NAJWYŻSZA IZBA KONTROLI
Delegatura w Katowicach

LKA – 4101-19-03/2014
P/14/004

BEI

3103911/11/2014

Urząd Miasta Mikołów
Zał. ..... Godz. .....
wpłynęło 04 -11- 2014
poczta | osobiście

WYSTĄPIENIE POKONTROLNE

NAJWYŻSZA IZBA KONTROLI
Delegatura w Katowicach
ul. Powstańców 29, 40-039 Katowice
T +48 32 784 42 00, F +48 32 784 42 30
lka@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

Jednostka przeprowadzająca kontrolę

Najwyższa Izba Kontroli Delegatura w Katowicach

Kontrolerzy

1. Arkadiusz Przytulski, specjalista kontroli państwowej, upoważnienie do kontroli nr 91665 z dnia 19 sierpnia 2014 r.

(dowód: akta kontroli str. 1-2)

2. Jerzy Horodecki, główny specjalista kontroli państwowej, upoważnienie do kontroli nr 91671 z dnia 19 sierpnia 2014 r.

(dowód: akta kontroli str. 3-4)

Jednostka kontrolowana

Urząd Miasta w Mikołowie[1] Rynek 16, 43-190 Mikołów

Kierownik jednostki kontrolowanej

Marek Balcer - Burmistrz Mikołowa[2]

(dowód: akta kontroli str. 219-221)

II. Ocena kontrolowanej działalności

Ocena ogólna

Burmistrz Mikołowa 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[3]:

- zapewnił współpracę systemów informatycznych z innymi systemami Urzędu oraz systemami innych jednostek administracji publicznej, co spełniało minimalne wymogi interoperacyjności, o których mowa w § 5 ust. 3 pkt 3 rozporządzenia w sprawie KRI,
- przeprowadził analizę zagrożeń występujących przy przetwarzaniu informacji i podjął działania w celu zminimalizowania stwierdzonego ryzyka, co było zgodne z § 20 ust. 2 pkt 3 rozporządzenia w sprawie 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 w sprawie KRI,
- we wszystkich badanych umowach na zakup i serwis oprogramowania zawarto zapisy gwarantujące zabezpieczenie poufności informacji przetwarzanych w systemach informatycznych, co było zgodne z § 20 ust. 2 pkt 10 rozporządzenia w sprawie KRI.

---

[1] Zwany dalej „Urzędem"
[2] Zwany dalej „Burmistrzem"
[3] Dz. U. z 2012 r., poz. 526 zwane dalej „rozporządzenie w sprawie KRI"

Stwierdzone nieprawidłowości wystąpiły głównie przy realizacji zadań określonych w rozporządzeniu w sprawie KRI i polegały na:

- nieopracowaniu i niewdrożeniu całościowej Polityki Bezpieczeństwa Informacji, która jest elementem systemu zarządzania bezpieczeństwem informacji, co było niezgodne z § 20 ust. 3 rozporządzenia KRI,
- nieustanowieniu podstawowych zasad gwarantujących bezpieczną pracę przy przetwarzaniu mobilnym i pracy na odległość, pomimo obowiązku wynikającego z § 20 ust. 2 pkt 8 rozporządzenia w sprawie KRI,
- niezłożeniu wniosków o wycofanie uprawnień do przetwarzania danych osobowych dla czterech pracowników, z którymi rozwiązano stosunek pracy po 31 maja 2012 r. będących użytkownikami systemów informatycznych, co było niezgodne z procedurą określoną w „Instrukcji zarządzania systemem informatycznym służącym do przetwarzania danych osobowych" stanowiącej załącznik do „Polityki Bezpieczeństwa Danych Osobowych Przetwarzanych w Urzędzie Miasta Mikołów" [4],
- nienadaniu 50 aktywnym użytkownikom Systemu elektronicznego zarządzania dokumentami *Intradok* uprawnień do przetwarzania danych osobowych w systemie informatycznym, co było niezgodne z art. 37 ustawy z dnia 29 sierpnia 1997 r. o ochronie danych osobowych[5] oraz procedurą określoną w ww. „Instrukcji zarządzania (...)" i „Polityce Bezpieczeństwa (...)",
- przyjęciu sprzętu komputerowego, otrzymanego w użyczenie na podstawie porozumienia z Ministrem Spraw Wewnętrznych i Administracji, jako środki trwałe Urzędu zamiast ujęcia ich w ewidencji ilościowej jako obce środki trwałe.

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

Dokumenty strategiczne

W Strategii Rozwoju Gminy Mikołów na lata 2008-2015 z kwietnia 2008 r.[6] jako jeden z celów strategicznych w sferze społecznej (dział 4.3. Zadania strategiczne) wymieniono „Rozwinięte społeczeństwo informacyjne – wysoka jakość usług publicznych". Jako zadania poprzez realizacje których miał nastąpić rozwój społeczeństwa informacyjnego wymieniono:

- powszechny dostęp do Internetu,

- budowę systemu informacji o terenie (GIS).

(dowód: akta kontroli str. 5-11)

Ponadto w Urzędzie opracowana została „Strategia rozwoju zasobów informatycznych Gminy Mikołów do roku 2015". W „Strategii rozwoju zasobów informatycznych ..." zidentyfikowano m.in. problemy związane z zakresem i dostępnością e-Usług, działania mające poprawić jakość i dostępność e-Usługi

[4] Zarządzenie Burmistrza nr 1163/543/2012 z 21 listopada 2012 r.
[5] Dz. U. z 2014r., poz. 1182 zwana dalej „ustawą o ochronie danych osobowych".
[6] Zatwierdzony przez Radę Miejską Mikołowa uchwałą nr XXI/330/2008 z dnia 22 kwietnia 2008 r.

w Gminie, wskazano działania mające poprawić jakość e-Usługi w Gminie, projekty jakie miały być realizowane oraz orientacyjny harmonogram rzeczowo-finansowy realizacji zadań.

Do końca maja 2014 r. zrealizowano trzy projekty:

- Zintegrowany System Informatyczny Urzędu Miasta dla Urzędu Miasta Mikołów (zakup sprzętu i oprogramowania). Projekt zakończony w grudniu 2011 r.,
- „Silesia-net – budowa społeczeństwa informacyjnego w subregionie centralnym województwa śląskiego: Powiat Mikołowski oraz Gminy Powiatu Mikołowskiego (Mikołów, Łaziska Górne, Orzesze, Ornontowice, Wyry)" – projekt był realizowany m.in. na podstawie umowy partnerskiej z 14 grudnia 2009 r. między gminami Powiatu Mikołowskiego i Powiatem Mikołowskim[7]. Projekt obejmował m.in. budowę infrastruktury telekomunikacyjnej oraz zakup sprzętu i został zakończony w kwietniu 2014 r.,
- „Budowa zintegrowanego systemu zarządzania Gminami Powiatu Mikołowskiego i Powiatem Mikołowskim w oparciu o system informacji o terenie (GIS)" - projekt był realizowany m.in. na podstawie umowy partnerskiej z 14 grudnia 2009 r. zawartej między gminami Powiatu Mikołowskiego i Powiatem Mikołowskim[8]. Projekt obejmował m.in. zakup sprzętu, budowę systemu informacji o terenie oraz integrację systemu obiegu dokumentów i innych systemów zewnętrznych. Projekt zakończono w maju 2014 r.

(dowód: akta kontroli str. 12-60)

Promowanie komunikacji elektronicznej

Działania Urzędu w zakresie promowania komunikacji elektronicznej, polegały na:

- informowaniu na stronie internetowej (www.mikolow.eu) o realizowanych projektach dotyczących rozwoju usług elektronicznych, tj. „Silesia-net" oraz „Budowa zintegrowanego systemu zarządzania Gminami Powiatu Mikołowskiego i Powiatem Mikołowskim w oparciu o system informacji o terenie (GIS)",
- zamieszczaniu w prasie lokalnej artykułów informujących o prowadzonych przedsięwzięciach przyczyniających się do rozwoju informatyzacji w gminie,
- zorganizowaniu konkursu wśród mieszkańców powiatu mikołowskiego dotyczącego zaprojektowania logo dla systemu GIS,
- zorganizowaniu w czerwcu 2014 r. z udziałem mieszkańców, konferencji podsumowujących realizację ww. zadań.

(dowód: akta kontroli str. 60, 66-74)

W Urzędzie nie przeprowadzano badań ankietowych (lub w innej formie) w celu analizy potrzeb korzystania z elektronicznej formy komunikacji z Urzędem. Jak wyjaśnił Burmistrz, kierunki realizowanych działań wynikały z wymogów przepisów prawa oraz dokumentów strategicznych.

(dowód: akta kontroli str. 60)

W latach 2012-2014, na podstawie zarządzenia Burmistrza, przeprowadzane były raz w roku badania oceniające stopień satysfakcji klienta, tj. klientów wewnętrznych

[7] Projekt został sfinansowany ze środków własnych jednostek samorządu terytorialnego oraz ze środków EFRR (Europejskiego Funduszu Rozwoju Regionalnego) na podstawie umowy zawartej z Województwem Śląskim w dniu 10 sierpnia 2011 r.

[8] Projekt został sfinansowany ze środków własnych jednostek samorządu terytorialnego oraz ze środków EFRR na podstawie umowy zawartej z Województwem Śląskim w dniu 20 grudnia 2010 r.

(pracownicy) i zewnętrznych Urzędu. Informacje uzyskiwano z anonimowych ankiet wypełnianych przez mieszkańców, w których pytania w części C „Komunikacja" dotyczyły m.in. oceny strony www. oraz strony BIP Urzędu, możliwości zasięgnięcia informacji za pomocą poczty elektronicznej. W analizie satysfakcji Klienta zewnętrznego opracowanej przez Wydział Rozwoju Miasta na podstawie badania przeprowadzonego w okresie marzec-kwiecień 2014 r.[9] stwierdzono, m.in., że wśród propozycji usprawnień działania Urzędu respondenci wymienili możliwość załatwiania spraw online oraz E-usługi dla mieszkańców.

(dowód: akta kontroli str. 75, 82-87, 88-89, 95-97, 101-102)

Korespondencja z Ministrem Administracji i Cyfryzacji

Po wejściu w życie rozporządzenia w sprawie KRI[10] Burmistrz nie zwracał się do Ministra Administracji i Cyfryzacji z problemami lub prośbą o pomoc w zakresie dostosowania swoich systemów/rejestrów informatycznych do wymogów Krajowych Ram Interoperacyjności.

(dowód: akta kontroli str. 60-61)

Procedury obiegu dokumentów/zarządzania dokumentami regulujące komunikację elektroniczną w Urzędzie

W § 1 ust. 2 zarządzenia Burmistrza nr 188/125/11 z 11 kwietnia 2011 r. w sprawie wprowadzenia instrukcji kancelaryjnej, jednolitego rzeczowego wykazu akt oraz instrukcji w sprawie organizacji i zakresu działania archiwum zakładowego[11] ustalono stosowanie w Urzędzie Miasta Mikołowa, w zakresie wykonywania czynności kancelaryjnych oraz postępowania z dokumentacją, przepisów tradycyjnego systemu wykonywania czynności kancelaryjnych do dnia 31 grudnia 2015 r.
W zarządzeniu tym (§ 4) zobowiązano kierownika Biura Informatyki do dostosowania systemu do wymogów rozporządzenia w sprawie instrukcji kancelaryjnej oraz rozbudowy systemu elektronicznego zarządzania dokumentami *Intradok* w celu rozpoczęcia wykonywania czynności kancelaryjnych oraz postępowania z dokumentacją począwszy od 1 stycznia 2016 r.

Wewnętrzna procedura w sprawie obiegu korespondencji określała m.in., że korespondencję wpływającą do Urzędu przyjmuje Biuro Obsługi Interesanta/Klienta, które rejestruje korespondencję w systemie elektronicznym *Intradok*, a następnie podlega ona dekretacji i rozdzieleniu do właściwych komórek organizacyjnych. Korespondencja wpływającą do Urzędu w wersji papierowej (np. wnioski/skargi), jest stemplowana pieczątką wpływu i skanowana do systemu *Intradok*, który nadaje pismom numer sprawy. Wygenerowany przez ww. system numer jest ręcznie nanoszony na pisma wpływające. Podobnie przebiega proces rejestracji pism przychodzących na skrzynkę mailową Urzędu. Po wydrukowaniu pisma skanuje się do ww. systemu. Dokumenty pobrane z platformy ePUAP są automatycznie pobierane do systemu *Intradok* i od razu rejestrowane. Po zarejestrowaniu w systemie wszystkie pisma trafiają w wersji papierowej do dekretacji kierownictwa, skąd wracają do Biura Obsługi Klienta, które rozprowadza je oraz rozsyła elektronicznie do kierowników wydziałów/referatów. Odbiór dokumentacji kierownicy potwierdzają na wygenerowanym z *Intradok* raporcie, będącym rejestrem korespondencji wpływającej do Urzędu. Następnie

[9] W 2013 r. badania te przeprowadzono również w marcu i kwietniu.
[10] 31 maja 2012 r.
[11] Dot. 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 Dz. U. Nr 14, poz. 67, zwane dalej „rozporządzeniem w sprawie instrukcji kancelaryjnej".

kierownicy przesyłają dokumentację papierową i w wersji elektronicznej pracownikom merytorycznym, celem załatwienia sprawy. Pracownicy załatwiają sprawę i udzielają odpowiedzi w formie papierowej. Odpowiedzi na korespondencję elektroniczną przesyłane są elektronicznie do adresatów oraz drukowane i dołączone do akt sprawy. Jeżeli adresat, który przesłał korespondencję w formie elektronicznej wskazał papierową formę odpowiedzi, wówczas przesyłana jest adresatowi w tej formie. W systemie *Intradok* nie rejestruje się dokumentacji wychodzącej (np. decyzji, odpowiedzi) w wersji papierowej, ani w elektronicznej.

(dowód: akta kontroli str. 104-105, 109, 526)

W okresie od 31 maja 2012 r. do 31 maja 2014 r.) do Urzędu wpłynęło łącznie 102 813 dokumentów, w tym 102 777 w postaci papierowej (99,96%) i 36 w formie elektronicznej (0,04%)[12]. W tym okresie Urząd wysłał ogółem 119 561 dokumentów, w tym 117 502 w postaci papierowej (98,28%) i 2 059 w formie elektronicznej (1,72%)[13].

(dowód: akta kontroli str. 453)

Usługi elektroniczne

Usługi elektroniczne zamieszczone na stronie ePUAP[14], wg stanu na 31 maja 2012 r. dotyczyły pięciu usług. Na dzień kontroli (2 października 2014 r.) liczba świadczonych usług zwiększyła się do sześciu, w związku z opublikowaniem na ePUAP, w dniu 22 września 2014 r. usługi „Rejestracja urodzeń".

W wyjaśnieniu w sprawie małej liczby usług świadczonych elektronicznie Burmistrz stwierdził m.in., że w związku z planowanym od 1 stycznia 2016 r. wdrożeniem pełnego elektronicznego obiegu dokumentów w celu pełnej integracji przepływu dokumentów z wykorzystaniem oprogramowania *Intradok* planowano udostępnienie większej liczby usług świadczonych drogą elektroniczną od 2015 r.

(dowód: akta kontroli str. 283-294, 308, 446-448)

Objęto badaniem pięć usług umieszczonych na platformie ePUAP, tj. wydanie zezwolenia na usunięcie drzew i krzewów, wydanie wypisu i wyrysu z miejscowego planu zagospodarowania przestrzennego, nadanie numeru porządkowego nieruchomości, udostępnienie informacji publicznej na wniosek oraz załatwianie skarg, wniosków i zapytań do urzędu. Stwierdzono, że faktyczne załatwianie ww. spraw przebiegało zgodnie z opisem usług opublikowanym na platformie ePUAP.

(dowód: akta kontroli str. 309-314, 492-525)

W Biuletynie Informacji Publicznej zamieszczone zostały opisy 81 usług świadczonych przez Urząd, w tym sześciu[15] świadczonych przez Urząd w formie elektronicznej.

Opisy procedur obowiązujących przy załatwianiu pięciu objętych badaniem usług świadczonych przez Urząd, opublikowane w Biuletynie Informacji Publicznej

---

[12] W formie elektronicznej do Urzędu wpłynęło od obywateli 17 dokumentów, od osób prawnych i innych podmiotów (m.in. prowadzących działalność gospodarczą, stowarzyszeń, fundacji itp.) 11 dokumentów, od innych urzędów 8 dokumentów.

[13] W formie elektronicznej z Urzędu wysłano do obywateli 12 dokumentów, do osób prawnych i innych podmiotów (m.in. prowadzących działalność gospodarczą, stowarzyszeń, fundacji itp.) 1 029 dokumentów, do innych urzędów 1 018 dokumentów

[14] Elektroniczna Platforma Administracji Publicznej – system teleinformacyjny udostępniający usługi elektroniczne administracji publicznej dla obywateli.

[15] Jeden opis dodano na stronie BIP Urzędu w trakcie kontroli.

zawierają dane dotyczące podmiotu, miejsca świadczenia usługi, aktualna podstawę prawną oraz sposób realizacji usługi.

(dowód: akta kontroli str. 298-302, 308-314, 483-489)

Centralne Repozytorium Dokumentów

Burmistrz nie przekazywał do centralnego repozytorium na ePUAP wzorów dokumentów elektronicznych, o których mowa w art. 19b ust. 3 ustawy z dnia 17 lutego 2005 r. o informatyzacji działalności podmiotów realizujących zadania publiczne[16], gdyż skorzystał z wzorów dokumentów dostępnych w katalogu usług na platformie ePUAP.

(dowód: akta kontroli str. 279)

Model usługowy

Urząd w podstawowym zakresie stosował model usługowy[17] dotyczący świadczenia usług elektronicznych. Dla pięciu objętych badaniem usług ustalono, że było możliwe zidentyfikowanie właściciela świadczonej usługi, tj. komórki organizacyjnej zajmującej się jej obsługą. Ze względu na fakt, że usługi świadczone są za pośrednictwem platformy ePUAP i Urząd nie ma możliwości technicznej ingerencji w jego funkcjonowanie, w opisie usługi nie wskazano maksymalnego ani dopuszczalnego czasu ich niedostępności, sposobu zgłaszania awarii oraz osób/komórek/podmiotów odpowiedzialnych za usuwanie awarii.

(dowód: akta kontroli str. 308-314)

Współpraca wybranych systemów informatycznych z innymi systemami

Zakres współpracy systemów informatycznych wewnątrz Urzędu skontrolowano dla wybranych w oparciu o dobór celowy, trzech systemów zakupionych po 31 maja 2012 r. i tak:

- System Zarządzania Odpadami Komunalnymi (SZOK) - wspierający działalność w zakresie zarządzania odpadami komunalnymi - umożliwia eksport danych dot. księgowań i naliczeń płatności z wygenerowanego pliku do systemu Finansowo-Księgowego, a przesyłanie danych zarówno do jak i z systemu FK wymaga działania użytkownika systemu. Ponadto w podobny sposób następuje przekazanie zaktualizowanych danych do Systemu informacji o terenie (GIS). Współpracę z innymi systemami można określić jako poziom jednostronnej komunikacji[18].
- System informacji o terenie (GIS) – który ma pełnić rolę zintegrowanego systemu zarządzania gminą – z zewnętrznymi aplikacjami współpracuje w następujący sposób:
  - z systemem Ewidencja Ludności komunikuje się w sposób transakcyjny, tj. dane z ewidencji ludności są aktualizowane w bazie systemu GIS automatycznie w trybie conocnym i nie jest wymagana ingerencja użytkowników,
  - z systemów: Podatkowego, Wieczystego Użytkowania Gruntów, Dzierżawy Ewidencja gruntów i budynków oraz SZOK dane są przekazywane do Systemu GIS po uruchomieniu odpowiedniej funkcji

[16] Dz. U. z 2014 r., poz. 1114 ze zm.

[17] Zgodnie z definicją zawartą w §2 pkt 8 rozporządzenia w sprawie KRI model usługowy to model struktury systemu informatycznego, w którym dla użytkowników zdefiniowano stanowiące odrębną całość funkcje systemu teleinformatycznego (usługi sieciowe) oraz opisano sposób korzystania z tych funkcji.

[18] Dane z jednego systemu są przekazywane do innego systemu za pośrednictwem pracownika (operatora systemu), który dane te importuje ręcznie do systemu – brak automatyzacji działania.

przez użytkownika. Współpracę taką można określić jako poziom jednostronnej komunikacji,

- z Systemem Obiegu Dokumentów *Intradok* jest to jednostronna komunikacja, tj. dokument (np. decyzja) wytworzony w Systemie GIS jest przekazywany do systemu *Intradok* za pośrednictwem pracownika. Podobnie może nastąpić przekazanie danych (dokumentu zarejestrowanego) z systemu *Intradok* do Systemu GIS, który ma możliwość pobrania danych z dokumentu do tworzonej decyzji.

- System Obiegu Dokumentów Intradok - ma możliwość jednostronnej komunikacji z Systemem GIS, co opisano powyżej19.

W ocenie NIK objęte kontrolą systemy informatyczne spełniają minimalne wymogi interoperacyjności w zakresie współpracy z innymi systemami Urzędu, określone w § 5 ust. 3 pkt 3 rozporządzenia w sprawie KRI.

(dowód: akta kontroli str.64-65, 246, 248-262)

Korespondencję w formie elektronicznej od 1 czerwca 2012 r., w zakresie wybranego katalogu spraw, Urząd prowadzi wyłącznie ze Śląskim Urzędem Wojewódzkim w Katowicach[20]. Korespondencja odbywa się z wykorzystaniem Systemu Obiegu Dokumentów *Intradok* za pośrednictwem ePUAP.
Ustalono, że system *Intradok* współpracuje z ePUAP oraz Systemem GIS, który pobiera automatycznie dane z systemu informatycznego Ewidencja gruntów i budynków będącego elementem zasobu geodezyjnego[21], co spełnia minimalne warunki interoperacyjności określone w § 5 ust. 3 pkt 3 rozporządzenia w sprawie KRI.

(dowód: akta kontroli str. 64-65,110, 112-113, 247, 263-264, 269-273)

Ocena cząstkowa

Najwyższa Izba Kontroli ocenia pozytywnie działalność Urzędu w zakresie realizacji wymagań określonych w § 5 ust. 3 pkt 3 rozporządzenia w sprawie KRI. Podjęto właściwe działania w celu dostosowania posiadanych systemów teleinformatycznych do współpracy z innymi systemami informatycznymi oraz systemami innych jednostek administracji publicznej. Na stronie Urzędu zamieszczono opisy sześciu świadczonych przez Urząd usług w formie elektronicznej. Podejmowano działania promocyjne w zakresie korzystania z elektronicznej formy komunikacji z Urzędem. Prowadzono ponadto komunikację elektroniczną ze Śląskim Urzędem Wojewódzkim.

2. Wdrożenie systemu zarządzania bezpieczeństwem systemów informatycznych

Opis stanu faktycznego

Dokumenty z zakresu bezpieczeństwa informacji

Zarządzeniem nr 75/144/2004 z dnia 23 listopada 2004 r. w sprawie określenia zasad postępowania przy przetwarzaniu danych osobowych w Urzędzie[22], wprowadzono do stosowania opisującą sposób przetwarzania danych osobowych oraz środki techniczne i organizacyjne zapewniające ochronę danych osobowych „Dokumentację przetwarzania danych osobowych", stanowiącą załącznik do tego zarządzenia. Załącznikiem do niej była m.in. „Polityka bezpieczeństwa" (zał. nr 1)

---

[19] Możliwość przekazywania danych systemu *Intradok* będzie wykorzystywana po wdrożeniu obsługi poczty wychodzącej w systemie *Intradok*. Aktualnie wykorzystywany jest on w zakresie obsługi poczty przychodzącej.
[20] Śląski Urząd Wojewódzki w tej sprawie wystąpił pismem z dnia 19 marca 2012 r. (nr BDiV.021.3.2012)
[21] Prowadzony przez Powiatowy Ośrodek Dokumentacji Geodezyjnej i Kartograficznej przy Starostwie Powiatowym w Mikołowie.
[22] Zarządzenie straciło moc z dniem 21 listopada 2012 r.

oraz „Instrukcja zarządzania systemami informatycznymi służącymi do przetwarzania danych osobowych" (zał. nr 2). Z dniem 21 listopada 2012 r. wydane zostało zarządzenie nr 1163/543/2012 w sprawie zasad ochrony danych osobowych przetwarzanych w Urzędzie Miasta Mikołów, do którego załączono „Politykę bezpieczeństwa danych osobowych przetwarzanych w Urzędzie Miasta Mikołów" oraz „Instrukcję zarządzania systemami informatycznymi służącymi do przetwarzania danych osobowych"[23].

Na Administratora Bezpieczeństwa Informacji powołany został Sekretarz Miasta, a do jego zadań należała m.in. aktualizacja polityki bezpieczeństwa.

(dowód: akta kontroli str. 111, 114-128, 222-239, 527-528)

Posiadanie zinwentaryzowanego sprzętu informatycznego oraz zapobieganie możliwości instalacji nieautoryzowanego oprogramowania

Ewidencja zasobów informatycznych Urzędu prowadzona była przy użyciu oprogramowania biurowego OpenOffice, a od 2014 r. programu MagicInfo. Oględziny zapisów zawartych w ww. ewidencjach dotyczących wybranych 10 komputerów oraz jednego serwera wykazały, że dane techniczne w zakresie sprzętu oraz zainstalowanego oprogramowania były ujęte w ww. ewidencjach, co spełniało wymogi określone w § 20 ust. 2 pkt 2 rozporządzenia w sprawie KRI.

Na podstawie badania 15 komputerów, w tym pięciu otrzymanych z Ministerstwa Spraw Wewnętrznych i Administracji, w zakresie możliwości zainstalowania na nich dowolnego oprogramowania przez użytkowników niebędących pracownikami Wydziału Informatyzacji stwierdzono, że pracownicy nie mogli samodzielnie instalować oprogramowania na komputerach służbowych. Było to zgodne z § 20 ust. 2 pkt 4 rozporządzenia w sprawie KRI stanowiącym, że zarządzanie bezpieczeństwem informacji realizowane jest w szczególności przez podjęcie działań zapewniających, że osoby zaangażowane w proces przetwarzania informacji posiadają stosowne uprawnienia do realizowanych przez nie zadań oraz obowiązków mających na celu zapewnienie bezpieczeństwa informacji.

(dowód: akta kontroli str. 320-344, 399, 436-445, 449)

Na podstawie porozumienia z 5 listopada 2010 r. Urząd otrzymał od Ministra Spraw Wewnętrznych i Administracji w użyczenie sprzęt komputerowy, który został odebrany na podstawie protokołów w okresie od września do grudnia 2011 r. Część sprzętu, tj. 6 komputerów[24], oraz 14 czytników dualnych kart została ujęta w ewidencji środków trwałych Urzędu w czerwcu 2013 r., natomiast pozostały sprzęt znajdował się poza ewidencją księgową, co opisano w dalszej części niniejszego wystąpienia pokontrolnego.

(dowód: akta kontroli str.398-434)

Analizy utraty integralności, poufności lub dostępności informacji

W okresie objętym kontrolą w Urzędzie nie dokumentowano czynności jakie były prowadzone w zakresie okresowych analiz utraty integralności, dostępności lub poufności informacji, o których mowa w § 20 ust. 2 pkt 3 rozporządzenia w sprawie KRI. Działania te, jak wyjaśnił Burmistrz, prowadzone były na bieżąco i nie była z tego opracowywana dokumentacja papierowa. W dalszej części wyjaśnień stwierdził, że wątpliwości związane z możliwością wystąpienia nieprawidłowości były na bieżąco omawiane z naczelnikiem Wydziału Informatyzacji Urzędu

[23] pracownicy Urzędu zostali zaznajomieni z tymi zarządzeniami.
[24] Jeden komputer nie był użytkowany.

i wspólnie z pracownikami podejmowane były określone działania mające na celu zapobieganie incydentom.

(dowód: akta kontroli str. 240-241, 244)

Zarządzanie uprawnieniami do pracy w systemach informatycznych

Zasady obowiązujące przy nadawaniu, modyfikowaniu i odbieraniu uprawnień użytkownikom systemów informatycznych określono w „Polityce bezpieczeństwa danych osobowych przetwarzanych w Urzędzie Miasta Mikołów" i „Instrukcji zarządzania systemem informatycznym służącym do przetwarzania danych osobowych"[25]. W wyniku przeglądu uprawnień do systemów i zasobów informatycznych dla 15 pracowników[26] będących użytkownikami trzech systemów informatycznych objętych kontrolą[27] stwierdzono, że 13 osób zgodnie z § 20 ust. 2 pkt 4 rozporządzenia w sprawie KRI uczestniczyło w procesie przetwarzania informacji w stopniu adekwatnym do zadań wynikających z zakresów obowiązków. Pozostałe dwie osoby przetwarzające informacje w systemie *Intradok* nie posiadały upoważnień do użytkowania tego systemu, co opisano w dalszej części wystąpienia.

(dowód: akta kontroli str. 114-115, 122-123, 222-225, 234-237, 345-382, 384-386)

W toku kontroli sprawdzono zablokowanie dostępu do systemów informatycznych dla byłych pracowników i stwierdzono, że spośród 18 osób, z którymi rozwiązano stosunek pracy w okresie od 31 maja 2012 r. do 30 września 2014 r.[28] pięć posiadało uprawnienia do pracy w systemach komputerowych. Osoby te miały zablokowany dostęp do systemów informatycznych. Dla czterech z tych osób przełożeni nie sporządzili wniosków o odebranie uprawnień wymaganych „Instrukcją zarządzania systemem informatycznym służącym do przetwarzania danych osobowych".

(dowód: akta kontroli str. 222-224, 390-392)

Szkolenia pracowników przetwarzających informacje

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 procesie przetwarzania informacji, ze szczególnym uwzględnieniem takich zagadnień jak: zagrożenia bezpieczeństwa informacji; skutki naruszenia zasad bezpieczeństwa informacji, w tym odpowiedzialność prawna i stosowanie środków zapewniających bezpieczeństwo informacji, w tym urządzenia i oprogramowanie minimalizujące ryzyko błędów ludzkich.

W dniach 11 i 30 kwietnia 2012 r. 78 pracowników Urzędu wzięło udział w szkoleniu z zakresu „Ochrony danych osobowych w administracji publicznej"[29], którego tematyka obejmowała m.in. takie zagadnienia jak: proces przetwarzania danych osobowych i ich praktyczny aspekt; prawa osób, których dane są przetwarzane; odpowiedzialność karna i sposoby zabezpieczenia danych osobowych na terenie siedziby jednostki.

Zgodnie z zapisami w „Polityce bezpieczeństwa danych osobowych przetwarzanych w Urzędzie Miasta Mikołów" osoby upoważnione do przetwarzania danych

---

[25] Zarządzenie Burmistrza z 21 listopada 2012 r. nr 1163/543/2012.
[26] W tym 5 osób zajmujących stanowiska kierownicze.
[27] System Informacji o Terenie GIS, System SZOK oraz system *Intradok*.
[28] Osoby, które nie były pracownikami Urzędu na dzień 30 września 2014 r.
[29] Wcześniej szkolenie w tym zakresie odbyło się w październiku 2008 r. i objęło 128 pracowników Urzędu.

osobowych przed dopuszczeniem ich do pracy zostały przeszkolone w zakresie obowiązujących przepisów o ochronie danych osobowych.

Ponadto osoby przyjmowane do pracy, były zapoznawane z treścią zarządzenia Burmistrza w sprawie zasad ochrony danych osobowych przetwarzanych w Urzędzie oraz „Instrukcją zarządzania systemem informatycznym służącymi do przetwarzania danych osobowych".

(dowód: akta kontroli str. 61-62, 123, 130, 245, 345-383)

Praca na odległość i mobilne przetwarzanie danych

W § 20 ust. 2 pkt 8 rozporządzenia w sprawie KRI określono obowiązek ustanowienia podstawowych zasad gwarantujących bezpieczną pracę przy przetwarzaniu mobilnym i pracy na odległość. W „Instrukcji zarządzania systemem informatycznym służącym do przetwarzania danych osobowych" stanowiącej załącznik do Polityki Bezpieczeństwa (rozdział IV „Rozpoczęcie, zawieszenie i zakończenie pracy przez użytkowników systemu") punkty 11-13 odnosiły się do sposobu użytkowania komputerów przenośnych, w których użytkownicy zostali zobowiązani do:

- chronienia komputerów przed kradzieżą i dostępem osób postronnych oraz zachowania ostrożności podczas transportu,

- zmiany hasła nie rzadziej niż co 30 dni.

Poza zapisami w opisanej wyżej „Instrukcji (...)" nie opracowano odrębnych zasad/procedur gwarantujących bezpieczną pracę przy przetwarzaniu mobilnym i pracy na odległość. Jak wyjaśnił Burmistrz, szczegółowa procedura obejmująca zasady użytkowania sprzętu oraz prawa i obowiązki użytkownika zostanie opracowana i włączona do Polityki Bezpieczeństwa Informacji przy jej najbliższej aktualizacji nie później niż do końca 2014 r.

(dowód: akta kontroli str. 188, 227-228, 242-243)

Umowy serwisowe

W umowach na dostawy/usługi opieki technicznej dotyczących trzech systemów komputerowych[30] objętych kontrolą zawarto zapisy zobowiązujące wykonawców do zachowania tajemnicy informacji, do których mieli dostęp w związku z realizacją tych umów, w tym wykonywaniem usług serwisowych, co spełniało wymogi określone w § 20 ust. 2 pkt 10 rozporządzenia w sprawie KRI.

(dowód: akta kontroli str. 131, 140-141,143-145, 156, 160-168)

W sytuacji awarii pozostałego sprzętu komputerowego, jak wyjaśnił Sekretarz Miasta był on naprawiany przez pracowników Referatu Obsługi Informatycznej. Umowy serwisowe zawierane z podmiotami zewnętrznymi nie dotyczyły sprzętu komputerowego.

(dowód: akta kontroli str. 110, 169-172)

Zgłaszanie incydentów naruszenia bezpieczeństwa informacji

W Urzędzie stosownie do § 20 ust. 2 pkt 13 rozporządzenia w sprawie KRI wprowadzona została procedura postępowania w przypadku naruszenia ochrony danych osobowych określona w „Instrukcji zarządzania systemem informatycznym

[30] Umowa z 30 grudnia 2011 r. na „Budowę systemu informacji o terenie[30] (dostarczenie aplikacji, opracowanie warstw tematycznych, wdrożenie, uzupełnienie danymi, integracja systemu obiegu dokumentów, szkolenia) wraz z zakupem, dostawą konfiguracją sprzętu teleinformatycznego" (§ 14); umowa z 3 października 2011 r. na „Dostawę i konfigurację Systemu Zarządzania Odpadami Komunalnymi (SZOK) w Urzędzie Miasta Mikołów" (§ 11) oraz umowa z 4 lutego 2013 r. na świadczenie usług opieki technicznej w zakresie eksploatacji systemu *Intradok* (§ 5).

służącym do przetwarzania danych osobowych" stanowiącej załącznik do „Polityki Bezpieczeństwa danych osobowych przetwarzanych w Urzędzie Miasta Mikołów"[31]. Pracownicy byli zobowiązani do bezzwłocznego podejmowania działań określonych w tej procedurze.

Ponadto zgodnie z zaleceniami audytu wewnętrznego (z 2013 r.) opracowana została w grudniu 2013 r. przez zastępcę Administratora Bezpieczeństwa Informacji „Procedura reagowania na incydenty bezpieczeństwa IT w Urzędzie Miasta Mikołów". W ww. Procedurze określono skład zespołu odpowiedzialnego za operacje związane z obsługą incydentów oraz sposób postępowania w razie zaistnienia takiego zdarzenia.

Procedura ta została udostępniona na serwerze dostępnym dla pracowników w katalogu „ochrona danych osobowych". Jak wyjaśnił Burmistrz ww. Procedura zostanie włączona do Polityki bezpieczeństwa Informacji nie później niż do końca 2014 r.

(dowód: akta kontroli str. 114, 123-127, 213-216, 241-242, 274)

W okresie od 31 maja 2012 r. do dnia zakończenia kontroli zarejestrowano jeden incydent (15 września 2014 r.) polegający na braku zasilania (wyłączenie serwerów podstawowych). Podjęte działania po włączeniu zasilania polegały m.in. na analizie i weryfikacji usług.

(dowód: akta kontroli str. 217)

Audyt wewnętrzny z zakresu bezpieczeństwa informacji

W latach 2012-2014 (do dnia zakończenia kontroli) przeprowadzono dwa audyty wewnętrzne w zakresie bezpieczeństwa informacji:

- w 2012 r. audyt obejmował „System informatyczny urzędu – gospodarowanie sprzętem komputerowym", w ramach którego audytor sformułował zalecenia w zakresie polityki bezpieczeństwa dotyczące m.in.:

– wdrożenia polityki blokowania konta po określonej liczbie błędnych prób logowania,

– prowadzenia „dziennika zdarzeń" wskazujących na naruszenie bezpieczeństwa systemu informatycznego, w tym ewidencję prób złamania hasła, prób uzyskania dostępu ponad wcześniej przyznane uprawnienia. W Rejestrze incydentów bezpieczeństwa informacji zarejestrowano jeden incydent w 2014 r., natomiast w 2013 r. wpisano, że nie wystąpiły incydenty.

– wdrożenie oprogramowania *MagicInfo*, służącego do monitoringu funkcjonujących stanowisk komputerowych (użytkowane w trakcie kontroli NIK),

– zlecenia przeprowadzenia audytu zewnętrznego. W grudniu 2013 r. w wyniku przetargu nieograniczonego na przeprowadzenie audytu bezpieczeństwa informacji w Urzędzie, wybrany został wykonawca, który jednakże 9 grudnia 2012 r. odstąpił od podpisania umowy,

[31] Wprowadzona zarządzeniem Burmistrza nr 1163/543/2012 z 21 listopada 2012 r.

- w 2013 r. audytor przeprowadził przegląd wstępnego zadania zapewniającego, w zakresie bezpieczeństwa informacji, w wyniku którego zwrócił uwagę na konieczność opracowania procedury postępowania związanej z incydentami naruszenia bezpieczeństwa informacji. Procedura taka została opracowana w grudniu 2013 r.

(dowód: akta kontroli str. 186-188, 199-205, 217, 274)

W 2014 r. audyt w zakresie bezpieczeństwa informacji, jak stwierdził Sekretarz Miasta, ma zostać przeprowadzony przez firmę zewnętrzną, której wybór ma nastąpić w trybie zapytania o cenę. W dniu 15 października 2014 r. Sekretarz Miasta wyraził zgodę na rozpoczęcie procedury wyboru wykonawcy tego audytu.

(dowód: akta kontroli str. 279)

Kopie zapasowe

W Urzędzie obowiązywała „Instrukcja zarządzania systemem informatycznym służącym do przetwarzania danych"[32], w której określono częstotliwość tworzenia kopii zapasowych danych i aplikacji przetwarzających (raz w tygodniu). Kopie zapasowe tworzone były częściej niż raz w tygodniu i przechowywane na specjalnie wydzielonym do tego celu obszarze dysku na serwerze. Raz w tygodniu kopie były zgrywane na nośniki zewnętrzne, które są przechowywane w odrębnym pomieszczeniu. Pomieszczenie serwerowni było właściwie zabezpieczone, a kopie zapasowe były tworzone na zewnętrznym dysku znajdującym się poza główną siedzibą Urzędu Miasta.

Testowanie/sprawdzanie kopii zapasowych pod kątem ich przydatności do odtworzenia w przypadku awarii miało następować okresowo, lecz przeprowadzenie tych czynności nie było odnotowywane w żadnej dokumentacji. Od dnia 1 października 2014 r., tj. w czasie trwania kontroli, Administrator Bezpieczeństwa Informacji wprowadził do stosowania Rejestr ewidencji odtwarzania kopii zapasowych. Powyższe spełniało wymogi określone w § 20 ust. 2 pkt 12 lit b rozporządzenia w sprawie KRI, tj. minimalizowania ryzyka utraty informacji w wyniku awarii.

(dowód: akta kontroli str. 222, 238, 240, 244, 303-307, 315-317)

Format danych udostępniany przez badane systemy

Systemy informatyczne objęte kontrolą udostępniały zasoby informacyjne, w co najmniej jednym z formatów określonych w załączniku nr 2 do rozporządzenia w sprawie KRI, tj. eksport danych w formacie XLS (wszystkie systemy), a ponadto System Informacji o Terenie (GIS) w formatach: pdf, jpg, doc, xml, geotiff.

(dowód: akta kontroli str.265-268)

Ustalone nieprawidłowości

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

1. W Urzędzie nie opracowano i nie wdrożono całościowej Polityki Bezpieczeństwa Informacji, która jest elementem systemu zarządzania bezpieczeństwem informacji, co było niezgodne z § 20 ust. 3 rozporządzenia KRI, który stanowi, że wymagania w zakresie systemu zarządzania bezpieczeństwem informacji, uznaje się za spełnione, jeżeli system został opracowany na podstawie Polskiej Normy PN-ISO/27001 oraz powiązanej z nią Polskiej Normy PN-ISO/IEC-17799. W pkt 5.1. normy PN-ISO/IEC-17799 wskazano opracowanie i stosowanie dokumentu polityki bezpieczeństwa

[32] Załącznik do polityki Bezpieczeństwa Danych Osobowych.

informacji wraz z zaleceniami odnoszącymi się do zawartości tego dokumentu. W 2012 r. opracowano „Politykę Bezpieczeństwa danych osobowych przetwarzanych w Urzędzie Miasta Mikołów" oraz „Instrukcję zarządzania systemami informatycznymi służącymi do przetwarzania danych osobowych", jednak nie dotyczyła ona wszystkich informacji jakie są przetwarzane w Urzędzie lecz odnosiła się tylko do danych osobowych.

(dowód: akta kontroli str. 111, 114-128, 222-239)

Burmistrz wyjaśnił, że Urząd nie posiada całościowej polityki bezpieczeństwa informacji. Stwierdził m.in.: „(...) Polityka Bezpieczeństwa Danych Osobowych, w przyjętych definicjach »System informatyczny« oraz »bezpieczeństwo systemu Informatycznego«, opis ten odnosi się do całości systemu bezpieczeństwa informacji w Urzędzie. Dodatkowo posiadamy Plan Ochrony Fizycznej Informacji Niejawnych oraz Plan Ochrony Obiektów Urzędu Miasta Mikołów, w których zawarty jest opis zabezpieczenia całości Urzędu." W dalszej części wyjaśnień Burmistrz stwierdził, że mając na uwadze treść § 23 rozporządzenia w sprawie KRI oraz wdrożony System GIS i obecnie wdrażany System SZOK prowadzone są prace aktualizacyjne dotyczące polityki Bezpieczeństwa Informacji Danych Osobowych oraz innych procedur, które zostaną wdrożone do końca 2014 r., natomiast całościowa polityka bezpieczeństwa Informacji zostanie wprowadzona do 28 lutego 2015 r.

(dowód: akta kontroli str. 527-528)

2. W badanym okresie w Urzędzie nie ustanowiono procedury gwarantującej bezpieczną pracę przy przetwarzaniu mobilnym i pracy na odległość, co stanowiło naruszenie § 20 ust. 2 pkt 8 rozporządzenia w sprawie KRI. Zapisy w „Instrukcji zarządzania systemem informatycznym służącym do przetwarzania danych osobowych" dotyczyły użytkowania komputerów przenośnych jednakże nie stanowiły pełnych zasad (procedur), o których wyżej mowa.

   W wyjaśnieniu Burmistrz Mikołowa stwierdził, że zapisy w „Instrukcji (...)" odnoszą się do ochrony danych na stanowiskach mobilnych, natomiast szczegółowa procedura obejmująca zasady użytkowania sprzętu oraz prawa i obowiązki użytkownika zostanie opracowana i włączona do Polityki Bezpieczeństwa Informacji przy jej najbliższej aktualizacji nie później niż do końca 2014 r.

   (dowód: akta kontroli str. 228, 242-243)

3. Stwierdzono, że 50 pracowników, będących aktywnymi użytkownikami systemu *Intradok*, którym przekazano ustnie loginy i hasła (na 142 założonych użytkowników) nie posiadało nadanych uprawnień do przetwarzania danych osobowych w systemie informatycznym, co stanowi naruszenie art. 37 ustawy o ochronie danych osobowych. Ponadto zgodnie z zapisami w Polityce bezpieczeństwa danych osobowych przetwarzanych w Urzędzie Miasta Mikołów i Instrukcji zarządzania systemem informatycznym służącym do przetwarzania danych osobowych[33] do obsługi takich systemów mogły być dopuszczone osoby, którym administrator danych osobowych wydał upoważnienia do przetwarzania danych osobowych.

[33] Zarządzenie Burmistrza z 21 listopada 2012 r. nr 1163/543/2012

Jak wyjaśnił Burmistrz niezwłocznie zostaną nadane niezbędne uprawnienia do korespondencji przychodzącej i wychodzącej w formie papierowej i elektronicznej dla osób pracujących na bieżąco w systemie.

(dowód: akta kontroli str. 387-389, 458-461)

4. Przełożeni czterech pracowników (z którymi rozwiązano stosunek pracy po 31 maja 2012 r.) nie złożyli wniosków o wyrejestrowanie ich, jako użytkowników systemów informatycznych (SEPOBIS, REKORD, CIDG, FK, zbiór komputerowy dot. nieruchomości), o których mowa w pkt II 4 c „Instrukcji zarządzania systemem informatycznym służącym do przetwarzania danych osobowych" stanowiącej załącznik do Polityki Bezpieczeństwa Danych Osobowych Przetwarzanych w Urzędzie Miasta Mikołów"[34].

(dowód: akta kontroli str. 278, 390-392)

Jak wyjaśnili przełożeni pracowników, niezłożenie wniosków o wyrejestrowanie zwolnionych pracowników spowodowane było natłokiem obowiązków służbowych, co zdaniem NIK nie może uniemożliwiać wypełniania obowiązków wynikających z przyjętych procedur.

Burmistrza wyjaśnił m.in., że naczelnicy i kierownicy zostaną upomniani o konieczności składania odrębnych pisemnych wniosków, a celem dodatkowego zabezpieczenia, do karty obiegowej zostanie dopisany Administrator Systemu Informatycznego z adnotacją o konieczności złożenia tego wniosku.

(dowód: akta kontroli str. 393-394, 450-452)

5. Sprzęt komputerowy otrzymany w użyczenie na mocy porozumienia zawartego z Ministrem Spraw Wewnętrznych i Administracji w dniu 5 listopada 2010 r. został w części przyjęty na stan środków trwałych Urzędu i wyceniony na kwotę 25.200 zł. (sześć zestawów komputerowych, 14 czytników kart dualnych), co było niezgodne z art. 3 ust. 1 pkt 15 i ust. 3 ustawy z dnia 29 września 1994 r. o rachunkowości[35]. Natomiast pozostały sprzęt, tj. serwer, skaner, trzy drukarki, oraz router pozostały poza ewidencją księgową Urzędu.

(dowód: akta kontroli str. 400-434)

W wyjaśnieniu Główna Księgowa Urzędu potwierdziła błędne przyjęcie sprzętu do ewidencji środków trwałych i jednocześnie poinformowała, że niezwłocznie zostaną dokonane stosowne korekty zarówno w księgach rachunkowych, jak i inwentarzowych, a sprzęt komputerowy zostanie ujęty ilościowo w kartotekach jako obcy środek trwały. W dniu 14 października 2014 r., w trakcie kontroli NIK dokonano korekt w księgach (dokument PK 16) oraz założono kartoteki dla całego otrzymanego z MSWiA sprzętu.

(dowód: akta kontroli str. 435, 462-478)

Uwagi dotyczące badanej działalności

NIK zwraca również uwagę na niedokumentowanie przeprowadzanych czynności w zakresie analiz utraty integralności, poufności lub dostępności informacji, o których mowa w § 20 ust. 2 pkt 3 rozporządzenia w sprawie KRI. Brak dokumentacji nie pozwala w sposób jednoznaczny stwierdzić, kto i kiedy przeprowadzał określone czynności oraz jakie były dalsze działania związane z wynikami tych analiz. Zasadnym wydaje się wdrożenie stosownej procedury, która uporządkowałaby dotychczas stosowane praktyki w tym zakresie.

[34] Zarządzenie Burmistrza z 21 listopada 2012 r. nr 1163/543/2012.
[35] Dz. U. z 2013, poz. 330 ze zm. zwana dalej „ustawą o rachunkowości"

Ocena cząstkowa

Najwyższa Izba Kontroli ocenia pozytywnie mimo stwierdzonych nieprawidłowości działalność Burmistrza w zakresie wdrożenia systemu zarządzania bezpieczeństwem systemów informatycznych. W umowach dotyczących zakupu oprogramowania i sprzętu informatycznego zamieszczono zapisy gwarantujące odpowiedni poziom bezpieczeństwa informacji. Zabezpieczono komputery wykorzystywane w Urzędzie przed możliwością zainstalowania nieautoryzowanego oprogramowania. Byłym pracownikom Urzędu, pomimo braku wniosków przełożonych, odbierano uprawnienia do pracy w systemach informatycznych. Właściwie przechowywano kopie zapasowe danych. Ustalenia kontroli wykazały jednak nieprawidłowość przy realizacji zadań określonych w rozporządzeniu w sprawie KRI polegające na nie ustanowieniu procedury gwarantującej bezpieczną pracę przy przetwarzaniu mobilnym i pracy na odległość. Ponadto stwierdzono nieprawidłowości w ewidencjowaniu otrzymanego w użyczenie sprzętu komputerowego oraz dopuszczenia pracy w systemie informatycznym *Intradok* użytkowników bez nadania uprawnień do przetwarzania danych osobowych.

3. Zapewnienie dostępności informacji dla osób niepełnosprawnych

Opis stanu faktycznego

W toku kontroli dokonano weryfikacji strony internetowej Urzędu[36] oraz strony BIP[37] Urzędu przy wykorzystaniu narzędzia dostępnego:

- na stronie http://www.w3.org i w rezultacie stwierdzono:
  - 27 błędów na stronie internetowej Urzędu (w dniu 28 sierpnia 2014 r.), których liczba, po zmianach dokonanych przez autora strony, zmniejszyła się do pięciu i jednego ostrzeżenia (w dniu 29 września 2014 r.),
  - 10 błędów i jedno ostrzeżenie na stronie BIP Urzędu (w dniu 28 sierpnia 2014 r.), które w trakcie kontroli zostały skorygowane i na dzień zakończenia kontroli strona ta nie wykazała błędów,
- na stronie http://jigsaw.w3.org/css-validator nie stwierdzono błędów na ww. stronach Urzędu.

(dowód: akta kontroli str. 281-282, 319-320, 479-480)

Ocena cząstkowa

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

IV. Uwagi i 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[38], wnosi o:

1. **Opracowanie i wdrożenie Polityki Bezpieczeństwa Informacji, określającej zasady bezpieczeństwa informacji, zgodnie z wymaganiami wynikającymi z § 20 ust. 3 rozporządzenia KRI.**
2. **Opracowanie zasad gwarantujących bezpieczną pracę przy przetwarzaniu mobilnym.**

[36] www.mikolow.eu
[37] www.bip.mikolow.eu
[38] Dz. U. z 2012 r., poz.82 ze zm.

3. **Dopuszczanie do użytkowania systemów informatycznych przetwarzających dane osobowe wyłącznie pracowników posiadających uprawnienia wymagane ustawą o ochronie danych osobowych.**
4. **Zapewnienie przestrzegania obowiązującej procedury w zakresie sporządzania w każdym uzasadnionym przypadku wniosków o wyrejestrowanie pracowników jako użytkowników systemów informatycznych.**

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 Katowicach.

Obowiązek poinformowania NIK o sposobie wykorzystania uwag i wykonania wniosków

Zgodnie z art. 62 ustawy o NIK proszę o poinformowanie Najwyższej Izby Kontroli, w terminie 21 dni od otrzymania wystąpienia pokontrolnego, o sposobie wykorzystania uwag i wykonania wniosków pokontrolnych oraz o podjętych działaniach lub przyczynach niepodjęcia tych działań.

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

Katowice, dnia 30 listopada 2014 r.

Najwyższa Izba Kontroli
Delegatura w Katowicach

DYREKTOR
Delegatura Najwyższej Izby Kontroli
w Katowicach
z up. Mariusz Marquardt
WICEDYREKTOR

Kontrolerzy
Arkadiusz Przytulski
specjalista k.p.

Jerzy Horodecki
główny specjalista k.p.