NAJWYŻSZA IZBA KONTROLI
Delegatura w Katowicach

LKA – 4101-019-01/2014
P/14/004

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

– Jerzy Horodecki, główny specjalista k.p, upoważnienie do kontroli nr 91670 z dnia 25 sierpnia 2014 r.

[Dowód: akta kontroli str. 4÷5]

– Arkadiusz Przytulski, spec. k.p., upoważnienie do kontroli nr 90666 z dnia 25 czerwca 2014 r.

[Dowód: akta kontroli str. 1÷2]

Jednostka kontrolowana

Urząd Miejski w Dąbrowie Górniczej, ul. Graniczna 21, 41-300 Dąbrowa Górnicza[1]

Kierownik jednostki kontrolowanej

Zbigniew Podraza, Prezydent Miasta

[Dowód: akta kontroli str. 6÷8]

II Ocena kontrolowanej działalności

Ocena ogólna

Prezydent Dąbrowy Górniczej realizując zadania określone w rozporządzeniu Rady Ministrów z dnia 12 kwietnia 2012 r. w sprawie Krajowych Ram Interoperacyjności, minimalnych wymagań dla rejestrów publicznych i wymiany informacji w postaci elektronicznej oraz minimalnych wymagań dla systemów teleinformatycznych[2]:

- stosował rozwiązania informacyjne oparte na modelu usługowym w zakresie świadczenia usług elektronicznych,
- 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 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,
- zapewnił realizowanie usług elektronicznych zgodnie z ich opisem zamieszczonym na platformie SEKAP[3] oraz na stronie podmiotowej BIP Urzędu oraz regularne tworzenie oraz testowanie kopii zapasowych danych i oprogramowania aplikacyjnego.

[1] Zwany dalej „Urzędem"
[2] Dz. U. z 2012 r., poz. 526, zwane dalej „rozporządzeniem KRI".
[3] System Elektronicznej Komunikacji Administracji Publicznej.

Stwierdzone nieprawidłowości wystąpiły m.in. przy realizacji zadań określonych w rozporządzeniu 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,
- zakupieniu przez Urząd Systemu vEdukacja, który uniemożliwiał osiągnięcie wymienności, o której mowa w § 4 ust. 1 pkt 2 rozporządzenia KRI,
- nieujęciu w ewidencji księgowej wartości niematerialnych i prawnych zakupionego oprogramowania informatycznego „Moduł do głosowania w ramach Dąbrowskiego Budżetu Partycypacyjnego",
- dopuszczeniu do przetwarzania danych osobowych przez wykonawcę ww. oprogramowania „Moduł do głosowania w ramach Dąbrowskiego Budżetu Partycypacyjnego", mimo niezawarcia umowy, co było niezgodne z art. 31 ustawy o ochronie danych osobowych z dnia 29 sierpnia 1997 r. o ochronie danych osobowych[4].

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 - *Dąbrowa Górnicza 2020*, przyjętej uchwałą Rady Miasta z dnia 28 listopada 2007 r., wśród celów strategicznych wyszczególnione zostały m.in. takie, które dotyczyły dostosowania jednostki do elektronicznego świadczenia usług, a mianowicie:

- Priorytet 2: Integracja wspólnot lokalnych, Cel_{22}: Dąbrowa Górnicza miastem silnie rozbudowanej infrastruktury informatycznej stwarzającej mieszkańcom warunki uczestnictwa w globalnym społeczeństwie informacyjnym. Strategicznymi kierunkami rozwoju były:
  - w opcji reaktywnej, m.in.: $K_{2.2.1}$ Utworzenie internetowej przestrzeni miejskiej i zapewnienie powszechnego, szerokopasmowego i bezpiecznego dostępu do Internetu; $K_{2.2.3}$ Promowanie i upowszechnianie wykorzystania nowoczesnych technologii informacyjno-telekomunikacyjnych;
  - w opcji proaktywnej, m.in: $K_{2.2.4}$ Rozbudowa e-administracji; $K_{2.2.5}$ Rozszerzenie zakresu usług publicznych świadczonych drogą elektroniczną.

Jako przedsięwzięcia strategiczne (Cel 2.2) wyszczególniono m.in. pozycje: budowa bezprzewodowej miejskiej sieci komputerowej, budowa publicznych punktów dostępu do Internetu, organizacja lokalnego ośrodka szkoleń informatycznych oraz utworzenie biura koordynującego rozwój społeczeństwa informacyjnego w Dąbrowie Górniczej, projekt *Miasto na platformie e-learningowej*, rozbudowa Internetowego portalu miejskiego www.dabrowa-gornicza.pl - jako centrum informacji miejskiej oraz

[4] Dz. U. z 2014 r. nr 1182 zwana dalej „ustawą o ochronie danych osobowych"

e-usług, wdrożenie karty e-usług publicznych, projekt *e-demokracja*, budowa telecentrum biznesowego.

Według informacji Kierownika Wydziału Rozwoju Miasta i Obsługi Inwestorów - w czasie niniejszej kontroli NIK prowadzono prace nad aktualizacją ww. Strategii, mające na celu dalsze dostosowanie Urzędu do świadczenia usług publicznych.

[Dowód: akta kontroli str. 9÷26]

Uzupełnieniem Strategii był Program rozwoju społeczeństwa informacyjnego w gminie Dąbrowa Górnicza, przyjęty uchwałą Rady Miejskiej z 13 czerwca 2008 r., opublikowaną na stronie BIP Urzędu. Dokument wyszczególniał w Polu strategicznym nr 3 — *Usługi i treści oparte na ICT*[5], Cel operacyjny 3.1 – *Rozwój elektronicznych usług świadczonych przez administrację*, osiągany poprzez wdrożenie m.in:

- podpisu elektronicznego weryfikowanego kwalifikowanym certyfikatem,
- elektronicznej skrzynki podawczej, e-formularzy oraz systemu przekazywania dokumentów elektronicznych do interesanta.

Przyjęto, że systemy te powinny działać zgodnie z ustawami i rozporządzeniami wymienionymi w opracowaniu.

Powołane wyżej dokumenty nie określały terminów wdrożenia działań.

[Dowód: akta kontroli str. 27÷32]

Promowanie komunikacji elektronicznej

Dla zapewnienia możliwości wymiany dokumentów elektronicznych Urząd przystąpił do projektu System Elektronicznej Komunikacji Administracji Publicznej (SEKAP) realizowanego w latach 2007 - 2008. Według wyjaśnień Naczelnika Wydziału Informatyki (WI) - główne działania promocyjne prowadzone były w I półroczu 2008 r. przez Śląskie Centrum Społeczeństwa Informacyjnego w Katowicach. Urząd włączył się do tych działań poprzez rozmieszczenie w Biurze Obsługi Interesanta (BOI) plakatów, ulotek i płyt CD z prezentacją projektu oraz organizację warsztatów dla mieszkańców, podczas których zakładali skrzynkę na portalu www.sekap.pl. Rozpowszechniano na stronach internetowych Urzędu informacje o elektronicznej skrzynce podawczej Urzędu na platformie SEKAP i o e-usługach.

[Dowód: akta kontroli str. 36÷37, 174]

W ramach promocji projektu: *Miejski System Informacji Przestrzennej* (MSIP) zamieszczono w latach 2010 - 2014 banery reklamowe w serwisach internetowych www.dabrowa.pl i www.dabrowagornicza.naszemiasto.pl, m.in.:

- zorganizowano prezentację MSIP dla pracowników Urzędu i jednostek budżetowych, połączoną ze szkoleniem na temat posługiwania się aplikacjami,
- rozprowadzono 20 tys. egzemplarzy folderów reklamowych, 50 tys. ulotek i 30 tys. broszur promujących ten projekt,
- MSIP zaprezentowano na konferencji *GIS Day* organizowanej przez Wydział Nauk o Ziemi Uniwersytetu Śląskiego oraz VIII Międzynarodowej Konferencji Naukowej „Internet w społeczeństwie informacyjnym" organizowanej przez Wyższą Szkołę Biznesu w Dąbrowie Górniczej.

[5] ang. Information and Communication Technologies — nowoczesne technologie informacji i komunikacji oparte o platformę elektroniczną.

Biuro Rozwoju Miasta i Obsługi Inwestorów prowadzi stronę internetową dla inwestora pod adresem www.dabrowa-gornicza.com, a obsługa informacyjna inwestorów odbywa się w 80% w formie elektronicznej.

[Dowód: akta kontroli str. 33÷35]

Ankiety lub inne formy poznania potrzeb mieszkańców gminy odnośnie elektronicznej formy komunikacji z Urzędem

Od 2012 r. badania satysfakcji mieszkańców prowadzone były w 40-jednostkach samorządu terytorialnego na zlecenie Śląskiego Związku Gmin i Powiatów przy wykorzystaniu środków unijnych. Wyniki badań na poziomie 3% błędu statystycznego wskazują, że udział osób, które załatwiły sprawę w Urzędzie przez Internet wynosił wg wyników badań przeprowadzonych w latach 2012 – 2014, odpowiednio: 15,5%, 7,8% i 9,8%. Odsetek osób, które potwierdziły posiadanie wiedzy o sprawach, które można załatwić przez Internet wyniósł, odpowiednio: 52,6%, 34,8% i 35,0%. Załatwianie spraw przez Internet jako preferowany sposób wskazało 35,5%, 34,8% i 29,8%.

[Dowód: akta kontroli str. 38÷46]

Współpraca z Ministrem Administracji i Cyfryzacji

Po wejściu w życie rozporządzenia KRI, tj. po 31 maja 2012 r. Prezydent Miasta nie zwracał się do Ministra Administracji i Cyfryzacji z prośbą o pomoc w zakresie dostosowania systemów informatycznych do wymogów ww. rozporządzenia.

[Dowód: akta kontroli str. 47÷52]

Obieg dokumentów

W Urzędzie opracowano i stosowano procedury obiegu dokumentów wprowadzone zarządzeniem Prezydenta Miasta z dnia 25 lipca 2014 r. w sprawie zasad i sposobu postępowania z dokumentacją w Urzędzie, w którym określono, że czynności kancelaryjne prowadzi się w systemie tradycyjnym przy wykorzystaniu Systemu Obiegu Dokumentów (SOD) SEKAP. Dokumenty elektronicznie są drukowane, a złożony na dokumentach elektronicznych podpis jest weryfikowany i potwierdzany przez pracownika Kancelarii Głównej na wydrukowanym dokumencie.

Przed wydaniem przez Prezydenta Miasta ww. zarządzenia, obieg dokumentów realizowano bezpośrednio na podstawie 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[6] i stosowano tradycyjny system zarządzania dokumentami, wspomagany elektronicznie.

W systemie elektronicznego obiegu dokumentów prowadzone jest 10 kategorii archiwalnych, wyszczególnionych w załączniku nr 4 do ww. zarządzenia Prezydenta Miasta. Dokumenty elektroniczne (SEKAP, ePUAP, e-mail) należące do tych kategorii są wczytywane do SOD, a dokumenty, które wpłynęły do Urzędu w formie papierowej są uprzednio skanowane i wczytywane do SOD. Dokumenty, dla których przepisy lub wnioskodawca wymagają formy papierowej (np. decyzje administracyjne, dokumenty tożsamości) są przekazywane do odbiorcy w formie papierowej. Załącznik nr 5 do ww. zarządzenia Prezydenta Miasta określał sposób załatwiania spraw w systemie SEKAP.

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

System ten jest narzędziem informatycznym wykorzystywanym w Urzędzie m.in. do: prowadzenia rejestrów, załatwiania spraw w SOD SEKAP i wspierania załatwiania spraw w systemie tradycyjnym, udoskonalania funkcjonującego w Urzędzie systemu obiegu dokumentów.

W teczkach spraw prowadzonych tradycyjnie, w myśl ww. Instrukcji, znajdują się spisy spraw generowane wyłącznie przez SOD SEKAP.

Postępowanie z przesyłkami wpływającymi na nośniku papierowym uregulowane zostało w rozdziale 3 Instrukcji. Przesyłki takie przyjmowane są w punkcie kancelaryjnym (Kancelaria Główna), gdzie umieszczana jest pieczęć wpływy, dekretuje się je i przekazuje do właściwej komórki organizacyjnej, w miarę możliwości technicznych wykonuje się pełne odwzorowanie dokumentu (bez załączników) i wprowadza się do rejestru przesyłek adresowanych do Urzędu.

Przesyłki wpływające na Elektroniczną Skrzynkę Podawczą przekazywane są do właściwej komórki organizacyjnej Urzędu bezpośrednio i rejestrowane w SOD SEKAP na poziomie Kancelarii Głównej. Pierwsza strona dokumentu jest drukowana i nanoszona na nią pieczęć wpływu. Potwierdzany jest podpis elektroniczny.

Rejestrowane w SOD SEKAP i przekazywane jw. są także dokumenty wpływające telefaksem na numer podany w BIP oraz przesyłki wpływające na główny adres poczty elektronicznej.

Dokumenty elektronicznie są drukowane, a podpis wpływających do elektronicznej skrzynki podawczej - weryfikowany i potwierdzany przez pracownika Kancelarii Głównej.

[Dowód: akta kontroli str. 53÷81]

W okresie od 31 maja 2012 r. do 31 maja 2014 r. wpłynęło łącznie 380.166 dokumentów, w tym 339.788 w postaci papierowej (89,4%) i 40.378 w formie elektronicznej (10,6%), i tak:

- 164 095 od obywateli, w tym 2 743 elektronicznych;
- 30 526 z innych urzędów, w tym 3 997 - w formie elektronicznej;
- 185 545 od pozostałych podmiotów, w tym 33 638 elektronicznych.

W tym okresie Urząd wysłał ogółem 732.929 dokumentów, w tym 678.673 w formie papierowej (92,4%) i 54.256 w formie elektronicznej (7,4%), i tak:

- 425 084 do obywateli, w tym 2 100 w formie elektronicznej;
- 47 529 do innych urzędów, w tym 14 706 elektronicznie;
- 260 316 do pozostałych podmiotów, w tym 37 450 w formie elektronicznej.

[Dowód: akta kontroli str. 82÷83]

Usługi elektroniczne

Na stronie internetowej zarządzanej przez Śląskie Centrum Społeczeństwa Informacyjnego w Katowicach[7] (SCSI), będącego liderem projektu, który łączy karty usług z jednostkami administracji samorządowej (platforma PeUP SEKAP) nie jest prowadzony dziennik zmian. Według stanu na 3 września 2014 r. w Katalogu usług na tej stronie wyszczególniono 356[8] kart usług dla Urzędu Miasta Dabrowa Górnicza.

[Dowód: akta kontroli str. 103÷138]

[7] Jednostka budżetowa Województwa Śląskiego.

[8] Liczba ta obejmowała trzy karty usług, które leżały w kompetencji urzędu marszałkowskiego.

Szczegółowym badaniem w zakresie zgodności świadczonych usług z ich opisami objęto 5 usług:

1. Wyrażenie zgody na usunięcie drzew i krzewów - usługa jest realizowana przez Wydział Ekologii i Rolnictwa.
2. Wydawanie zezwoleń na sprzedaż napojów alkoholowych przeznaczonych do spożycia w miejscu lub poza miejscem sprzedaży - usługa jest realizowana przez Wydział Zdrowia Polityki Społecznej i Aktywizacji Zawodowej.
3. Wydawanie Kart wędkarskich - usługa jest realizowana przez Wydział Ekologii i Rolnictwa.
4. Zgłoszenie zbycia pojazdu - usługa jest realizowana przez Wydział Komunikacji i Drogownictwa.
5. Zgłoszenie robót budowlanych - usługa jest realizowana przez Wydział Urbanistyki i Architektury.

Wymienione wyżej usługi były realizowane zgodnie z ich opisem zamieszczonym na stronie internetowej projektu PeUP SEKAP i na stronie podmiotowej BIP Urzędu.

[Dowód: akta kontroli str. 127÷169]

Urząd publikuje w BIP opisy procedur obowiązujących przy załatwianiu drogą elektroniczną spraw z zakresu jego właściwości, w zakładce Menu przedmiotowe: Sposoby załatwiania spraw.

Karty informacyjne spraw zamieszczone w BIP zawierały opisy procedur stosowanych przy załatwianiu pięciu objętych badaniem usług świadczonych przez Urząd, w tym m.in.: Opis, Miejsce świadczenia usługi, Wymagane dokumenty, Załączniki, Opłaty, Termin załatwienia sprawy, Tryb odwoławczy, Uwagi, Ochrona danych osobowych, Podstawa prawna, Pliki (do pobrania, jeśli są).

[Dowód: akta kontroli str. 150÷169]

Stwierdzono, że w katalogu usług SEKAP w zakresie: Budownictwo, opublikowano 18 Kart informacyjnych usług, z których w pięciu przypadkach Urząd nie został wskazany jako świadczący następujące usługi:

- wydanie decyzji o pozwoleniu na budowę wraz ze zmianą sposobu użytkowania obiektu budowlanego lub jego części,
- wydanie dziennika budowy,
- wydanie opinii konserwatorskiej,
- wydanie opinii zamierzenia inwestycyjnego na terenie objętym miejscowym planem zagospodarowania przestrzennego miasta,
- wydanie zaświadczenia potwierdzającego powierzchnię użytkową oraz wyposażenie techniczne domu jednorodzinnego.

Według wyjaśnień Pełnomocnika ds. ISO oraz Naczelnika Wydziału Urbanistyki i Architektury: w powyższej sprawie został złożony wniosek do SCSI i trzy z pięciu ww. usług zostały dołączone do usług świadczonych przez Urząd, natomiast w przypadku pozostałych kart trwa postępowanie wyjaśniające z SCSI.

[Dowód: akta kontroli str. 170÷171, 598]

Centralne Repozytorium Dokumentów

Ustawa z dnia 17 lutego 2005 r. o informatyzacji działalności podmiotów realizujących zadania publiczne[9] w art. 19b ust. 3 zobowiązała organy administracji publicznej do przekazania do Centralnego Repozytorium Wzorów Dokumentów na ePUAP oraz udostępnienia w Biuletynie Informacji Publicznej wzorów dokumentów elektronicznych. Urząd złożył 4 wnioski o opublikowanie wzorów dokumentów elektronicznych w Centralnym Repozytorium Wzorów na ePUAP[10]. Wzory zostały pozytywnie zweryfikowane ale początkowo nie zostały opublikowane. W 2014 r. Urząd pięciokrotnie kontaktował się przez skrzynkę ePUAP z Ministerstwem Administracji i Cyfryzacji (MAiC), prosząc o pomoc w rejestracji opracowanych wzorów dokumentów elektronicznych, udostępnionych w Katalogu usług na SEKAP i ePUAP, w Centralnym Repozytorium Wzorów Dokumentów. Według wyjaśnień Naczelnika WI — po wysłaniu formularzy uzyskano telefoniczną informację z MAiC, że wnioski wpłynęły, lecz nie zostały zarejestrowane, gdyż elektroniczna skrzynka podawcza Urzędu (ESP) na e-PUAP ma nazwę Urząd Miejski, a nie — Urząd Miejski w Dąbrowie Górniczej. Próba zmiany nazwy nie powiodła się, gdyż dane wczytywane były automatycznie z rejestru Regon, a jego zmiana miałaby daleko idące konsekwencje. Urząd zapytał o podstawę żądania zmiany nazwy ESP, zwłaszcza, że Standard Elektronicznej Skrzynki Podawczej, wersja 1.02 z 2014 r. nie określa żadnych wymagań odnośnie nazwy podmiotu ale otrzymał tylko instrukcję jak zmienić nazwę ESP do czasu zmiany numeru Regon.

Ostatecznie wnioski Urzędu o:

- wydanie duplikatu decyzji o wykreśleniu z ewidencji działalności gospodarczej,
- stwierdzenie wygaśnięcia pozwolenia na wprowadzanie gazów lub pyłów do powietrza na wniosek prowadzącego instalację,
- wydanie duplikatu zezwolenia na sprzedaż napojów alkoholowych,
- zmianę lub skreślenie z rejestru posiadaczy odpadów zwolnionych z obowiązku uzyskiwania zezwolenia na transport odpadów,

zostały opublikowane 29 sierpnia 2014 r. pod adresem epuap.gov.pl » Wzory dokumentów (lub: epuap.gov.pl » Podmioty Publiczne » Repozytorium » Lista wzorów).

[Dowód: akta kontroli str. 182÷191]

Model Usługowy

Urząd Miejski w Dąbrowie Górniczej w podstawowym zakresie stosował rozwiązania informacyjne oparte na modelu usługowym[11] do świadczenia usług elektronicznych. Na podstawie pięciu objętych badaniem usług ustalono, że było możliwe zidentyfikowanie właściciela świadczonej usługi, tj. komórki organizacyjnej zajmującej się jej obsługą. W opisie usługi nie wskazano maksymalnego ani dopuszczalnego czasu ich niedostępności, sposobu zgłaszania awarii oraz osób/komórek/podmiotów odpowiedzialnych za usuwanie awarii, ze względu na fakt, że usługi świadczone są za pośrednictwem portalu SEKAP, a Urząd nie ma możliwości ingerencji w ich funkcjonowanie.

---

[9] Dz. U z 2014 r. poz. 1114, zwana dalej „ustawą o informatyzacji".

[10] Dotyczyło to przypadków gdy nie korzystano ze wzorów dokumentów usług świadczonych na platformie ePUAP lub platformie SEKAP.

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

Karty usług publikowane na stronie www.sekap.pl składają się z części ogólnej (takiej samej dla wszystkich urzędów) i z części spersonalizowanej (z danymi konkretnego urzędu takimi jak numery rachunków bankowych). Zostały przygotowane wspólnie przez SCSI i przedstawicieli-redaktorów urzędów partnerskich.

Po integracji z portalem e-PUAP aktualizowane karty były tam automatycznie przesyłane z portalu SEKAP.

Projektem w imieniu Województwa Śląskiego (Lidera Projektu) zarządza SCSI. Zadaniem tej jednostki, zgodnie z informacją podaną pod adresem www.sekap.pl » O projekcie SEKAP, będzie także prowadzenie działań na rzecz dalszego rozwoju Projektu w przyszłości.

[Dowód: akta kontroli str. 140÷147, 172, 173]

Współpraca wybranych systemów informatycznych z innymi systemami

Zakres współpracy systemów informatycznych wewnątrz Urzędu[12] zbadano w oparciu o dobór celowy trzech licencji na korzystanie z oprogramowania komputerowego, zakupionych na podstawie umów zawartych po 31 maja 2012 r., tj. po wejściu w życie rozporządzenia KRI, a w tym:

- Skyline Basic Solution - wdrożenie technologii 3D w ramach rozbudowy portalu MSIP, obejmujące aplikacje TerraGate i TerraExplorer Pro. Oprogramowanie to realizuje usługę e-Goverment poziomu I - informacyjnego.

  Według Szczegółowego opisu wymagań funkcjonalnych, stanowiących załącznik do umowy oraz wyjaśnień Naczelnika Wydziału Geodezji i Kartografii - SkyLine jest przeznaczone do publikacji danych wektorowych 2D i 3D w Internecie i korzysta ze standardowych formatów plików (m.in.:.tiff,.jpg,.mdb,.dxf), jak i specjalistycznych (.fly - TerraExplorer Project,.kmz – Google Sketchup i innych).

  [Dowód: akta kontroli str. 498÷318]

- Udostępnienie systemu vEdukacja Nabór, w zakresie aplikacji: *Szkoły ponadgimnazjalne* w latach szkolnych 2012/2013 i 2013/2014. Zakupiona usługa na korzystanie z tego oprogramowania dotyczyła usprawnienia rekrutacji do szkół ponadgimnazjalnych.

  Umowa zawarta „w celu usprawnienia procesu rekrutacji do jednostek oświatowych za pomocą systemu komputerowego" nie określała jakie dane i z jakich źródeł będą wykorzystywane w procesie rekrutacji. Na lata następne umowy zawierały poszczególne szkoły.

  [Dowód: akta kontroli str. 519÷569]

- Wykonanie modułu do głosowania w ramach Dąbrowskiego Budżetu Partycypacyjnego za pośrednictwem którego przeprowadzone zostało głosowanie w listopadzie 2013 r. Z uwagi na brak danych o funkcjonowaniu Modułu, co opisano poniżej nie było możliwości przeprowadzenia oględzin.

  [Dowód: akta kontroli str. 570÷578]

[12] Przyjęto możliwość wystąpienia jednego z pięciu poziomów współpracy: 1. brak współpracy (interoperacyjności), 2. informacyjny (użytkownicy systemu wiedzą, że są gromadzone dane i w razie potrzeby mogą z nich skorzystać), 3. jednostronnej komunikacji, 4. dwustronnej komunikacji oraz 5. transakcyjny (wymiana danych pomiędzy systemami bez jakiegokolwiek pośrednictwa pracownika - przekazywanie danych odbywa się w sposób w pełni zautomatyzowany).

Według wyjaśnień Naczelnika WI Moduł znajduje się poza Urzędu i nikt z pracowników WI nie miał dostępu do Modułu, a aplikacja w żaden sposób nie została przekazana Wydziałowi.

[Dowód: akta kontroli str. 580]

Według wyjaśnień Kierownika Biura Organizacji Pozarządowych i Aktywności Obywatelskiej:

- nie został on poinformowany gdzie został zainstalowany Moduł,
- w związku z zakończonym w listopadzie 2013 r. głosowaniem w ramach Budżetu Partycypacyjnego, nie ma możliwości podglądu modułu do głosowania. Zostanie on uruchomiony ponownie w listopadzie 2014 r.

[Dowód: akta kontroli str. 581÷582]

Według wyjaśnień Naczelnika Wydziału Administracyjnego Urząd korzysta z możliwości prowadzenia korespondencji w formie elektronicznej z innymi jednostkami administracji publicznej gdy istnieją możliwości prawne i techniczne, a jednostka oczekuje odpowiedzi w tej formie. Odpowiedź na korespondencję otrzymaną drogą elektroniczną udzielana była także tą drogą. Urząd nie zwracał się do innych jednostek administracji publicznej o prowadzenie wzajemnej korespondencji w formie elektronicznej. Korespondencja w formie elektronicznej prowadzona jest z Urzędem Wojewódzkim, który zwrócił się z tą sprawą i przesłał do Urzędu katalog spraw, przy których obowiązuje korespondencja wyłącznie za pośrednictwem ePUAP.

[Dowód: akta kontroli str. 597]

Ustalone nieprawidłowości

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

1. System vEdukacja nie umożliwiał osiągnięcia wymienności, o której mowa w § 4 ust. 1 pkt 2 rozporządzenia KRI, tj. możliwości zastąpienia produktu, procesu lub usługi bez jednoczesnego zakłócenia wymiany informacji pomiędzy podmiotami realizującymi zadania publiczne lub pomiędzy tymi podmiotami a ich klientami, przy jednoczesnym spełnieniu wszystkich wymagań funkcjonalnych i pozafunkcjonalnych współpracujących systemów.

   Według wyjaśnień Prezydenta Miasta - podjęte zostały rozmowy z producentem ww. oprogramowania w celu stworzenia otwartego oprogramowania gwarantującego wymianę danych pomiędzy organami prowadzącymi szkoły bez konieczności wysyłania danych osobowych uczniów.

   [Dowód: akta kontroli str. 779]

2. Moduł do głosowania w ramach Dąbrowskiego Budżetu Partycypacyjnego nie został ujęty w ewidencji wartości niematerialnych i prawnych, gdyż komórka merytoryczna nie sporządziła dowodu OT, a płatność nastąpiła z wydatków bieżących — § 4300 zakup usług pozostałych.

   Według wyjaśnień Skarbnika Miasta - treść faktury nie sugerowała że jest to wartość niematerialna i prawna. Stwierdził, że Moduł zostanie wprowadzony do ewidencji oraz, że od II kwartału 2014 r. praktykowane jest w Urzędzie sporządzanie projektów umów w uzgodnieniu z Wydziałem Księgowo-

Budżetowym, przy udziale osób posiadających wiedzę merytoryczną (Wydział Informatyki, Wydział Inwestycji Miejskich).

[Dowód: akta kontroli str. 592]

W trakcie kontroli NIK Biuro Organizacji Pozarządowych i Aktywności Obywatelskiej sporządziło dowód OT przyjęcia modułu do ewidencji księgowej i został on w niej ujęty w dniu 6 października 2014 r.

[Dowód: akta kontroli str. 783]

3. Zapisy w BIP, w tym wnioski o udostępnienie informacji publicznej, wskazywały na obowiązek podania danych osobowych przez składającego wniosek, podczas gdy przepisy art. 10-14 ustawy o dostępie do informacji publicznej nie wymagają podawania danych osobowych przy składaniu ww. wniosków.

   Według wyjaśnień Naczelnika Wydziału Administracyjnego, odpowiedzialnej od 22 stycznia 2014 r. za udostępnienie informacji publicznej na wniosek - obowiązek podawania danych osobowych wprowadzony został w formularzu wniosku jeszcze w 2003 r.

   W wyniku dokonanej w trakcie kontroli NIK aktualizacji, z dniem 26 sierpnia 2014 r. strony podmiotowej BIP Urzędu: *Sposoby załatwiania spraw* » *„Informacja publiczna”* » *Udostępnienie informacji publicznej*, w pozycji *Ochrona danych osobowych* wprowadzono zapis o braku obowiązku podawania danych osobowych wnioskodawcy gdy nie jest oczekiwana decyzja o odmowie udostępnienia tych informacji.

   [Dowód: akta kontroli str. 757÷776]

Uwagi dotyczące badanej działalności

Należy zwrócić uwagę na następujące zagadnienia związane ze świadczeniem przez Urząd usług elektronicznych:

a) omówiona wcześniej Instrukcja postępowania z Kartami informacyjnymi oraz ich załącznikami nie wiązała kart publikowanych w BIP z kartami publikowanymi na platformach SEKAP i ePUAP. Nie określała też sposobu autoryzacji treści Kart (np. podpisem elektronicznym lub sumą kontrolną), czego skutkiem był brak możliwości ustalenia dynamiki przyrostu liczby kart usług na poszczególnych platformach.

   [Dowód: akta kontroli str. 95÷102]

b) Urząd nie prowadził, okresowo weryfikowanego, wykazu usług, w tym świadczonych elektronicznie (w pełni, częściowo, informacyjnie) obejmującego potwierdzenie publikacji w BIP Urzędu, zamieszczenie w katalogu usług SEKAP i ePUAP. W związku ze stwierdzoną niewystarczającą efektywnością systemu nadzoru nad kartami usług (BIP, SEKAP, ePUAP), Pełnomocnik ISO zaplanował czynności mające na celu wzmożenie nadzoru, a w tym m.in.: doprowadzenie do ustalenia wzajemnych relacji pomiędzy Urzędem i SCSI, możliwości dalszego rozwoju projektu SEKAP, zaktywizowanie działań promocyjnych tego projektu i uszczelnienie system ewidencji Kart.

   [Dowód: akta kontroli str. 599]

Ocena cząstkowa

Najwyższa Izba Kontroli ocenia pozytywnie działalność Urzędu w zakresie realizacji wymagań określonych w § 5 ust. 3 pkt 3 rozporządzenia KRI. Na stronie Urzędu zamieszczono opisy świadczonych przez Urząd usług w formie elektronicznej. Prowadzono również komunikację elektroniczną z innymi podmiotami. Stwierdzone

nieprawidłowości dotyczyły zakupu System vEdukacja, który nie umożliwiał osiągnięcia wymienności, o której mowa w § 4 ust. 1 pkt 2 rozporządzenia KRI, bezpodstawnego żądania podawania danych osobowych we wnioskach o udostępnienie informacji publicznej oraz nie ujęcia w ewidencji wartości niematerialnych i prawnych zakupionego oprogramowania komputerowego.

2. Wdrożenie systemu zarządzania bezpieczeństwem systemów informatycznych

Opis stanu faktycznego

Dokumenty z zakresu bezpieczeństwa informacji

Zarządzeniem Prezydenta Miasta z dnia 7 czerwca 2013 r. została wprowadzona dokumentacja dotycząca ochrony danych osobowych w Urzędzie[13] - Polityka Bezpieczeństwa Ochrony Danych Osobowych (Polityka), do której załącznikiem była Instrukcja zarządzania systemem informatycznym służącym do przetwarzania danych osobowych w Urzędzie. Ponadto w październiku 2013 r. zatwierdzona została przez Prezydenta Miasta. „Instrukcja postępowania w sytuacji naruszenia bezpieczeństwa informacji".

Polityka, jak wyjaśniła Sekretarz Miasta w zakresie bieżącego funkcjonowania Urzędu pokrywa prawie całość danych chronionych w Urzędzie. Dodała również, że zagadnienia dot. informacji niejawnych uregulowane są w Planie Ochrony Informacji Niejawnych.

Pełnomocnik ds. Informacji Niejawnych wyjaśnił, że opracowywany jest nowy dokument - *Polityka Bezpieczeństwa Informacji*, który będzie określał nie tylko zakres ochrony danych osobowych, ale wszelkie ważne informacje dla jednostki oraz zasady i szczegóły zabezpieczeń stosowanych w Urzędzie, a w tym sposób przepływu danych pomiędzy poszczególnymi systemami, opis struktury zbiorów danych wskazujących zawartość poszczególnych pól informacyjnych i powiązania między nimi, zasady udostępniania i powierzania danych osobowych, procedury rozpoczęcia, zawieszenia i zakończenia pracy, przeznaczone dla użytkowników systemu. Z uwagi na przewidywane zmiany prawa, nowa Polityka zostanie wprowadzona dopiero w 2015 r.

W dalszej części wyjaśnień Pełnomocnik ds. Ochrony informacji niejawnych stwierdził, że Polityka została za potwierdzeniem przekazana do wydziałów Urzędu, a zapoznanie się z jej treścią potwierdzali pisemnie pracownicy. Od 2014 roku każda nowo przyjęta osoba do pracy w Urzędzie, przy podpisywaniu karty obiegowej zostaje zobligowana do zapoznania się z Polityką Bezpieczeństwa Ochrony Danych Osobowych i Instrukcją Zarządzania systemem informatycznym służącym do przetwarzania danych osobowych w Urzędzie (Instrukcja).

[Dowód: akta kontroli str. 240÷298, 497, 626÷635, 807]

Inwentaryzacja sprzętu informatycznego

Urząd posiada zinwentaryzowany sprzęt informatyczny, którego szczegółowa ewidencja ilościowa prowadzona jest w WI według numerów inwentarzowych nadanych przez Wydział Księgowość. Ewidencja obejmuje dane w zakresie rodzaju i konfiguracji sprzętu komputerowego, zgodnie z wymogami określonymi w § 20 ust. 2 pkt 2 rozporządzenia KRI.
Na podstawie badania 15 komputerów (w tym pięciu otrzymanych w ramach projektu pl ID ZMOKU), w zakresie możliwości zainstalowania na nich dowolnego

[13] Poprzednio obowiązywała Polityka Bezpieczeństwa Danych Osobowych przyjęta zarządzeniem Prezydenta z dnia 9 czerwca 2009 r.,

oprogramowania przez użytkowników nie będących pracownikami Wydziału Informatyzacji stwierdzono, że pracownicy nie mogli samodzielnie instalować oprogramowania na komputerach służbowych. Było to zgodne z § 20 ust. 2 pkt 4 rozporządzenia 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. 361÷368, 416÷496, 833÷845]

Urząd otrzymał z Ministerstwa Spraw Wewnętrznych i Administracji, w ramach projektu pl ID (ZMOKU) – obsługa ewidencji ludności, dowodów osobistych i aktów stanu cywilnego — 14 stacji roboczych, serwer, router, 8 skanerów, 11 drukarek oraz czytniki kart kryptograficznych. Sprzęt został zaewidencjonowany w grupie obcych środków trwałych. Wykorzystywany jest serwer do systemu obiegu dokumentów SOD, SEKAP i 11 stanowisk komputerowych.

[Dowód: akta kontroli str. 299÷316]

Analizy utraty integralności, poufności lub dostępności informacji

W Urzędzie przeprowadzano okresowe analizy utraty integralności, poufności lub dostępności informacji, na podstawie zarządzenia Prezydenta Miasta z dnia 15 listopada 2013 r. w sprawie zasad funkcjonowania kontroli zarządczej w Urzędzie. Załącznik do Regulaminu tej kontroli stanowiło Kwartalne sprawozdanie z realizacji zadań i zidentyfikowania ryzyk. Sporządzane były ponadto przez naczelników wydziałów (w tym - WI) Kwestionariusze samooceny oraz Karty ryzyka. Powyższe działania były zgodne z § 20 ust. 2 pkt 3 rozporządzenia KRI.

[Dowód: akta kontroli str. 317÷357]

Zarządzanie uprawnieniami do pracy w systemach informatycznych

Procedury nadawania upoważnień do przetwarzania danych osobowych i rejestrowania tych uprawnień w systemie informatycznym określa ww. Instrukcja zarządzania systemem informatycznym służącym do przetwarzania danych osobowych, wprowadzona zarządzeniem z dnia 7 czerwca 2013 r. Prezydenta Miasta.

Na losowo wybranej próbie 15 pracowników Urzędu, w tym pięciu osób z kierownictwa, stwierdzono, że pracownicy Urzędu zaangażowani w proces przetwarzania informacji posiadali stosowne upoważnienia i uczestniczyli w tym procesie w stopniu adekwatnym do realizowanych przez nich zadań oraz obowiązków mających na celu zapewnienie bezpieczeństwa informacji zgodnie z § 20 ust. 2 pkt 4 rozporządzenia KRI.

[Dowód: akta kontroli str. 358÷359, 416÷496]

Ponadto, badaniem objęto konta dziesięciu pracowników, z którymi rozwiązano stosunek pracy w okresie objętym kontrolą. Stwierdzono, że osoby te zostały wyrejestrowane z systemów informatycznych Urzędu objętych badaniem (konta nie były aktywne). Było to zgodne z § 20 ust. 2 pkt 5 rozporządzenia KRI stanowiącym, że zarządzanie bezpieczeństwem informacji realizowane jest w szczególności poprzez bezzwłoczną zmianę uprawnień w przypadku zmiany zadań osób zaangażowanych w proces przetwarzania informacji.

[Dowód: akta kontroli str. 372÷415, 833÷845]

Szkolenia pracowników zaangażowanych w procesie przetwarzania informacji

Zgodnie z § 20 ust. 2 pkt 6 rozporządzenia 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.

Urząd zapewnił szkolenia pracowników zaangażowanych w proces przetwarzania informacji. Pracownicy byli m.in. szkoleni przez Pełnomocnika ds. Informacji Niejawnych w zakresie ustawy o ochronie danych osobowych i rozporządzeniem wykonawczym do tej ustawy. Szkolenia przeprowadzone były również przez firmy zewnętrzne np.: w listopadzie 2012 r. w szkoleniu z zakresu regulacji prawnych dotyczących ochrony danych osobowych uczestniczyło 53 pracowników, w szkoleniu z zakresu „Standardów zarządzania usługami i bezpieczeństwem IT, a obowiązki wynikające z KRI i kontroli zarządczej" uczestniczyła jedna osoba, w konferencji bezpieczeństwa informacji w czerwcu 2013 r. uczestniczyła jedna osoba. Zakres tematyczny szkoleń obejmował: zagrożenia bezpieczeństwa informacji, skutki naruszenia zasad bezpieczeństwa informacji, w tym odpowiedzialność prawna, stosowanie środków zapewniających bezpieczeństwo informacji, w tym urządzenia i oprogramowanie minimalizujące ryzyko błędów ludzkich.

[Dowód: akta kontroli str. 604÷622]

Praca na odległość i mobilne przetwarzanie danych

W § 20 ust. 2 pkt 8 rozporządzenia KRI wskazano na obowiązek ustanowienia podstawowych zasad gwarantujących bezpieczną pracę przy przetwarzaniu mobilnym i pracy na odległość.

W myśl § 7 ust. 2 Instrukcji zarządzania systemem informatycznym służącym do przetwarzania danych osobowych w Urzędzie, użytkownik przetwarzający dane osobowe na komputerze przenośnym, ma obowiązek w sposób szczególny chronić je przed nieuprawnionym dostępem, co najmniej zabezpieczając materiał silnymi hasłami dostępu, zwłaszcza podczas transportu, przechowywania i użytkowania komputera poza wyznaczonymi miejscami, o których mowa w Polityce Bezpieczeństwa.

[Dowód: akta kontroli str. 274÷275]

Według wyjaśnień Naczelnika WI — urządzenia mobilne typu laptop, notebook są zabezpieczone wymogiem autoryzacji w domenie UMDG, a konto użytkownika ma ograniczone uprawnienia, uniemożliwiające instalację oprogramowania. Praca zdalna na tych urządzeniach nie występuje, gdyż konfiguracja routerów celowo to uniemożliwia. Użytkownicy mogą jedynie korzystać z poczty elektronicznej.

[Dowód: akta kontroli str. 623÷625]

Serwis sprzętu informatycznego i oprogramowania

W dwóch umowach dotyczących zakupu licencji spośród trzech objętych kontrolą aplikacji zawarto zapisy gwarantujące odpowiedni poziom bezpieczeństwa informacji jak następuje:

- Umowa zawarta 26 listopada 2012 r. o wdrożenie technologii 3D w ramach rozbudowy portalu MSIP w § 10 ust. 2 zawierała zobowiązanie Wykonawcy do zachowania w tajemnicy informacji powziętych przy wykonywaniu umowy także po jej zakończeniu.

[Dowód: akta kontroli str. 503]

Dodatkowo zawarta została 27 listopada 2013 r. umowa dotycząca aktualizacji licencji użytkowanego przez Urząd oprogramowania *Intergraph Polska* sp. z o.o. w Warszawie, w tym - ww. pakietu *Skyline Globe Basic Solution*, poza aktualizacją oprogramowania i dokumentacji przewidywała m.in. usuwanie usterek i awarii. Strony w § 5 umowy zobowiązały się do zachowania poufności wszelkich danych dotyczących wykonania umowy, także po jej zakończeniu.

[Dowód: akta kontroli str. 722]

- Umowa zawarta 2 lipca 2012 r. w sprawie wykonania usługi polegającej na udostępnieniu systemu vEdukacja Nabór w zakresie aplikacji: Szkoły ponadgimnazjalne oraz przeprowadzenie szkoleń, obejmowała powierzenie wykonawcy przetwarzanie danych osobowych wyłącznie w celu określonym w umowie oraz nieudostępniania danych osobom nieuprawnionym. Wykonawca zobowiązał się także do zastosowania środków technicznych i organizacyjnych, o których mowa w art. 36 do 39 ustawy o ochronie danych osobowych oraz - dopuszczania do przetwarzania danych wyłącznie osób posiadających upoważnienie do przetwarzania danych osobowych oraz prowadzenia ewidencji tych osób.

  [Dowód: akta kontroli str. 521-569]

- Trzecia z objętych kontrolą umów została zawarta 12 listopada 2013 r. i obejmowała wykonanie modułu do głosowania w ramach Dąbrowskiego Budżetu Partycypacyjnego i nie przewidywała przetwarzania danych ani dostępu do nich Wykonawcy. Umowa ta nie zawierała zapisów dotyczących zachowania przez Wykonawcę poufności informacji.

  [Dowód: akta kontroli str. 572÷573]

Prezydent Miasta poinformował, że zostanie wprowadzony obowiązek rejestracji u Pełnomocnika ds. Informacji Niejawnych umów powierzenia przetwarzania danych osobowych.

[Dowód: akta kontroli str. 780]

Jak wyjaśnił Naczelnik WI, w umowach od 2012 r. wprowadzono zapisy, że uszkodzone dyski w sprzęcie komputerowym nie wracają w ramach gwarancji do producenta sprzętu tylko pozostają w Urzędzie. Nośniki zawierające dane osobowe są niszczone komisyjnie wraz z pracownikami kancelarii tajnej.

[Dowód: akta kontroli str. 814]

Zgłaszanie incydentów naruszenia bezpieczeństwa informacji

„Instrukcja postępowania w sytuacji naruszenia bezpieczeństwa informacji" zatwierdzona przez Prezydenta Miasta w październiku 2013 r., odnosiła się do „wszelkich mogących mieć miejsce zdarzeń lub działań niezamierzonych, które stanowią lub mogły stanowić przyczynę utraty zasobów, zmian poufności, integralności, dostępności informacji lub niezawodności systemów, a także odstępstw od obowiązujących procedur postępowania, nawet, jeżeli nie prowadzą do wyżej wymienionych skutków". Określała także obowiązki użytkownika, administratora aplikacji, Administratora Bezpieczeństwa Informacji i tym osobom została przez Pełnomocnika ds. Ochrony Informacji Niejawnych przekazana z prośbą o zapoznanie z nią pracowników.

[Dowód: akta kontroli str. 626÷635, 715÷716]

Ewidencja incydentów naruszenia bezpieczeństwa informacji obejmowała jedną pozycję z 2013 r. — zgubienie poza Urzędem *pendrive* z danymi osobowymi. Wszczęto natychmiast postępowanie wyjaśniające, w wyniku którego ustalono,

że dane z Wydziału Komunikacji i Drogownictwa do Urzędu Skarbowego przekazywane były w pamięci USB dane o zarejestrowanych i wyrejestrowanych pojazdach. Ostatecznie pamięć została odnaleziona a następnie podjęto decyzję o przekazywaniu danych drogą elektroniczną przez ePUAP.

[Dowód: akta kontroli str. 636÷659]

Audyt wewnętrzny z zakresu bezpieczeństwa informacji

W 2013 r. w Urzędzie przeprowadzono audyt bezpieczeństwa informacji, a w 2014 r. w trakcie kontroli NIK prowadzony był audyt bezpieczeństwa informacji w jednostkach organizacyjnych Miasta.

W wyniku Audytu przeprowadzonego w 2013 r. wydanych zostało 40 rekomendacji. oraz 11 zaleceń obejmujących m.in.: dostosowanie ochrony informacji do wymagań rozporządzenia KRI, umożliwienie sprawnej i bezpiecznej wymiany informacji w formie elektronicznej, udoskonalenie działania bezzwłocznej zmiany uprawnień w przypadku zmiany zadań pracownika, wprowadzenie w umowach serwisowych zapisów gwarantujących odpowiedni poziom bezpieczeństwa informacji. Wykonanie rekomendacji z audytu wewnętrznego nie było monitorowane do czasu przeprowadzenia audytu sprawdzającego. Dopiero w trakcie kontroli NIK, poleceniem służbowym Prezydenta Miasta z dnia 10 października 2014 r. wprowadzony został obowiązek przesyłania informacji o wykonaniu rekomendacji po upływie terminu jej realizacji.

[Dowód: akta kontroli str. 660÷713, 730÷732]

Kopie zapasowe

Zgodnie z wymogami określonymi w § 20 ust. 2 pkt 12 lit. b i e rozporządzenia KRI, zarządzanie bezpieczeństwem informacji realizowane jest w szczególności przez zapewnienie przez kierownictwo podmiotu publicznego warunków umożliwiających realizację i egzekwowanie m.in. zapewnienia odpowiedniego poziomu bezpieczeństwa w systemach teleinformatycznych, polegającego w szczególności na: minimalizowaniu ryzyka utraty informacji w wyniku awarii i zapewnieniu bezpieczeństwa plików systemowych.

Procedury tworzenia kopii zapasowych zbiorów danych osobowych oraz programów i narzędzi programowych służących do przetwarzania danych osobowych opisane zostały w § 15 i 16 Instrukcji Zarządzania Systemem Informatycznym służącym do przetwarzania danych osobowych w Urzędzie. Sposób, miejsce i okres przechowywania elektronicznych nośników informacji i kopii ujęto w § 17.

[Dowód: akta kontroli str. 278÷281]

W Urzędzie regularnie tworzono i testowano kopie zapasowe danych i oprogramowania aplikacyjnego. Prowadzona była weryfikacja poprawnego zapisu sporządzonej kopii oraz jej odczytania. Kopie przechowywane były poza pomieszczeniem serwerowni.

[Dowód: akta kontroli str. 736]

Przeprowadzone oględziny Serwerowni wykazały, że zapewniono bezpieczne warunki pracy urządzeń zarówno w zakresie zasilania jak i warunków klimatycznych. Budynek Urzędu był objęty monitoringiem wizyjnym. Zainstalowany został alarm pożarowy i włamaniowy jak i odpowiednie zamknięcia w drzwiach wejściowych.

[Dowód: akta kontroli str. 735÷746]

Format danych udostępniania przez badane systemy informatyczne

Badane systemy/oprogramowanie korzystały z własnych zasobów informacyjnych. Nie udostępniały danych innym aplikacjom. Zawarte umowy z ich producentami nie przewidywały takiego ich wykorzystania.

[Dowód: akta kontroli str. 499÷596]

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. Było to 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 informacji wraz z zaleceniami odnoszącymi się do zawartości tego dokumentu. Zarządzeniem Prezydenta Miasta z dnia 7 czerwca 2013 r. wprowadzono „Politykę Bezpieczeństwa danych osobowych przetwarzanych w Urzędzie Miasta" do której załącznikiem była „Instrukcja zarządzania systemami informatycznymi służącymi do przetwarzania danych osobowych", a w październiku 2013 r. „Instrukcję postępowania w sytuacji naruszenia bezpieczeństwa informacji", jednakże za wyjątkiem „Instrukcji postępowania w sytuacji naruszenia…" dokumenty te nie obejmowały wszystkich informacji jakie są przetwarzane w Urzędzie lecz odnosiły się głównie do danych osobowych.

   [Dowód: akta kontroli str. 240÷298, 626÷635]

   Polityka, jak wyjaśniła Sekretarz Miasta w zakresie bieżącego funkcjonowania Urzędu pokrywa prawie całość danych chronionych w Urzędzie. Dodała również, że zagadnienia dot. informacji niejawnych uregulowane są w Planie Ochrony Informacji Niejawnych.

   Pełnomocnik ds. Informacji Niejawnych wyjaśnił, że opracowywany jest nowy dokument — Polityka Bezpieczeństwa Informacji, który będzie określał nie tylko zakres ochrony danych osobowych, ale wszelkie ważne informacje dla jednostki oraz zasady i szczegóły zabezpieczeń stosowanych w Urzędzie, a w tym sposób przepływu danych pomiędzy poszczególnymi systemami, opis struktury zbiorów danych wskazujących zawartość poszczególnych pól informacyjnych i powiązania między nimi, zasady udostępniania i powierzania danych osobowych, procedury rozpoczęcia, zawieszenia i zakończenia pracy, przeznaczone dla użytkowników systemu. Z uwagi na przewidywane zmiany prawa, nowa Polityka zostanie wprowadzona dopiero w 2015 r.

   [Dowód: akta kontroli str. 497, 807]

2. Pełnomocnik ds. Ochrony Informacji Niejawnych zlecająca na wniosek naczelników wydziałów nadanie lub cofanie uprawnień poszczególnym użytkownikom systemów nie miała możliwości samodzielnego sprawdzenia wykonania tych zleceń, z uwagi na brak stosownych uprawnień.

   [Dowód: akta kontroli str. 600÷602]

Poleceniem służbowym z dnia 5 września 2014 r. Prezydenta Miasta, ustalony został dla administratorów aplikacji obowiązek udostępniania na każde żądanie Administratora Bezpieczeństwa Informacji wglądu do panelu administracyjnego.

[Dowód: akta kontroli str. 603]

Według wyjaśnień Prezydenta Miasta - funkcja wydruku i kontroli uprawnień użytkowników do przetwarzania danych nie jest na razie standardową funkcją oprogramowania. Uznając za zasadne wprowadzenie takich funkcji — prowadzone jest rozeznanie możliwości i ceny jej wdrożenia.

[Dowód: akta kontroli str. 780]

3. Dopuszczeniu do przetwarzania danych osobowych przez wykonawcę oprogramowania „Moduł do głosowania w ramach Dąbrowskiego Budżetu Partycypacyjnego", mimo niezawarcia umowy, co było niezgodne z art. 31 ustawy o ochronie danych osobowych. Stwierdzono bowiem, że:
   - w dniu 12 listopada 2013 r. Gmina Dąbrowa Górnicza reprezentowana przez Prezydenta Miasta oraz Kierownika Biura Organizacji Pozarządowych i Aktywności Obywatelskiej zawarła umowę z firmą, która zobowiązała się do wykonania „Modułu do głosowania w ramach Dąbrowskiego Budżetu Partycypacyjnego",
   - w listopadzie 2013 r. przeprowadzone zostało głosowanie w sprawie Budżetu Partycypacyjnego, zgodnie z zarządzeniem Prezydenta Miasta[14], a w instrukcji głosowania wskazano m.in. że:
     - głosowanie odbywa się: elektronicznie poprzez formularz znajdujący się na stronie Budżetu partycypacyjnego lub korespondencyjnie poprzez przesłanie formularza na adres Urzędu Miasta lub wrzucenie bezpośrednio do skrzynek (UM) znajdujących się w Punkcie Konsultacyjnym,
     - głosujący składali oświadczenie, w którym wyrażali zgodę na przetwarzanie danych osobowych dla potrzeb niezbędnych do opracowania wyników głosowania w ramach prowadzonych wydatków z budżetu Miasta Dąbrowa Górnicza czyli Budżetu Partycypacyjnego,

     co świadczy, że administratorem danych osobowych był Prezydent Miasta, ponieważ zgodnie z art. 7 pkt 4 ustawy o ochronie danych osobowych decydował o celach i środkach przetwarzania danych osobowych.
   - ww. Moduł nie był zainstalowany na serwerze Urzędu,
   - w dniu 10 stycznia 2014 r. zawarta została umowa powierzenia danych osobowych, w której w pkt 1 stwierdzono, że przedmiotem umowy jest przekazanie Urzędowi zbioru danych osobowych, które wykonawca ww. Modułu uzyskał w związku z przeprowadzonym w listopadzie 2013 r. głosowaniem mieszkańców w ramach Budżetu Partycypacyjnego. Załącznikiem do tej umowy był protokół przekazania Urzędowi przez wykonawcę w dniu 14 stycznia 2014 r. danych osobowych, który ze strony Urzędu podpisał Kierownik Biura Organizacji Pozarządowych i Aktywności Obywatelskiej. Nośnik, tj. płyta CD została przyjęta do depozytu przez

[14] Zarządzenie Prezydenta Miasta nr 1952/2013 z 30 października 2013 r. w sprawie zmian do zarządzenia nr 1904/2013 w sprawie terminu głosowania oraz wzoru karty do głosowania w ramach Budżetu Partycypacyjnego.

Pełnomocnika ds. Ochrony Informacji Niejawnych bez sprawdzenia zawartości.

[Dowód: akta kontroli str. 572-573, 584÷591, 808]

Prezydent Miasta udzielając wyjaśnień potwierdził, że umowa zawarta z dostawcą oprogramowania nie przewidywała przetwarzania danych oraz nie wskazał podstaw powierzenia przetwarzania danych przez tego dostawcę.

[Dowód: akta kontroli str. 782]

Uwagi dotyczące badanej działalności

NIK zwraca uwagę, że Prezydent Miasta powierzył w umowie producentowi oprogramowania systemu vEdukacja przetwarzanie danych osobowych, lecz nie kontrolował tego czy podmiot, któremu dane powierzono, przetwarza je zgodnie z postanowieniami umowy. W toku kontroli NIK, w dniu 15 października 2014 r. pracownicy Urzędu przeprowadzili kontrolę deklarowanych warunków przetwarzania danych, nie stwierdzając nieprawidłowości.

[Dowód: akta kontroli str. 521-569, 781, 817-832]

Ocena cząstkowa

Najwyższa Izba Kontroli ocenia pozytywnie mimo stwierdzonych nieprawidłowości działalność Prezydenta w zakresie wdrożenia systemu zarządzania bezpieczeństwem systemów informatycznych. Zabezpieczono komputery wykorzystywane w Urzędzie przed możliwością zainstalowania nieautoryzowanego oprogramowania. Byłym pracownikom Urzędu odbierano uprawnienia do pracy w systemach informatycznych. Właściwie przechowywano kopie zapasowe danych. Ustalenia kontroli wykazały jednak nieprawidłowość przy realizacji zadań określonych w rozporządzeniu KRI polegającą na nieopracowaniu i niewdrożeniu całościowej Polityki Bezpieczeństwa Informacji, która jest elementem systemu zarządzania bezpieczeństwem informacji, co było niezgodne z § 20 ust. 3 rozporządzenia KRI, a ponadto powierzono przetwarzanie danych osobowych bez zawarcia umowy wymaganej przepisem art. 31 ustawy o ochronie danych osobowych.

3. Zapewnienie dostępności informacji dla osób niepełnosprawnych

Opis stanu faktycznego

W toku kontroli zweryfikowano stronę internetową Urzędu oraz stronę BIP Urzędu pod względem dostosowania sposobu prezentacji danych do potrzeb osób niedowidzących z wykorzystaniem narzędzia dostępnego pod adresem http://validator.w3.org/ i stwierdzono wystąpienie:

- http://www.dabrowa-gornicza.pl/ - trzech błędów i dwóch ostrzeżeń,
- http://www.bip.dabrowa-gornicza.pl/ - sześciu błędów i jednego ostrzeżenia.

W badaniu z wykorzystaniem narzędzia dostępnego na stronie [http://jigsaw.w3.org/css-validator/] Walidator arkuszy stylu, stwierdzono brak błędów i 124 ostrzeżenia na stronie Urzędu oraz 47 błędów i 45 ostrzeżeń na stronie BIP Urzędu.

Według wyjaśnień Naczelnika WI - informacja o błędach walidacji strony BIP została przekazana wykonawcy tej strony.

[Dowód: akta kontroli str. 756]

Ocena cząstkowa

Najwyższa Izba Kontroli nie formułuje oceny cząstkowej w tym obszarze, gdyż zgodnie z § 22 Rozporządzenia 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 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[15], wnosi o:

1. **Opracowanie i wdrożenie Polityki Bezpieczeństwa Informacji, określającej zasady bezpieczeństwa informacji, zgodnie z wymaganiami wynikającymi z § 20 ust. 3 rozporządzenia KRI.**
2. **Dostosowanie dokumentów związanych z usługami elektronicznymi do zgodności z przepisami ustawy o ochronie danych osobowych.**
3. **Zapewnienie w zawieranych umowach związanych z systemami informatycznymi bezpieczeństwa w zakresie w ochrony przetwarzania danych osobowych, w tym unikanie powierzania przetwarzania danych osobowych jeśli nie jest to niezbędne.**

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 października 2014 r.

Najwyższa Izba Kontroli
Delegatura w Katowicach

Kontrolerzy
Arkadiusz Przytulski
specjalista kontroli państwowej

. . . . . .

. . . . . .

Jerzy Horodecki
gł. specjalista kontroli państwowej

. . . . . .

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