KONTROLI
Delegatura w Szczecinie
ul. Jacka Odrowąża 1, 71-420 Szczecin
T +48 91 831 39 00, F +48 91 831 39 66
lsz@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 Szczecinie

Kontroler

Agata Prochotta - Miłek, specjalista kontroli państwowej, upoważnienie do kontroli nr 91856 z dnia 08.08.2014 r.

(dowód: akta kontroli str. 1 – 2)

Jednostka kontrolowana

Urząd Miejski w Stargardzie Szczecińskim, ulica Czarneckiego 17, 73-110 Stargard Szczeciński, REGON 811685734, (dalej: Urząd).

Kierownik jednostki kontrolowanej

Sławomir Pajor, Prezydent Miasta Stargard Szczeciński (dalej: Prezydent).

(dowód: akta kontroli str. 3)

II. Ocena kontrolowanej działalności

Ocena ogólna

Prezydent Miasta Stargard Szczeciński realizując w okresie od 31 maja 2012 r. do 12 września 2014 r. 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[1] (KRI):

- zapewnił współpracę pomiędzy wybranymi do badania systemami informatycznymi Urzędu, co spełniało minimalne wymogi interoperacyjności, o których mowa w § 5 ust. 3 pkt 3 rozporządzenia KRI,
- przeprowadził analizę zagrożeń występujących przy przetwarzaniu informacji, 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,
- udostępnił klientom Urzędu 176 usług, w przypadku których przynajmniej część czynności można było wykonać drogą elektroniczną,
- zapobiegał możliwości zainstalowania nieautoryzowanego oprogramowania.

[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 zarzadzania 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 Urzędzie obowiązywało zarządzenie Nr 21 Prezydenta Miasta Stargardu Szczecińskiego z dnia 2 sierpnia 1999 r. w sprawie instrukcji określającej sposób zarządzania zbiorami danych osobowych. Procedura ta nie dotyczyła jednak wszystkich danych jakie są przetwarzane w Urzędzie, lecz tylko danych osobowych,
- 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.

III. Opis ustalonego stanu faktycznego

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

Opis stanu faktycznego

1.1.„Strategia Rozwoju Społeczno - Gospodarczego dla Miasta Stargard Szczeciński do roku 2020" została przyjęta uchwałą Nr XXIV/261/08 Rady Miejskiej w Stargardzie Szczecińskim z dnia 30 września 2008 r. Obejmowała ona w priorytecie 5 „Społeczność" cel szczegółowy 5.2 „Podniesienie jakości usług w obiektach użyteczności publicznej", w ramach którego wyznaczono kierunek działania 5.2.5. „Informatyzacja oraz usprawnienie funkcjonowania administracji samorządowej w ramach projektu e-urząd". W opisie kierunku podano, że jego główną ideą jest w końcowym etapie jego realizacji doprowadzenie do pełnej możliwości obsługi petenta na drodze elektronicznej". Dla powyższego celu nie wskazano żadnych mierników. W roku 2013 rozpoczęto projekt „Profesjonalny Urząd = satysfakcja mieszkańców", w ramach którego wykonano m.in. karty usług oraz przeprowadzono szkolenia pracowników Urzędu w zakresie bezpieczeństwa informatycznego, co zostało opisane w dalszej treści niniejszego wystąpienia pokontrolnego.

(dowód: akta kontroli str. 219 – 221, 225 – 228, 229)

1.2. Prezydent wyjaśnił, że promocja komunikacji elektronicznej następuje poprzez popularyzację strony internetowej i poczty elektronicznej, udostępnienie dla mieszkańców zarówno w BIP (forma elektroniczna) jak i w postaci papierowej kart usług opisujących sposób załatwienia spraw, przeprowadzanie telekonferencji Prezydenta Miasta z mieszkańcami miasta (m.in. z wykorzystaniem tzw. czatu),

wdrożenie systemu elektronicznego obiegu dokumentów umożliwiającego składanie wniosków wraz z załącznikami z wykorzystaniem zintegrowanej platformy ePUAP, przeprowadzanie konkursów za pośrednictwem formularzy on-line na stronie www, udostępnianie na stronie internetowej planów zagospodarowania przestrzennego, działek, punktów adresowych, interaktywnego turystycznego planu miasta.

(dowód: akta kontroli str. 18 – 19, 20)

1.3. Prezydent wyjaśnił, że *„Przeprowadzono badania ankietowe klientów urzędu przez Szczecińską Szkołę Wyższą Collegium Batlicum dotyczącą procedur świadczonych usług (w tym elektronicznych) w ramach projektu „Profesjonalny Urząd = satysfakcja mieszkańców Stargardu Szczecińskiego". Badanie prowadzono na próbie 150 klientów urzędu. (…) Przeprowadzono ankiety badające poziom zadowolenia z aktualnej wersji strony internetowej miasta. Mieszkańcy mogą zgłaszać potrzeby i problemy bezpośrednio przez stronę internetową. Przeprowadzono badania związane z projektem „Stargardzki budżet obywatelski" nt. możliwości składania wniosków poprzez stworzony do tego celu formularz on-line, platformę ePUAP i pocztę elektroniczną. Badania wykazały, iż wnioski złożone drogą elektroniczną stanowiły 40% wniosków ogółem, wobec czego należy rozwijać tego typu formy elektronicznej komunikacji. Monitorowano środki masowego przekazu (prasa, radio, forum itp.) celem analizy opinii mieszkańców nt. funkcjonowania form komunikacji z UM. Bieżąco analizowano statystyki odwiedzin strony internetowej w zakresie komunikacji elektronicznej, preferencji internautów (wyszukiwanie frazy itp.)."*

(dowód: akta kontroli str. 18 – 19, 20 - 21)

1.4. Ze złożonych przez Prezydenta wyjaśnień wynika, że po wejściu w życie rozporządzenia KRI korespondencja z Departamentem Informatyzacji Ministerstwa Administracji i Cyfryzacji dotyczyła przeprowadzenia weryfikacji uprawień spółek komunalnych, w których wykorzystywana była funkcjonalność podmiotu publicznego na platformie ePUAP. Pierwotnie spółki komunalne uwzględniane były w jednolitych zasadach dotyczących wymiany korespondencji pomiędzy Urzędem Miejskim a instytucjami i jednostkami miejskimi poprzez platformę ePUAP. Przez pewien okres czasu korespondencja ta była realizowana wyłącznie poprzez platformę ePUAP. Ustalono, że zgodnie z paragrafem 8 rozporządzenia Ministra Spraw Wewnętrznych i Administracji z dnia 27 kwietnia 2011 r. w sprawie zakresu i warunków korzystania z elektronicznej platformy usług administracji publicznej oraz art. 2 ustawy z dnia 17 lutego 2005 r. o informatyzacji realizujących zadania publiczne spółki komunalne nie wchodzą w zakres katalogu podmiotów publicznych.

(dowód: akta kontroli str. 18 – 19,21)

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[2] (dalej: Instrukcja Kancelaryjna). W Urzędzie obowiązywał tradycyjny (papierowy) system wykonywania czynności kancelaryjnych, jako podstawowy sposób dokumentowania przebiegu, załatwiania i rozstrzygania spraw, który został ustalony zarządzeniem nr 142/2013 Prezydenta Miasta Stargard Szczeciński z dnia 17.04.2013 r. w sprawie nadania Regulaminu Wewnętrznego Urzędowi Miasta Stargard Szczeciński.

(dowód: akta kontroli str. 219 - 221)

[2] Dz. U. Nr 14, poz. 67 ze zm.

Zarządzeniem Prezydenta Miasta Stargard Szczeciński z dnia 31 lipca 2013 r.[3] wprowadzono w Urzędzie „Procedurę stosowania systemu elektronicznego obiegu dokumentów (system zarządzania dokumentami) przez pracowników urzędu miejskiego w Stargardzie Szczecińskim" (dalej: SZD).

Zgodnie z SZD korespondencja wpływa do Urzędu w następujących formach:

- przesyłek pocztowych i kurierskich oraz wniosków i pism składanych bezpośrednio przez Klientów, które przyjmowane są w Biurze Obsługi Klienta (Kancelaria) lub w sekretariacie Prezydenta Miasta lub sekretariacie Zastępcy Prezydenta,
- elektronicznej za pośrednictwem elektronicznej skrzynki podawczej, która przyjmowana jest przez Kancelarię,
- faksu, który przyjmowany jest w Kancelarii oraz w Sekretariatach,
- e-maila, które przyjmowane są przez pracowników Kancelarii oraz Sekretariatów.

Korespondencja w Urzędzie Miejskim podlega rejestracji w SZD, za pomocą dostępnej w systemie metryczki rejestracji korespondencji. Korespondencja otrzymana w formie papierowej jest skanowana, a jej odwzorowanie jest dołączane jako załącznik do metryczki rejestracji korespondencji w SZD. W przypadku korespondencji otrzymanej za pomocą elektronicznej skrzynki podawczej, załączniki w sposób automatyczny są dołączane do formularza rejestracji korespondencji w SZD. Korespondencja przyjęta w Kancelarii jest przekazywana do Sekretarza Miasta, który dokonuje dekretacji merytorycznej na właściwe wydziały Urzędu. Korespondencja przyjęta w Sekretariacie Prezydenta Miasta jest przekazywana do Prezydenta Miasta, który dokonuje dekretacji merytorycznej na właściwe wydziały Urzędu. Korespondencja przyjęta w Sekretariacie Zastępcy Prezydenta Miasta jest przekazywana do Zastępcy Prezydenta Miasta, który dokonuje dekretacji merytorycznej na właściwe wydziały Urzędu. Kancelaria drukuje przy pomocy SZD książkę korespondencji otrzymanej danego dnia. Osoba kierująca wydziałem dokonuje dekretacji pisma na konkretnego pracownika, w ramach obowiązków którego znajduje się tematyka danej sprawy. Dekretacja, jak i zapoznanie się z korespondencją, są odnotowywane w systemie eDokument, poprzez wykorzystanie odpowiednich funkcji systemu. Pracownik w ramach obowiązków którego znajduje się tematyka sprawy podejmuje działania:

a) rejestruje sprawę zgodnie z Jednolitym Rzeczowym Wykazem Akt, rejestracja odbywa się w systemie eDokument,
b) rozpatruje sprawę oraz sprawdza, czy wniosek nie zawiera braków formalnych i ewentualnie wysyła wezwanie do usunięcia braków,
c) przygotowuje projekt odpowiedzi, która przekazywana jest do akceptacji kierownikowi merytorycznej komórki,
d) odpowiedź do danej sprawy jest rejestrowana w systemie Dokument, ewentualna akceptacja ze strony kierownika komórki merytorycznej jest odnotowywana w SZD z wykorzystaniem odpowiednich funkcji programu,
e) dokument przeznaczony do wysłania jest oznaczany specjalnie w systemie eDokument, wraz z informacją o sposobie wysłania,
f) dokument przeznaczony do wysłania w formie papierowej jest drukowany i podpisywany przez upoważnione osoby, a następnie przekazywany do Kancelarii,
g) dokumenty przeznaczone do wysłania w formie elektronicznej podpisywane są za pomocą bezpiecznego podpisu elektronicznego w systemie Dokument, ponadto w systemie wskazany zostaje adres skrytki adresata dokumentu.

[3] Nr 274/2013.

Wysyłka odbywa się w następujący sposób: Kancelaria nadaje przesyłki przygotowane w Wydziałach do wysłania. Przesyłki adresowane na teren Miasta – podlegają rejestracji w rejestrze korespondencji prowadzonej przez Kancelarię i doręczane są przez gońców; w indywidualnych przypadkach dopuszcza się możliwość doręczania korespondencji przez operatora pocztowego. Rejestracja odbywa się w systemie eDokument. Przesyłki polecone, wartościowe oraz paczki adresowane poza granice miasta – podlegają rejestracji w systemie eDokument i doręczeniu przez operatora pocztowego. Przesyłki wysyłane drogą elektroniczną są wysyłane na wskazany adres skrytki Elektronicznej Skrzynki Podawczej przy pomocy systemu eDokument. Rejestracja takiej korespondencji odbywa się automatycznie po wysłaniu przesyłki. Kancelaria drukuje przy pomocy SZD książkę korespondencji otrzymanej danego dnia.

(Dowód: akta kontroli str. 93 - 96)

Z 5.382 dokumentów w formie elektronicznej, które w badanym okresie wpłynęły do Urzędu, badaniem szczegółowym objęto 10 dokumentów stwierdzając, że ich rejestracja i procedowanie odbyło się w sposób opisany powyżej.

(dowód: akta kontroli str. 28 - 57)

1.6. W badanym okresie do Urzędu wpłynęło łącznie 85.795 dokumentów, z czego 5.382 w formie elektronicznej (tj. 6,27%). Obywatele wnieśli łącznie 62.544 dokumentów (z czego 454 w formie elektronicznej, tj. 0,73%), osoby prawne lub inne podmioty 8.601 dokumentów (z czego 311 w formie elektronicznej, tj. 3,62%), inne urzędy 14.650 dokumentów (z czego 4.617 w formie elektronicznej, tj. 31,52%). W tym samym okresie z Urzędu wysłano łącznie 94.103 dokumentów (z czego 6.487 w formie elektronicznej, tj. 6,89%). Do obywateli wysłano łącznie 72.061 dokumentów (z czego 211 droga elektroniczną, tj. 0,29%), do osób prawnych lub innych podmiotów 5.855 dokumentów (z czego 196 w formie elektronicznej, tj. 3,35%) i do innych urzędów 16.187 (z czego 6.080 w formie elektronicznej, tj. 37,56%).

(Dowód: akta kontroli str. 218)

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

W badanym okresie Urząd świadczył usługę elektroniczną, z wykorzystaniem platformy e-PUAP (Elektroniczna Platforma Usług Administracji Publicznej), tj. „Skargi, wnioski, zapytania do urzędu". W zakładce @-urząd lub na stronie BIP (Biuletyn Informacji Publicznej) Urzędu zamieszczone były karty usług. Przedmiotowe karty pozwalały na wykonanie części czynności drogą elektroniczną.

(Dowód: akta kontroli str. 58 – 70, 229, 230 – 232, 232 - 233)

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

- Przeniesienie decyzji o warunkach zabudowy,
- Zezwolenie na usunięcie drzew i krzewów,
- Pomoc materialna dla uczniów o charakterze socjalnym – stypendium szkolne,
- Dodatek mieszkaniowy,

– Wydawanie odpisów stanu cywilnego.

Badanie wykazało, że opisy wszystkich objętych badaniem usług oraz karta usługi „Skargi, wnioski, zapytania do urzędu" były zgodne z faktycznie świadczonymi. Opisy usług nie zawierały jednak dat ich ostatniej aktualizacji.

(Dowód: akta kontroli str. 58 – 70, 229, 230 – 232, 232 - 233)

Prezydent wyjaśnił: „Wdrożenie systemu kart e-usług na stronie internetowej www.stargard.pl zostało rozpoczęte w 2013 roku w ramach projektu „ Profesjonalny urząd =satysfakcja mieszkańców Stargardu Szczecińskiego". Wdrożenie prowadzi firma zewnętrzna i system funkcjonuje na zewnętrznym serwerze tej firmy. Zakończenie wdrożenia systemu planowane jest na grudzień 2014 roku. System umożliwia wprowadzanie danych o sposobie załatwienia sprawy, przez poszczególne uprawnione osoby w każdym wydziale Urzędu Miejskiego. Osoby te posiadają loginy i hasła dostępowe. O szczegółowości wprowadzanych danych decyduje ta właśnie uprawniona osoba. W formularzu wprowadzania danych (który stanowi załącznik do wyjaśnienia), poza polami podstawowymi, istnieją pola dodatkowe w które można wprowadzić:

- datę zamieszczenia karty oraz datę jej aktualizacji,

- osobę odpowiedzialną za wprowadzone dane,

- dopuszczalny czas niedostępności usług elektronicznych,

- sposób zgłaszania awarii,

- technicznego właściciela usług,

- podmiot odpowiedzialny za usuwanie awarii itp.

Ze względu na to że system nie jest w pełni wdrożony, osoby odpowiedzialne za konkretne sprawy wprowadzały do tej pory, jedynie dane podstawowe (podstawy prawne, terminy, opłaty, wzory wniosków i załączników itp.) W chwili obecnej zostanie położony nacisk na pracowników, aby dokładniej wypełniali dane w formularzu o brakujące pola.

Dodatkowo Wydział Informatyki przy jakiejkolwiek awarii, uniemożliwiającej korzystanie z usług elektronicznych, podaje na stronie głównej www informację o awarii z terminem ich ponownego uruchomienia oraz sposobem postępowania."

(Dowód: akta kontroli str. 224, 225 – 228)

1.8. Badanie zapisów procedur dotyczących usługi „Skargi, wnioski, zapytania do urzędu" oraz pięciu usług, dla których wykonanie części czynności Urząd umożliwiał drogą elektroniczną (opisanych w punkcie 1.7 niniejszego wystąpienia pokontrolnego) wykazało, że ich opisy zamieszczone na stronie BIP Urzędu zawierały zgodnie z wymogami rozporządzenia Ministra Spraw Wewnętrznych i Administracji z dnia 27 kwietnia 2011 r. w sprawie zakresu i warunków korzystania z elektronicznej platformy usług administracji publicznej[4] - dane dotyczące: podmiotu świadczącego usługę, miejsca świadczenia usługi, aktualnej podstawy prawnej, wysokości opłat, trybu odwoławczego, wymaganych dokumentów.

(Dowód: akta kontroli str. 58 – 70, 229, 230 – 232, 232 - 233)

[4] Dz. U. Nr 93, poz. 546, uchylone z dniem 11.05.2014 r. Obecnie obowiązuje rozporządzenie Ministra Administracji i Cyfryzacji z dnia 6 maja 2014 r. w sprawie zakresu i warunków korzystania z elektronicznej platformy usług administracji publicznej (Dz. U. z 2014 r., poz. 584).

1.9 W badanym okresie do Centralnego Repozytorium Wzorów Dokumentów ePUAP nie przekazywano wzoru usług.

(dowód: akta kontroli str. 219 - 221)

1.10 Ustalono, że w procesie zarządzania wyżej opisanymi usługami Urząd w podstawowym zakresie wspierał model usługowy. Zgodnie z definicją zawartą w § 2 pkt 8 rozporządzenia KRI, model usługowy jest modelem architektury systemu informatycznego, w którym dla użytkowników zdefiniowano stanowiące odrębną całość funkcje systemu teleinformatycznego (usługi sieciowe) oraz opisano sposób korzystania z tych funkcji. Sporządzono karty opisu usług, w których określono właściciela usługi (poszczególne wydziały Urzędu), a także czas realizacji, wymagane dokumenty, opłaty, tryb odwoławczy i podstawę prawną.

(Dowód: akta kontroli str. 58 - 70)

1.11 Zakres współpracy systemów informatycznych wewnątrz Urzędu zbadano w oparciu o dobór celowy dwóch systemów, zakupionych po 31 maja 2012 r., tj. po wejściu z życie rozporządzenia KRI:

- RATUSZ – moduł wymiaru podatku od nieruchomości, wersja 6.35.1.3746 (dalej: RATUSZ),

- AZAK, wersja 7.19.0; służący do prowadzenia archiwum zakładowego (dalej: AZAK),

(dowód: akta kontroli str. 25 – 27, 115, 116)

System RATUSZ sposób dwustronny komunikuje się z systemem „RATUSZ – moduł księgowość wersja 6.35.1.2533". Pracownik wprowadza ręcznie dane z informacji w sprawie podatku od nieruchomości (m.in. dane podatnika, dane o nieruchomościach i obiektach budowlanych podlegających opodatkowaniu) do systemu RATUSZ. Po ich zatwierdzeniu system ustala wymiar podatku od nieruchomości, który automatycznie przejmowany jest przez system RATUSZ – moduł księgowość jako przypis należności. Pracownik obsługujący system RATUSZ otrzymuje z modułu księgowość automatycznie informacje o fakcie wygenerowania przypisu podatkowego.

System AZAK posiada możliwość dwustronnego komunikowania się z systemami zewnętrznymi, jednakże do dnia 02.09.2014 r. możliwość ta nie była wykorzystywana, ponieważ Archiwum Państwowe taką możliwość zamierza wprowadzić dopiero w przyszłości. W chwili obecnej pracownik wprowadza do systemu spis zdawczo – odbiorczy (zawierający m.in. dane o numerze wpisu, dacie przycięcia, symbol komórki organizacyjnej Urzędu, która dokonała wpisu, informacje o rodzaju dokumentacji: aktowa bądź techniczna) i następnie zapisuje te informacje.

(Dowód: akta kontroli str. 115, 116 - 120)

1.12 W sprawie procedur i praktyk postępowania stosowanych we współpracy z innymi jednostkami administracji publicznej Prezydent wyjaśnił, że: *„Elektroniczna komunikacja z innymi jednostkami administracji publicznej jest realizowana na wielu płaszczyznach (…) System Ewidencji Ludności zasila elektronicznie ogólnopolski rejestr PESEL, System Dowody Osobiste posiada moduł komunikacji z ogólnopolskim Rejestrem Utraconych i Unieważnionych Dowodów Osobistych, komunikacja elektroniczna dotycząca nowych nr PESEL poprzez Portal Informacyjny Administracji, wielotematyczna elektroniczna sprawozdawczość statystyczna US, komunikacja systemu finansowo – księgowego, kadrowo –*

płacowego z systemami ministerstw (Bestia, sprawozdawczość finansowa), elektroniczne wysyłanie uchwał do publikacji w dzienniku urzędowym województwa w formacie XML, komunikacja elektroniczna z PFRON, funkcjonalność wymiany danych dot. Ewidencji gruntów Starostwa z systemem Posesja, elektroniczny dostęp do bazy ewidencji gruntów w Starostwie, elektroniczna publikacja zamówień publicznych na portalu UZP, elektroniczna komunikacja z Systemem Informacji Oświatowej."

(dowód: akta kontroli str. 18 –19, 20 - 22)

Ze złożonych przez Prezydenta wyjaśnień wynika, że z wnioskiem o prowadzenie wzajemnej komunikacji elektronicznej zwrócił się Zachodniopomorski Urząd Wojewódzki i Urzędy Skarbowe.

(dowód: akta kontroli str. 18 – 19, 20 – 22)

W badanym okresie Urząd nie zwracał się do innych jednostek z wnioskiem o prowadzenie komunikacji elektronicznej.

(dowód: akta kontroli str. 229)

Ustalone nieprawidłowości

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

Ocena cząstkowa

Najwyższa Izba Kontroli ocenia pozytywnie działalność kontrolowanej jednostki w zbadanym zakresie[5].

2. Wdrożenie systemu zarządzania bezpieczeństwem systemów informatycznych

Opis stanu faktycznego

2.1 W Urzędzie nie opracowano i nie wdrożono Polityki Bezpieczeństwa Informacji opracowanej na podstawie Polskiej Normy PN-ISO/IEC 27001, która jest elementem systemu zarządzania bezpieczeństwem informacji.

(dowód: akta kontroli str. 219 - 221)

Obowiązywały:

- zarządzenie Nr 18 Prezydenta Miasta Stargardu Szczecińskiego z dnia 6 lipca 1999 r. w sprawie wyznaczenia administratora bezpieczeństwa informacji,

- zarządzenie Nr 19 Prezydenta Miasta Stargardu Szczecińskiego z dnia 6 lipca 1999 r. w sprawie instrukcji postępowania w sytuacji naruszenia danych osobowych z załączaniem „instrukcja postępowania w sytuacji naruszenia ochrony danych osobowych",

- zarządzenie Nr 20 Prezydenta Miasta Stargardu Szczecińskiego z dnia 6 lipca 1999 r. w sprawie określenia budynków, pomieszczeń lub innych części, tworzących obszar, w którym przetwarzane są dane osobowe z użyciem stacjonarnego sprzętu komputerowego,

[5] W Urzędzie wprowadzono „Procedurę stosowania systemu elektronicznego obiegu dokumentów (system zarządzania dokumentami) przez pracowników urzędu miejskiego w Stargardzie Szczecińskim". Objęte badaniem szczegółowym systemy RATUSZ i AZAK posiadają możliwość dwustronnego komunikowania się z innymi systemami, stanowiło o ich interoperacyjności.

- zarządzenie Nr 21 Prezydenta Miasta Stargardu Szczecińskiego z dnia 2 sierpnia 1999 r. w sprawie instrukcji określającej sposób zarządzania zbiorami danych osobowych.

(Dowód: akta kontroli str. 136 – 142, 143 – 144, 145- 146,147)

2.2 Inwentaryzacja zasobów informatycznych Urzędu była prowadzona w plikach programu Excel. Badaniem szczegółowym objęto zapisy w ewidencji dotyczące łącznie 10 zestawów komputerowych oraz jednego serwera. Dane dotyczące badanych zestawów komputerowych zawierały m.in. informację o jednostce Urzędu, w której znajduje się zestaw, osobie, która obsługuje komputer (imię i nazwisko, numer służbowy), typie, producencie, pamięci RAM, kartach audio i video, nazwę hosta mc adres IP, urządzeniach peryferyjnych oraz zainstalowanym systemie operacyjnym i oprogramowaniu. Dane dotyczące badanego serwera zawierały m.in. informację o jednostce organizacyjnej Urzędu, której podlega serwer, nazwie, typie, przeznaczeniu serwera, jego umiejscowieniu.

(dowód: akta kontroli str. 121 - 135)

W dniu 2 września 2014 r. przeprowadzono badanie możliwości zainstalowania nieautoryzowanego oprogramowania na 15 wybranych losowo komputerach Urzędu. Stwierdzono, że użytkownicy systemów informatycznych niebędący pracownikami służb informatycznych nie posiadali uprawnień administracyjnych i nie mogli samodzielnie instalować oprogramowania na komputerach służbowych.

(dowód: akta kontroli str.148 – 149, 150 – 151, 152 – 158, 159 - 162)

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

(dowód: akta kontroli str. 71 – 79, 80 - 88)

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

(dowód: akta kontroli str. 185 – 187, 188 - 215)

Nadawanie, modyfikowanie i odbieranie uprawnień w systemach informatycznych nie było realizowane w oparciu o przyjęte w Urzędzie regulacje pisemne (brak PBI).O uprawnieniach pracowników w systemach informatycznych decydowali kierownicy komórek organizacyjnych poprzez złożenie w systemie Help Desk odpowiedniego wniosku w formie maila do administratora danych i załączali do niego upoważnienie do przetwarzania danych osobowych. Dokonano sprawdzenia zablokowania dostępu do systemów informatycznych dla dziesięciu pracowników, którzy ostatnio zakończyli pracę w Urzędzie i ustalono, że ich konta użytkownika zostały zablokowane w pełnym zakresie. Przełożeni sporządzili stosowne wnioski o zablokowanie dostępu do kont w systemach informatycznych.

(dowód: akta kontroli str. 219 - 221, 163 - 184)

2.5 W badanym okresie Urząd zapewnił szkolenia pracowników zaangażowanych w proces przetwarzania informacji, co stanowiło wymóg § 20 ust. 2 pkt 6 rozporządzenia KRI. Zakres szkolenia obejmował zasady obiegu e-dokumentu, dostęp do systemów IT po podaniu hasła.

(dowód: akta kontroli str. 219 - 221)

2.6 Zasady pracy na urządzeniach przenośnych nie były w badanym okresie uregulowane pisemnie (brak PBI). W praktyce każdorazowo zgodę na wyniesienie urządzenia przenośnego poza siedzibę Urzędu (targi, prezentacje, imprezy promocyjne) wydawał administrator bezpieczeństwa informatycznego po złożeniu odpowiedniego wniosku w systemie Help Desk. W badanym okresie pracownicy Urzędu posiadali 10 urządzeń mobilnych.

(dowód: akta kontroli 219 - 221)

2.7 W okresie objętym kontrolą, tj. od 31.05.2012 r. do 29.07.2014 r. Urząd zakupił 10 komputerów. Urząd nie serwisuje swojego sprzętu IT w serwisie zewnętrznym – poza drukarkami. Przy serwisowaniu komputerów przez informatyków Urzędu nie występuje wydawanie dysków twardych na zewnątrz.

(dowód: akta kontroli str. 219 – 221, 229)

W dwóch umowach licencyjnych i serwisowych, jakie w badanym okresie Urząd zawarł z dostawcami systemów, które zostały opisane w punkcie 1.11 niniejszego wystąpienia pokontrolnego, zawarto klauzule zapewniające poufność wszystkich danych Urzędu, do których licencjodawca ma dostęp w wyniku realizacji przedmiotowej umowy, o których mowa w § 20 ust. 2 pkt 10 rozporządzenia KRI.

(dowód: akta kontroli str. 89 – 91, 92)

2.8 Sposób realizacji określonego w § 20 ust. 2 pkt 13 rozporządzenia KRI obowiązku bezzwłocznego naruszenia bezpieczeństwa informacji został uregulowany w „Instrukcji postępowania w sytuacji naruszenia danych osobowych z dnia 6 lipca 1999 r. W myśl tej instrukcji osoba przetwarzająca dane osobowe była obowiązana do niezwłocznego powiadomienia administratora bezpieczeństwa informacji lub osobę przez niego upoważnioną albo bezpośredniego przełożonego, w przypadku stwierdzenia naruszenia zabezpieczenia systemu informatycznego, gdy stan urządzeń, zawartość zbioru danych, sposób działania programu lub jakość komunikacji w sieci telekomunikacyjnej mogą wskazywać na naruszenie zabezpieczeń danych osobowych, stwierdzenia obecności osób nieupoważnionych w pomieszczeniach, w których przetwarzane są dane osobowe, awarii sprzętu komputerowego służącego do przetwarzania danych, awarii zasilania lub zakłóceń w sieci zasilającej.

(dowód: akta kontroli str. 146)

Pracownicy mieli możliwość zgłaszania przypadków stwierdzenia naruszenia zabezpieczenia systemu informatycznego poprzez system Help Desk bezpośrednio w formie maila do administratora bezpieczeństwa informacji.

(dowód: akta kontroli str. 146, 219 - 221)

2.9 W badanym okresie nie przeprowadzono audytu wewnętrznego z zakresu bezpieczeństwa informacji (§ 20 ust. 2 pkt 14 rozporządzenia KRI). Audyt taki został uwzględniony na rok 2014.

(dowód: akta kontroli str. 97 – 100, 101 – 104, 105 – 108)

2.10 Zasady tworzenia i przechowywania kopii zapasowych nie zostały uregulowane pisemnie (brak PBI).

(dowód: akta kontroli str. 219 - 221)

Kopie zapasowe danych i oprogramowania w Urzędzie tworzone były w dedykowanym oprogramowaniu. Program był skonfigurowany w taki sposób, że kopie zapasowe baz danych tworzone, t.j. codziennie w dni robocze o określonej porze, a kopie zapasowe na nośnikach danych co miesiąc. Kopie zapasowe były przechowywane poza miejscem ich wytwarzania. Pomieszczenia przechowywania kopii zapasowych były właściwie zabezpieczone. Stan taki spełniał wymogi

określone w § 20 ust. 2 pkt 12 lit. b rozporządzenia KRI, dzięki czemu minimalizowano ryzyko utraty informacji w wyniku awarii. Kopie zapasowe były regularnie testowane.

(dowód: akta kontroli str. 222 - 223)

2.11 Badane systemy informatyczne posiadały możliwość udostępniania danych w następujących formatach:

- AZAK - xls,
- Ratusz – raf, txt, xls, wk1, wq1, htm, prn, pdf.

Tym samym spełniony został warunek określony w załączniku nr 2 do rozporządzenia KRI o możliwości zapisywania danych w co najmniej jednym z formatów wymienionych w KRI.

(dowód: akta kontroli str. 115, 116)

Ustalone nieprawidłowości

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

1) W Urzędzie nie opracowano i nie wdrożono Polityki Bezpieczeństwa Informacji, która jest elementem systemu zarządzania bezpieczeństwem informacji. Że w myśl § 20 ust. 3 ww. rozporządzenia, wymagania w zakresie systemu zarządzania bezpieczeństwem informacji uznaje się za spełnione jeżeli została opracowana 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.* W pkt 5.1.1. normy PN-ISO/IEC17799 wskazuje się, aby opracowano i stosowano w Urzędzie dokument polityki bezpieczeństwa informacji. W Urzędzie obowiązywało zarządzenie Nr 21 Prezydenta Miasta Stargardu Szczecińskiego z dnia 2 sierpnia 1999 r. w sprawie instrukcji określającej sposób zarządzania zbiorami danych osobowych. Procedura ta nie dotyczyła jednak wszystkich danych jakie są przetwarzane w Urzędzie, lecz tylko danych osobowych.

(dowód: akta kontroli str. 219 - 221)

Prezydent wyjaśnił*: „Aktualnie funkcjonująca Polityka Bezpieczeństwa Informacji Urzędu Miejskiego (PBI) składa się z rozporządzeń Prezydenta Miasta dotyczących wyznaczenia administratora bezpieczeństwa, sposobu zarządzania danymi osobowymi, postępowania w sytuacji naruszenia ochrony danych osobowych, określenia budynków, pomieszczeń lub ich części tworzących obszar w którym są przetwarzane dane osobowe. Są to elementy PBI które nie były uaktualniane do momentu wejścia w życie rozporządzenia Rady Ministrów w sprawie Krajowych Ram Interoperacyjności, minimalnych wymagań dla rejestrów publicznych i wymiany informacji w postaci elektronicznej oraz minimalnych wymagań dla systemów teleinformatycznych, ponieważ ich zawartość merytorycznie i technicznie nie uległa zmianie. Zapisy zawarte w rozporządzeniach funkcjonują w dalszym ciągu. Po wejściu w życie ww. rozporządzenia został rozszerzony obowiązek utworzenia zestawów procedur bezpieczeństwa i zasad wraz z ich udokumentowaniem, planem wdrożenia i egzekwowania. Dotychczasowa PBI (…) wymagała szczegółowego rozszerzenia poszczególnych zapisów (np. polityka haseł, bezpieczeństwa systemów, kopii awaryjnych, procedur rozpoczęcia i zakończenia pracy, konserwacji, przechowywania i zabezpieczania danych osobowych). W związku z tym został rozpoczęty proces aktualizacji dokumentacji elektronicznej zgodnej z zapisami rozporządzenia. Stworzono szereg nowych dokumentów oraz*

zaktualizowano dotychczasowe. Zakończenie prac związanych z aktualizacją PBI planowane jest w połowie miesiąca września."

(dowód: akta kontroli str. 18 – 19, 20 - 24)

2) W Urzędzie nie przeprowadzano corocznego audytu w zakresie bezpieczeństwa informacji, co było sprzeczne z § 20 ust. 2 pkt 14 rozporządzenia KRI.

(dowód: akta kontroli str. 97 – 100, 101 – 104, 105 – 108)

Prezydent wyjaśnił: *„ Okresowy audyt wewnętrzny bezpieczeństwa informacji planowany jest w ostatnim kwartale bieżącego roku".*

(dowód: akta kontroli str. 224, 225 – 228)

Ocena cząstkowa

Najwyższa Izba Kontroli ocenia pozytywnie mimo stwierdzonych nieprawidłowości działalność Urzędu w badanym obszarze.[6]

3. Zapewnienie dostępności informacji dla osób niepełnosprawnych.

Opis stanu faktycznego

W toku kontroli dokonano weryfikacji zgodności strony internetowej Urzędu Miejskiego w Stargardzie Szczecińskim[7] oraz strony BIP Urzędu[8] ze standardem WCAG 2.0. w zakresie zasady 4-Kompatybilność z uwzględnieniem poziomu A. W jej wyniku ustalono, że strona BIP Urzędu nie zawierała błędów, a strona Urzędu zawierała 75 błędów (narzędzie dostępne na stronie http://jigsaw.w3.org/css-validator). Badanie z wykorzystaniem narzędzia dostępnego na stronie http://validator.w3.org wykazało 8 błędów dla strony BIP Urzędu i 8 błędów dla strony Urzędu.

(dowód: akta kontroli str. 4 – 11, 12 - 17)

Prezydent Miasta Stargard Szczeciński podał m.in., że po wejściu na stronę www Urzędu istnieje możliwość odczytania zamieszczonego tam tekstu, przy użyciu syntezatora mowy IVONA.

(dowód: akta kontroli str. 18 – 19, 21)

Ocena cząstkowa

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

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[9], wnosi o: opracowanie i wdrożenie Polityki Bezpieczeństwa Informacji, określającej zasady bezpieczeństwa informacji, zgodnej z normą PN-ISO/IEC.

---

[6] Mimo braku sformalizowanej PBI oraz nieprzeprowadzania corocznego audytu w zakresie bezpieczeństwa informacji w Urzędzie sporządzano kopie zapasowe systemów i danych operacyjnych i prawidłowo zabezpieczano nośniki tych kopii. Pracownikom zapewniono szkolenia z zakresu bezpieczeństwa informacji oraz zapobiegano możliwości nieautoryzowanego zainstalowania oprogramowania.

[7] http://www.stargard.pl.

[8] http://www.bip.um.stargard.pl.

[9] Dz. U. z 2012 r., poz. 82 ze zm., zwana dalej: „ustawą o NIK".

V. Pozostałe informacje i pouczenia

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

Prawo zgłoszenia zastrzeżeń

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

Obowiązek poinformowania NIK o sposobie wykonania wniosków

Zgodnie z art. 62 ustawy o NIK proszę o poinformowanie Najwyższej Izby Kontroli, w terminie 21 dni od dnia otrzymania wystąpienia pokontrolnego, o sposobie wykonania wniosku pokontrolnego 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.

Szczecin, dnia października 2014 r.

Najwyższa Izba Kontroli
Delegatura w Szczecinie

Kontroler
Agata Prochotta-Miłek
Specjalista k.p.

.....
podpis

.....
podpis