OR. 1710. 9. 2014

NAJWYŻSZA IZBA KONTROLI
Delegatura w Szczecinie

ul. A. Frątczak 1 Cz.

URZĄD MIASTA SZCZECINEK
Biuro Obsługi Interesanta
wpł. 06-10-2014
Nr 8401
przydzielono OR. termin.

LSZ - 4101-011-01/2014
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

Kontrolerzy

Agata Prochotta Miłek, specjalista kontroli państwowej, upoważnienie do kontroli nr 90592 z dnia 26.06.2014 r. Tomasz Cyranka, główny specjalista kontroli państwowej, upoważnienie do kontroli nr 90602 z dnia 23.07.2014 r.

(dowód: akta kontroli str. 1 – 2, 11 - 12)

Jednostka kontrolowana

Urząd Miasta w Szczecinku, Plac Wolności 13, 78-400 Szczecinek, REGON 330920890, (dalej: Urząd).

Kierownik jednostki kontrolowanej

Jerzy Hardie - Douglas, Burmistrz Miasta Szczecinek (dalej: Burmistrz).

(dowód: akta kontroli str. 3)

II. Ocena kontrolowanej działalności

Ocena ogólna

Uzasadnienie oceny ogólnej

Burmistrz Miasta Szczecinek realizując w okresie od 31 maja 2012 r. do 28 lipca 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 trzema (z czterech wybranych do badania) systemami informatycznymi w sposób spełniający minimalne wymogi w zakresie interoperacyjności, w szczególności poprzez wzajemną komunikację oraz udostępnianie we wszystkich czterech badanych systemach danych w formatach określonych w ww. rozporządzeniu,

- opracował i zatwierdził Polityką Bezpieczeństwa Informatycznego,

- spełnił w odniesieniu do strony internetowej Urzędu i strony BIP wymagania, sformułowane w rozporządzeniu KRI, dotyczące dostosowania systemów prezentujących treści do wymagań w zakresie ich dostępności dla osób niepełnosprawnych[2].

Stwierdzone w toku kontroli nieprawidłowości dotyczyły:

- braku interoperacyjności systemu FK 2, który nie współpracował z żadnym innym systemem w Urzędzie, a tym samym nie spełniał minimalnych wymogów

[1] Dz. U. z 2012 r., poz. 526.
[2] Wymagania w zakresie Web Content Accesisbility Guideliness (WCAG 2.) określone w załączniku nr 4 do rozporządzenia KRI.

interoperacyjności w zakresie współpracy z innymi systemami funkcjonującymi w Urzędzie, o których mowa w § 5 ust. 3 pkt 3 rozporządzenia KRI,

- nieprzeprowadzania okresowych aktualizacji Polityki Bezpieczeństwa Informatycznego w okresie od 19 września 1999 r. do 24 czerwca 2014 r. wymaganej przepisami § 20 ust. 2 pkt 1 rozporządzenia KRI,

- nieograniczenia na 10 (z badanych 14) zestawach komputerowych możliwości instalowania nieautoryzowanego oprogramowania, co było sprzeczne z zaleceniem zawartym w załączniku A do normy PN-ISO/EC 27001:2007 w punkcie A.11.2.2, stwierdzającym, że należy ograniczyć i kontrolować przyznawanie i korzystanie z przywilejów w systemach informatycznych,

- nieprzeszkolenia w badanym okresie pracowników zaangażowanych w proces przetwarzania informacji w zakresie szyfrowania dysków, szyfrowania kluczy USB, dostępu do systemów IT po podaniu hasła, co stanowiło wymóg § 20 ust. 2 pkt 6 rozporządzenia KRI.

III. Opis ustalonego stanu faktycznego

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

Opis stanu faktycznego

1.1. Strategia Rozwoju Miasta Szczecinek na lata 2008 – 2017[3] w ramach celu strategicznego „Poprawa życia i sytuacji materialnej mieszkańców, rozwiązywanie problemów społecznych" zawierała program „Infrastruktura społeczeństwa informacyjnego". W ramach tego programu przyjęto w Strategii projekt „Intensyfikacja rozwoju społecznego i gospodarczego poprzez poprawę warunków dostępu do Internetu, rozwoju komunikacji, a przez to poprawę warunków dostępu do informacji publicznej, publicznych e-usług świadczonych drogą elektroniczną oraz gospodarki elektronicznej".

(dowód: akta kontroli str. 85)

1.2. Burmistrz wyjaśnił, że *„Promocja komunikacji elektronicznej jako metody kontaktu z interesantem prowadzona jest regularnie. Najczęstszym sposobem promocji komunikacji elektronicznej są programy samorządowe Urzędu Miasta emitowane w dwóch lokalnych telewizjach kablowych (Gawex Media i TV Zachód), w których mieszkańcy Szczecinka informowani są na bieżąco o możliwości załatwienia spraw administracyjnych drogą elektroniczną. Analogicznie do przekazu telewizyjnego, o możliwościach elektronicznej komunikacji z urzędem, informujemy również poprzez współpracę z lokalnymi portalami internetowymi, które działają na terenie naszego miasta. Kolejnym kanałem dystrybucji jest miejska strona internetowa, na której zamieszczane są regularnie informacje związane z elektroniczną metodą komunikacji z urzędem."*

(Dowód: akta kontroli str. 4, 6)

1.3. W sprawie ankiet i innych form rozpoznania potrzeb mieszkańców dotyczących korzystania z elektronicznej formy komunikacji z Urzędem Burmistrz wyjaśnił: *„Dokonywane są analizy e-maili przychodzących na adres ogólny poczty*

[3] Strategia Rozwoju Miasta Szczecinek została przyjęta przez Radę Miasta Szczecinek uchwałą nr XII/164/08 w dniu 28 stycznia 2008 r. Uchwała weszła w życie z dniem jej podjęcia.

elektronicznej Urzędu z uwagami i sugestiami dotyczącymi komunikacji elektronicznej z Urzędem oraz rozpatrywane są uwagi i propozycje pojawiające się w czasie rozmów telefonicznych".

(dowód: akta kontroli str. 4, 6)

1.4. Ze złożonych przez Burmistrza wyjaśnień wynika, że po wejściu w życie rozporządzenia KRI nie zwracano się do Ministra Administracji i Cyfryzacji z problemami bądź z prośbą o pomoc w zakresie dostosowania swoich systemów/ rejestrów informatycznych do wymogów KRI.

(dowód: akta kontroli str. 4, 6)

1.5. W Urzędzie, w celu zarządzania obiegiem dokumentów i dokumentacją, stosowane są 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] (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 82/2011 Burmistrza Miasta Szczecinek z dnia 7 lipca 2011 r. w sprawie ustalenia zadań wynikających z instrukcji kancelaryjnej.

(dowód: akta kontroli str. 13 – 14, 15)

Z 1.406 dokumentów w formie elektronicznej, które w badanym okresie wpłynęły do Urzędu, badaniem szczegółowym objęto 10 dokumentów stwierdzając, że po wpływie do Urzędu poprzez elektroniczną skrzynkę podawczą lub e-usługę „Składanie skarg i wniosków", dokumenty były drukowane, a następnie procedowane jako dokumenty papierowe. Ich elektroniczne oryginały pozostają na serwerze Urzędu bądź na platformie ePUAP.

(dowód: akta kontroli str. 31 - 64, 86)

1.6. W badanym okresie do Urzędu wpłynęło łącznie 61.789 dokumentów, z czego 1.406 w formie elektronicznej (tj. 2,28%). Obywatele wnieśli łącznie 36.711 dokumentów (z czego 18 w formie elektronicznej, tj. 0,05%), osoby prawne lub inne podmioty 13.890 dokumentów (z czego 266 w formie elektronicznej, tj. 1,92%), inne urzędy 11.188 dokumentów (z czego 1.122 w formie elektronicznej, tj. 10,03%). W tym samym okresie Urząd przekazał łącznie 97.571 dokumentów (z czego 600 w formie elektronicznej, tj. 0,61%). Obywatelom przekazał łącznie 74.598 dokumentów (z czego 12 droga elektroniczną, tj. 0,02%), osobom prawnym lub innym podmiotom 10.039 dokumentów (z czego 95 w formie elektronicznej, tj. 0,95%) i innym urzędom 12.934 (z czego 493 w formie elektronicznej, tj. 3,81%).

(Dowód: akta kontroli str. 16)

1.7. W badanym okresie Urząd świadczył usługę elektroniczną, z wykorzystaniem platformy e-PUAP (Elektroniczna Platforma Usług Administracji Publicznej), tj. „Skargi, wnioski, zapytania do urzędu" (elektroniczna skrzynka podawcza). Poprzez stronę BIP (Biuletyn Informacji Publicznej) Urzędu, w zakładce Poradnik interesanta – Procedury załatwiania spraw umieszczone były karty usług. Przedmiotowe karty pozwalały na wykonanie części czynności drogą elektroniczną. Badaniem szczegółowym objęto następujące karty usług:

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

- wpis do rejestru działalności regulowanej przedsiębiorców prowadzących działalność z zakresie odbierania odpadów komunalnych,
- wydanie decyzji o warunkach zabudowy,
- ustalenie i odtworzenie aktu stanu cywilnego,
- wydawanie zaświadczenia potwierdzającego dzierżawienie gruntu,
- zezwolenie na utrzymanie psów ras agresywnych.

Karty powyższych usług oraz usługi „Skargi, wnioski, zapytania do urzędu" były zgodne z ich opisem zamieszczonym na stronie internetowej BIP Urzędu. Wnioski oraz zeskanowane załączniki można było przesłać korzystając z elektronicznej skrzynki podawczej na platformie e-PUAP. W pięciu badanych przypadkach, dla których część czynności Urząd umożliwiał wykonanie przez elektroniczną skrzynkę podawczą, formą załatwienia sprawy był odbiór osobisty zezwolenia, zaświadczenia bądź decyzji administracyjnej lub jej odbiór drogą pocztową za potwierdzeniem odbioru. W przypadku karty „Skargi, wnioski, zapytania do urzędu", formą zadławienia sprawy było: w przypadku skarg, wniosków - zawiadomienie o sposobie załatwienia skargi, w pozostałych przypadkach - zgodnie z przepisami obowiązującymi w danej kategorii spraw.

(Dowód: akta kontroli str. 17 – 18, 65 – 84, 85 – 86,242)

1.8. Badanie zapisów procedur dotyczących pięciu usług (procedury opisane w kartach usług na stronie BIP Urzędu), dla których część czynności Urząd umożliwiał wykonanie przez elektroniczną skrzynkę podawczą 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[5] - dane dotyczące: podmiotu świadczącego usługę, miejsca świadczenia usługi, aktualnej podstawy prawnej, sposobu realizacji usługi.

(dowód: akta kontroli str. 65 - 84)

1.9. Do Centralnego Repozytorium Wzorów Dokumentów ePUAP przekazano wzór dokumentu opisujący korzystanie z elektronicznej skrzynki podawczej „Skargi, wnioski, zapytania do urzędu".

(dowód: akta kontroli str. 17 – 18, 19 – 20)

1.10. Ustalono, że w procesie zarządzania usługą „Skargi wnioski, zapytania do urzędu" oraz usługami, dla których część czynności można wykonać poprzez elektroniczną skrzynkę podawczą urzędu na platformie e-PUAP, 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 kartę opisu usługi, w której określono właściciela usługi (komórkę organizacyjną urzędu), aktualną podstawę prawną, wymagane dokumenty, tryb odwoławczy i wymagane dokumenty.

Zarządzanie usługami realizowanymi przez badane systemy teleinformatyczne odbywa się w oparciu o udokumentowane w Polityce Bezpieczeństwa Informatycznego procedury niezbędne dla określenia zakresu i sposobu świadczenia usług elektronicznych z wykorzystaniem systemów informatycznych.

---

[5] 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).

Dla objętych badaniem szczegółowym pięciu usług Urząd posiadał spisane wewnętrzne karty wymagań dla usług, co umożliwiało ustalenie wewnątrz Urzędu właściciela tych usług na poziomie wydziału. Dla usług elektronicznych świadczonych poprzez stronę BIP Urzędu zawarto z firmą zewnętrzną umowę o utrzymanie Biuletynu Informacji Publicznej. W umowie tej określono m.in. maksymalny czas niedostępności strony BIP oraz sposób zgłaszania błędów w jej działaniu (numer telefonu, stronę internetową).

(Dowód: akta kontroli str. 65 – 84, 108 – 109, 240 - 241)

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

- GOMiG – Moduł Wymiarowy wersja 4.13.0.638; system służący rejestracji/ aktualizacji deklaracji o wysokości opłat za zagospodarowanie odpadami komunalnymi (dalej: GOMiG),

- FK2 – wersja 1.1.9A z dnia 30.06.2014 r.; system służący do rejestracji mandatów (dalej: FK2),

- System Rozliczania Tytułów Wykonawczych Taxi+, wersja v.12.2.13.2; system służący do rozliczania tytułów wykonawczych dotyczący opłat za zagospodarowanie odpadów komunalnych (dalej: Taxi+),

- FORTIS – Wydawanie licencji na przewóz osób taxi i zezwoleń na przewozy regionalne osób (komunikacja miejska), wersja 1.18.30 (dalej: FORTIS).

(dowód: akta kontroli str. 21, 89 - 108)

System GOMiG automatycznie przesyła dane z deklaracji o wysokości opłaty za zagospodarowanie odpadami komunalnymi do systemu Gmina 2 (system finansowo - księgowy w Urzędzie). Komunikacja jest jednostronna, dane z jednego systemu są przekazywane do innego systemu za pośrednictwem pracownika – operatora systemu, który ręcznie wprowadza dane do systemu GOMiG i są one widoczne w systemie Gmina 2.

System Taxi+ jednostronnie komunikuje się z systemem Gmina 2, tzn. że pracownik automatycznie importuje dane w zakresie tytułu wykonawczego z systemu Gmina 2 do systemu Taxi+ i generuje tytuły wykonawcze.

System FORTIS jednostronnie komunikuje się z systemem CEIDG, tzn. że pracownik ręcznie wprowadza dane z wniosków o udzielenie licencji na wykonywanie transportu drogowego do systemu FORTIS i eksportuje je ręcznie do systemu CEIDG. Pracownik ma możliwość podglądu, czy dane zostały prawidłowo zaimportowane przez system CEIDG. System FORTIS współpracuje tylko z tym zewnętrznym systemem informatycznym, nie komunikuje się z żadnym innym systemem w Urzędzie.

System FK 2 nie komunikuje się z żadnym innym systemem w Urzędzie (brak interoperacyjności), tzn. pracownik ręcznie wprowadza dane do systemu, a system pozwala na wygenerowanie raportu w formie wydruku. Tym samym system FK 2, w przeciwieństwie do trzech systemów opisanych powyżej, nie spełniał minimalnych wymogów interoperacyjności w zakresie współpracy z innymi systemami funkcjonującymi w Urzędzie, o których mowa w § 5 ust. 3 pkt 3 rozporządzenia KRI.

(Dowód: akta kontroli str. 89 – 108)

1.12. W sprawie procedur i praktyk postępowania stosowanych we współpracy z innymi jednostkami administracji publicznej Burmistrz wyjaśnił: *„W Urzędzie*

odbywa się elektroniczna komunikacja z innymi jednostkami administracji publicznej za pośrednictwem ePUAP oraz PIA (Platforma Informacyjna Administracji). Dodatkowo pracownicy Urzędu kontaktują się z ww. jednostkami za pośrednictwem poczty elektronicznej. Urząd nie zwracał się do innej jednostki administracji publicznej z wnioskiem o prowadzenie wzajemnej komunikacji elektronicznej. (...) Wystąpiła sytuacja, że inny organ administracji publicznej zwrócił się do tutejszego Urzędu z prośbą o prowadzenie wzajemnej wymiany elektronicznej w sprawach prowadzonych przez ten organ".

(Dowód: akta kontroli str. 4, 6)

Burmistrz wyjaśnił, że w odpowiedzi poinformowano, iż w tutejszym Urzędzie podstawowym sposobem dokumentowania przebiegu załatwiania i rozstrzygania spraw w Urzędzie jest tradycyjny system wykonywania czynności kancelaryjnych. W przypadku doręczenia pisma za pomocą środków komunikacji elektronicznej, które organ złożył przez elektroniczną skrzynkę podawczą Urzędu lub w którym wystąpił o doręczenie odpowiedzi w formie dokumentu elektronicznego, Urząd przekaże odpowiedź w żądanej formie. W innym przypadku, korespondencja wychodząca z Urzędu jest w formie papierowej.

Z wyjaśnień Burmistrza wynika, że Urząd prowadził korespondencję za pomocą platformy ePUAP z:

1) Zachodniopomorskim Urzędem Wojewódzkim m.in. w zakresie spraw obywatelskich, urzędu stanu cywilnego, spraw dot. pomocy społecznej, przyznanych dotacji i zarządzania kryzysowego,
2) innymi jednostkami administracji publicznej – wymiana korespondencji dot. zadań Miasta,
3) urzędami skarbowymi – sprawozdania budżetowe.

Ponadto Urząd przesyła dane statystyczne dot. urodzeń, małżeństw i zgonów do GUS, sprawozdania budżetowe do RIO oraz wymienia dane za pomocą portalu PIA z Zachodniopomorskim Urzędem Wojewódzkim (zmiany meldunkowe) oraz z Ministerstwem Spraw Wewnętrznych (nadanie/ zmiana/ usunięcie numeru Pesel).

Wyżej opisany system FORTIS komunikował się jednostronnie z systemem zewnętrznym CEDIG.

(dowód: akta kontroli str. 22, 23 – 24, 105 - 107)

Ustalone nieprawidłowości

W działalności kontrolowanej jednostki w przedstawionym wyżej zakresie stwierdzono następującą nieprawidłowość:

System FK-2 nie współpracował z żadnym innym systemem w Urzędzie (brak interoperacyjności), a tym samym nie spełniał minimalnych wymogów interoperacyjności w zakresie współpracy z innymi systemami funkcjonującymi w Urzędzie, o których mowa w § 5 ust. 3 pkt 3 rozporządzenia KRI.

Burmistrz wyjaśnił: *„System FK-2 obecnie jest dostosowywany do komunikacji z systemami Straży Miejskiej w Szczecinku: eMANDATY i MANDATY-SUMPRO. Systemy te również są w trakcie modernizacji i opracowywania nowych modułów umożliwiających wyprowadzanie danych. Końcowym efektem prac będzie możliwość zaczytywania plików wyprowadzonych z ww. systemów Straży, co wyeliminuje ręczne wprowadzanie danych. Na dzień dzisiejszy trwają prace testowe, sprawdzające poprawność zaczytywanych plików z systemów zewnętrznych".*

Ocena cząstkowa

Najwyższa Izba Kontroli ocenia pozytywnie, mimo stwierdzonej nieprawidłowości, działalność kontrolowanej jednostki w zbadanym zakresie.

2. Wdrożenie systemu zarządzania bezpieczeństwem systemów informatycznych

Opis stanu faktycznego

2.1. Urząd opracował i wdrożył w praktyce, zatwierdzoną przez Burmistrza, Politykę Bezpieczeństwa Informacji (załącznik nr 2 do zarządzenia Burmistrza Nr 65/2014 z dnia 24 czerwca 2014 r., dalej PBI). Jako administrator danych w PBI wyznaczony został Burmistrz Miasta Szczecinek. Administratorem bezpieczeństwa informacji w badanym okresie wyznaczona została przez Burmistrza Pani Joanna Gawrych, Dyrektor Wydziału Organizacyjnego. Administrator Bezpieczeństwa Informacji odpowiadał również za przegląd PBI wykonywany nie rzadziej niż raz na sześć miesięcy.

(dowód: akta kontroli str. 85 – 86, 110, 111)

Poprzednio obowiązujące zarządzenie nr 11/99 Burmistrza Miasta Szczecinka z dnia 14.09.1999r. w sprawie ustalenia instrukcji regulującej sprawy ochrony danych osobowych zawartych w systemach eksploatowanych w sieci Novell NetWare w Urzędzie Miasta Szczecinek nie było aktualizowane. Zapewnienie aktualizacji regulacji wewnętrznych w zakresie zmieniającego się otoczenia stanowi wymóg §20 ust. 2 pkt 1 rozporządzenia KRI.

(Dowód: akta kontroli str. 112 – 120)

2.2. Inwentaryzacja zasobów informatycznych Urzędu była prowadzona w plikach programu Excel. Badaniem szczegółowym objęto zapisy w ewidencji dotyczące łącznie 14 zestawów komputerowych oraz jednego serwera. Dane dotyczące badanych zestawów komputerowych zawierały m.in. informacje o jednostce Urzędu, w której znajduje się zestaw, osobie, która obsługuje komputer (imię i nazwisko, profil), typie, producencie, pamięci RAM, kartach audio i video, sieci LAN, monitorze oraz zainstalowanym oprogramowaniu. Dane dotyczące badanego serwera zawierały m.in. informacje o jednostce organizacyjnej Urzędu, w której znajduje się serwer, nazwie, typie, producencie, pamięci RAM połączeniu LAN, karcie video oraz zainstalowanym oprogramowaniu.

(dowód: akta kontroli str. 121 – 125, 126)

Przeprowadzone w dniu 9 lipca 2014 r. badanie możliwości zainstalowania nieautoryzowanego oprogramowania na 10 wybranych losowo komputerach Urzędu wykazało, że użytkownicy systemów informatycznych niebędący pracownikami służb informatycznych posiadali uprawnienia administracyjne w związku z czym mogli samodzielnie instalować oprogramowanie na komputerach służbowych. Zalecenia zawarte w załączniku A do normy PN-ISO/EC 27001:2007 w punkcie A.11.2.2 stanowią, że należy ograniczyć i kontrolować przyznawanie i korzystanie z przywilejów w systemach informatycznych.

(dowód: akta kontroli str. 127 – 129)

Przeprowadzone w dniu 16 lipca 2014 r. badanie możliwości zainstalowania na czterech komputerach, które Urząd otrzymał w ramach realizacji projektu „pl.ID – 'Polska ID karta" wykazało, że na żadnym z badanych komputerów użytkownicy niebędący pracownikami służb informatycznych nie mogli zainstalować dowolnego oprogramowania.

(dowód: akta kontroli str. 142 – 147)

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. 148, 149)

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

(dowód: akta kontroli str. 150 – 151, 152 – 181)

Nadawanie, modyfikowanie i odbieranie uprawnień w systemach informatycznych było realizowane w oparciu o przyjętą w Urzędzie PBI, rozdział 3 „Organizacja przetwarzania danych osobowych" oraz Instrukcja zarządzania systemem informatycznym służącym do przetwarzania danych osobowych w Urzędzie Miasta Szczecinek (będąca załącznikiem nr 2 do ww. zarządzenia nr 65/2014 Burmistrza Miasta Szczecinek), zgodnie z § 20 ust. 2 pkt 4 i 5 rozporządzenia KRI. O uprawnieniach pracowników w systemach informatycznych decydowali kierownicy komórek organizacyjnych poprzez złożenie odpowiedniego wniosku do administratora danych i załączali do niego upoważnienie do przetwarzania danych osobowych. Dokonano sprawdzenia zablokowania dostępu do systemów informatycznych dla dwóch 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. 85 – 86, 182,183 – 194, 195 - 202)

2.5. W badanym okresie Urząd nie zapewnił szkolenia pracowników zaangażowanych w proces przetwarzania informacji, co stanowiło wymóg § 20 ust. 2 pkt 6 rozporządzenia KRI.

(dowód: akta kontroli str. 85 – 86)

2.6. W PBI w rozdziale 6 „Przetwarzanie danych osobowych na komputerach przenośnych" ustalono (zgodnie z § 20 ust. 2 pkt 8 rozporządzenia KRI) podstawowe zasady w zakresie bezpiecznej pracy użytkowników przy wykorzystaniu komputerów przenośnych. Zgodnie z zapisami PBI wyniesienie komputera przenośnego poza teren Urzędu wymaga bezwzględnej zgody administratora danych lub administratora bezpieczeństwa informacji. Komputery przenośne przetwarzające dane osobowe pozostają zawsze pod opieką upoważnionego pracownika. W badanym okresie pracownicy Urzędu posiadali trzy urządzenia mobilne.

(dowód: akta kontroli 183 – 194, 195 – 202)

2.7. W okresie objętym kontrolą, tj. od 31.05.2012 r. do 29.07.2014 r. Urząd zakupił 31 komputerów. We wszystkich umowach zakupu ww. komputerów ich integralną częścią były oferty ostatecznie wybranego dostawcy. W ofertach tych zawarto następujące oświadczenie „Oświadczam, że w przypadku awarii dysku twardego, dysk pozostaje u Zamawiającego". Urząd nie serwisuje swojego sprzętu IT w serwisie zewnętrznym – poza drukarkami.

(dowód: akta kontroli str. 85 – 86)

W czterech umowach licencyjnych i serwisowych, jakie w badanym okresie Urząd zawarł z dostawcami systemów, które zostały opisane w punkcie 1.11 niniejszego wystąpienia pokontrolnego, tylko w dwóch umowach z firmą Rewucki (z dnia 18 czerwca 2013 r. oraz 7 lipca 2014 r. zawarto klauzule zapewniające poufność

wszystkich danych licencjobiorcy, do których licencjodawca ma dostęp w wyniku przedmiotowej umowy, o których mowa w § 20 ust. 2 pkt 10 rozporządzenia KRI. W pozostałych trzech umowach brak było takich zapisów.

(dowód: akta kontroli str. 203 – 205, 206 – 209, 210 – 216, 217 – 218, 219 – 220)

Burmistrz wyjaśnił: *Umowy licencyjne z Informicą i Arisco Sp. z o. o. dotyczą tylko udzielenia licencji na zakupiony produkt, nie dotyczą serwisowania tych programów. Jest to tylko potwierdzenie, że Urząd może legalnie korzystać z oprogramowania. Umowa z 26 marca 2013 r. zawarta z ZETO Sp. z o. o. w Koszalinie dotyczy serwisu systemu do księgowania mandatów FK-2. Wykonawca (ZETO) nie ma dostępu do danych zapisywanych w programie. Wszelkie uwagi zgłaszane są telefonicznie bądź za pomocą e-mail, po czym Wykonawca przesyła aktualizację na adres e-mail, którą pracownik Urzędu wgrywa do wskazanego katalogu".*

(dowód: akta kontroli str. 22, 23)

2.8. Sposób realizacji określonego w § 20 ust. 2 pkt 13 rozporządzenia KRI obowiązku bezzwłocznego zgłaszania naruszenia bezpieczeństwa informacji został uregulowany w PBI rozdział 4 „Postępowanie w przypadku stwierdzenia naruszenia bezpieczeństwa przetwarzania danych osobowych". Zgodnie z jego zapisami administrator bezpieczeństwa informacji jest obowiązany poinformować administratora danych o przypadkach naruszenia zasad PBI. Każdy pracownik jest obowiązany powiadomić bezpośredniego przełożonego lub administratora bezpieczeństwa informacji o każdym naruszeniu lub zaistnieniu okoliczności wskazujących na naruszenie ochrony danych osobowych. Z faktu naruszenia bezpieczeństwa przetwarzania danych osobowych administrator bezpieczeństwa informacji sporządza raport zgodnie ze wzorem określonym w załączniku nr 8 do PBI i przekazuje go administratorowi danych. Pracownicy przetwarzający dane osobowe zostali zobowiązani do zapoznania się z treścią ww. zarządzenia nr 65/2014 oraz przestrzegania PBI i Instrukcji zarządzania systemem informatycznym służącym do przetwarzania danych osobowych w Urzędzie Miasta Szczecinek.

(dowód: akta kontroli str. 183 – 194)

2.9. W badanym okresie nie przeprowadzono audytu wewnętrznego z zakresu bezpieczeństwa informacji (§ 20 ust. 2 pkt 14 rozporządzenia KRI). Audytor wewnętrzny Urzędu został zatrudniony z dniem 1 czerwca 2013 r. w wymiarze pół etatu. Poprzednie nabory na to stanowisko nie powiodły się, ponieważ kandydaci nie spełniali kryteriów formalnych. W toku kontroli NIK Burmistrz zwrócił się pismem z dnia 2 lipca 2014 r. do audytora wewnętrznego Urzędu z poleceniem przeprowadzenia poza planem audytu zadania audytowego w zakresie bezpieczeństwa informacji.

(dowód: akta kontroli str. 221 – 222, 223 – 232, 233, 234, 242)

2.10. Procedury tworzenia i przechowywania kopii zapasowych regulują rozdziały 5 (Procedury tworzenia kopii zapasowych zbiorów danych oraz programów i narzędzi programowych służących do ich przetwarzania) oraz 6 (Sposób, miejsce i okres przechowywania elektronicznych nośników informatycznych zawierających dane osobowe oraz kopii zapasowych).

(dowód: akta kontroli str. 195 – 202)

Kopie zapasowe danych i oprogramowania są w Urzędzie tworzone w dedykowanym oprogramowaniu. Ustawienia programu potwierdziły, że kopie zapasowe baz danych tworzone są codziennie 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. W badanym okresie kopie zapasowe były testowane sześciokrotnie.

(dowód: akta kontroli str. 235, 236, 237, 243)

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

- TAXI+: format (bazodanowy) txt po wykonaniu wpisanego polecenia SQL,
- Fortis: rtf i pdf,
- GOMiG: pdf i csv
- FK 2: xml.

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

(dowód: akta kontroli str. 89, 90, 96, 105)

Ustalone nieprawidłowości

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

1) W okresie od 14 września 1999 r. do 24 czerwca 2014 r. w Urzędzie nie przeprowadzono aktualizacji PBI, czym naruszono wymogi § 20 ust. 2 pkt 1 rozporządzenia KRI, mówiące o aktualizacji regulacji wewnętrznych w zakresie zmieniającego się otoczenia. W ocenie NIK przy dzisiejszym postępie technologicznym należy przyjąć, że PBI powinna być poddawana przeglądom nie rzadziej niż raz na sześć miesięcy.

(dowód: akta kontroli str. 110, 111, 112 – 120)

W sprawie nieprzeprowadzania aktualizacji PBI w okresie od 14.09.1999 r. do 24.06.2014 r. Burmistrz wyjaśnił: *„Odpowiedzialność za spełnienie przepisów prawa ochrony danych osobowych ponosi Burmistrz, jako administrator danych osobowych. W celu zapewnienia właściwej realizacji zadań przez pracowników i innych uprawnionych użytkowników (stażyści), wdrożona została procedura ochrony danych i informacji jako proporcjonalna odpowiedzialność wszystkich uczestników procesu przetwarzania danych. Zarządzeniem Nr 11/99 Burmistrza Miasta Szczecinka z dnia 14 września 1999 r. wprowadzono zasady przetwarzania i zabezpieczenia danych osobowych w Urzędzie Miasta. (...) Odpowiedni poziom wymaganej przepisami dokumentacji (procedur) ochrony danych osobowych jako szczególnie wrażliwej informacji o osobach, których dane dotyczy określono w wewnętrznej dokumentacji, adekwatnie do potrzeb Urzędu, w oparciu o potencjalne zagrożenia (zdefiniowane w okresie poprzedzającym wdrożenie i w trakcie obowiązywania przepisów). (...) W okresie obowiązywania, wewnętrzne przepisy ochrony danych spełniały warunki adekwatności i proporcjonalności przetwarzania danych w zdefiniowanym środowisku potencjalnych zagrożeń (fizycznych i środowiskowych)."*

(dowód: akta kontroli str. 4, 7 – 8)

2) Na 10 z 14 poddanych badaniu zestawach komputerowych można było zainstalować nieautoryzowane oprogramowanie, co naruszało przepisy § 20 ust. 2 pkt 7c rozporządzenia KRI, który nakłada na kierownictwo podmiotu publicznego realizację i egzekwowanie zapewnienia środków uniemożliwiających nieautoryzowany dostęp na poziomie systemów operacyjnych, usług sieciowych

i aplikacji. Stan ten był niezgodny także z powszechnie przyjętą praktyką określoną w Załączniku A normy PN-ISO/IEC 27001:2007, punkt A.11.2.2, który stanowi, że należy ograniczyć i kontrolować przyznawanie i korzystanie z przywilejów w systemach informatycznych.

(dowód: akta kontroli str. 127 – 129)

Burmistrz wyjaśnił: *„Cztery komputery, spośród badanych dziesięciu komputerów, które podlegały badaniu przeprowadzonym 9 lipca 2014 r., przypisane są pracownikom wyższej kadry zarządzającej o najwyższej świadomości użytkowników. Na tych stanowiskach wymagana jest odpowiedzialność również w dziedzinie korzystania ze sprzętu technologii informatycznej. Czas pracy tych osób wykracza poza standardowe godziny pracy, co może skutkować potrzebą indywidualnej - osobistej instalacji specyficznego oprogramowania. Przyjęto założenie, że najwyższe kierownictwo ma uprawnienia administratora systemu. Na pozostałych sześciu komputerach, z uwagi na wymagane przez oprogramowanie specjalistyczne (branżowe) uprawnienia w dostępnie do systemu operacyjnego, zaistniała konieczność posiadania uprawnień administratora systemu. Ponadto każdy pracownik Urzędu podpisał oświadczenie o przestrzeganiu Polityki bezpieczeństwa informacji i Instrukcji zarządzania systemem informatycznym służącym do przetwarzania danych osobowych w Urzędzie Miasta Szczecinek i zobowiązał się do ich przestrzegania. Dodatkowo w zakresie obowiązków pracownika, w dziale „Odpowiedzialność" wprowadzony został zapis: „Materialna odpowiedzialność za powierzony sprzęt komputerowy i zainstalowane oprogramowanie oraz jego prawidłowe wykorzystywanie", który pracownik przyjął do wiadomości i stosowania".*

(dowód: akta kontroli str. 130, 131)

W ocenie NIK, wskazane przez Burmistrza działania nie gwarantowały bezpiecznej pracy w systemie informatycznym. Potrzeba ograniczenia uprawnień związana jest z minimalizacją ryzyka polegającego m.in. na możliwości nieświadomego zainstalowania przez użytkownika złośliwego oprogramowania dokonanego w trakcie przeglądania stron internetowych.

3) W badanym okresie Urząd wbrew wymogom § 20 ust. 2 pkt 6 rozporządzenia KRI nie zapewnił szkolenia pracowników zaangażowanych w proces przetwarzania informacji.

(dowód: akta kontroli str. 85 – 86)

Burmistrz wyjaśnił: *„Pracownikom nie zapewniono szkoleń dotyczących zagrożenia bezpieczeństwa informacji, skutków naruszenia bezpieczeństwa informacji, stosowania środków zapewniających bezpieczeństwo informacji ze względu na wysokie koszty takich szkoleń oferowane do tej pory przez firmy zewnętrzne. Budżet przeznaczony na szkolenia jest ograniczony i Urząd na dzień dzisiejszy nie może pozwolić sobie na wydatkowanie tak dużej kwoty na przeszkolenie wszystkich pracowników z ww. tematyki. W związku z ograniczonymi kosztami zapewniono pracownikom szkolenia wewnętrzne z zakresu ustawy ODO. Niektórzy pracownicy Urzędu brali udział w szkoleniach on-line z tematyki bezpieczeństwa informacji, jednakże z takich szkoleń nie otrzymywali potwierdzenia odbycia szkolenia. Celem podniesienia poziomu wiedzy oraz świadomości istniejących zagrożeń sukcesywnie przeprowadzamy okresowe szkolenia wewnętrzne pracowników z tematyki bezpieczeństwa informacji w grupach, w skład których wchodzą wytypowani pracownicy poszczególnych komórek organizacyjnych, bądź też pracownicy wybranych komórek.*

(dowód: akta kontroli str. 22, 23)

Uwagi dotyczące badanej działalności

Zdaniem NIK należałoby w PBI w większym stopniu niż ma to aktualnie miejsce uwzględnić bezpieczeństwo wszystkich danych przetwarzanych w Urzędzie w systemach informatycznych. Bezpieczeństwo informatyczne nie obejmuje bowiem wyłącznie danych osobowych.

Ocena cząstkowa

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

3. Zapewnienie dostępności informacji dla osób niepełnosprawnych.

Opis stanu faktycznego

W toku kontroli dokonano weryfikacji zgodności strony internetowej Urzędu Miasta Szczecinek[6] oraz strony BIP Urzędu[7] ze standardem WCAG 2.0. w zakresie zasady 4-Kompatybilność z uwzględnieniem poziomu A. W jej wyniku ustalono, że strona internetowa Urzędu nie zawierała błędów. Na stronie BIP Urzędu wystąpiły 3 błędy stwierdzone przy badaniu z wykorzystaniem narzędzia dostępnego na stronie http://validator.w3.org oraz 22 błędy stwierdzone z wykorzystaniem narzędzia dostępnego na stronie http://jigsaw.w3.org/css-validator.

(dowód: akta kontroli str. 26 – 30)

Burmistrz wyjaśnił: *„Zgodnie z przyjętym harmonogramem i dostępnymi środkami finansowymi, Urząd planuje dostosowanie systemów informatycznych, w szczególności publikatorów informacji publicznej do wymagań technicznych zawartych w rozporządzeniu KRI. Z uwagi na fakt, że BIP ma opracowany system CMS przez firmę zewnętrzną, terminy modyfikacji zostały ustalone z firmą prowadzącą zarówno hosting, jak i aktualizację narzędzi ww. publikatora. Z raportu walidacji strony BIP wynika, że liczba błędów i ostrzeżeń, które należy zweryfikować lub poprawić pozwoli na zachowanie terminu wyznaczonego w powyższym rozporządzeniu. Rozporządzenie KRI nakłada obowiązek, aby każdy nowy serwis był już wykonany w oparciu o określone w nim wymagania, natomiast serwisy istniejące powinny być dostosowywane sukcesywnie lub wymieniane. Po wykonaniu określonych prac zostanie wykonany audyt dostępności, mający na celu weryfikację systemu zgodną ze standardem WCAD 2.0. Harmonogram prac dla Biuletynu Informacji Publicznej przedstawia następujące terminy:*

1) *poprawki związane z treścią i standardami - do końca lutego 2015 r.,*
2) *audyt dostępności – do połowy marca 2015 r.,*
3) *synteza wyników audytu i sporządzenie odpowiedniej dokumentacji – do końca kwietnia 2015 r."*

(dowód: akta kontroli str. 4 – 5, 6 – 10)

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[8], wnosi o:

[6] http://www.szczecinek.pl.
[7] http://www.bip.szczecinek.pl.
[8] Dz.U. z 2012 r., poz.82 ze zm., zwana dalej: „ustawą o NIK".

1. Dostosowanie systemu FK-2 do minimalnych wymogów interoperacyjności określonych w przepisach rozporządzenia KRI.
2. Przeprowadzanie aktualizacji PBI, zgodnie z wymogami § 20 ust. 2 pkt 1 rozporządzenia KRI.
3. Uniemożliwienie instalowania oprogramowania przez użytkowników nie będących pracownikami służb informatycznych.
4. Przeszkolenie pracowników zaangażowanych w proces przetwarzania informacji, zgodnie z wymogiem § 20 ust. 2 pkt 6 rozporządzenia KRI.

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 wniosków pokontrolnych oraz o podjętych działaniach lub przyczynach niepodjęcia tych działań.

W przypadku wniesienia zastrzeżeń do wystąpienia pokontrolnego, termin przedstawienia informacji liczy się od dnia otrzymania uchwały o oddaleniu zastrzeżeń w całości lub zmienionego wystąpienia pokontrolnego.

Szczecin, dnia 3 października 2014 r.

Najwyższa Izba Kontroli
Delegatura w Szczecinie

Kontroler
Agata Prochotta Miłek
Specjalista k.p.

.....
podpis

DYREKTOR
Delegatura Najwyższej Izby Kontroli
w Szczecinie

.....
Jarosław Stańszewski
podpis