NAJWYŻSZA IZBA KONTROLI
Delegatura we Wrocławiu

LWR-4101-013-03/2014
P/14/004

WYSTĄPIENIE POKONTROLNE

NAJWYŻSZA IZBA KONTROLI
Delegatura we Wrocławiu
ul. Marszałka J. Piłsudskiego 15/17, 50-044 Wrocław
T +48 71 711 83 00, F +48 71 711 83 50
lwr@nik.gov.pl

I. Dane identyfikacyjne kontroli

Numer i tytuł kontroli

P/14/004 – Wdrażanie wybranych wymagań dotyczących systemów teleinformatycznych, wymiany informacji w postaci elektronicznej oraz Krajowych Ram Interoperacyjności na przykładzie niektórych urzędów gmin miejskich i miast na prawach powiatu.

Jednostka przeprowadzająca kontrolę

Najwyższa Izba Kontroli
Delegatura we Wrocławiu

Kontrolerzy

1. Cezary Mazik, inspektor k.p., upoważnienie do kontroli nr 89805 z dnia 15 lipca 2014 r.
2. Małgorzata Grudowska, starszy inspektor k.p, upoważnienie do kontroli nr 89804 z dnia 15 lipca 2014 r.

(Dowód: akta kontroli str. 1-4)

Jednostka kontrolowana

Urząd Miejski w Głogowie, Rynek 10, 67-200 Głogów (dalej: Urząd)

Kierownik jednostki kontrolowanej

Jan Kazimierz Zubowski, Prezydent Miasta Głogowa (dalej: Prezydent Miasta)

(Dowód: akta kontroli str. 300; 302-303)

II. Ocena kontrolowanej działalności

Ocena ogólna[1]

Prezydent Miasta Głogowa, 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* (dalej: *rozporządzenie w sprawie KRI*)[2] w okresie od 31 maja 2012 r. do 14 sierpnia 2014 r.:

- zapewnił współpracę pomiędzy systemami informatycznymi w sposób zapewniający minimalne wymogi w zakresie interoperacyjności,
- zapewnił wykorzystanie elektronicznego obiegu dokumentów wewnątrz Urzędu,
- udostępnił mieszkańcom 141 usług elektronicznych,
- wprowadził Elektroniczny Obieg Dokumentów do jednostek organizacyjnych Gminy Miejskiej Głogów,
- wdrożył procedury nakazującej pracownikom niezwłoczne zgłaszanie incydentów naruszenia bezpieczeństwa informacji w sposób umożliwiający podjęcie działań korygujących.

W wyniku kontroli stwierdzono również nieprawidłowości przy realizacji zadań określonych w *rozporządzeniu w sprawie KRI*, które w szczególności polegały na: **[1]** braku Polityki Bezpieczeństwa Informacyjnego, spełniającej wymogi *rozporządzenia w sprawie KRI*; **[2]** nieobjęciu niektórych systemów i zasobów informatycznych procedurą nadawania uprawnień w Urzędzie; **[3]** niesporządzaniu w większości badanych przypadków wniosków o nadanie/cofnięcie uprawnień do wykorzystywanych systemów i modułów informatycznych dla pracowników lub

[1] Najwyższa Izba Kontroli stosuje 3-stopniową skalę ocen: pozytywna, pozytywna mimo stwierdzonych nieprawidłowości, negatywna. Jeżeli sformułowanie oceny ogólnej według proponowanej skali byłoby nadmiernie utrudnione, albo taka ocena nie dawałaby prawdziwego obrazu funkcjonowania kontrolowanej jednostki w zakresie objętym kontrolą, stosuje się ocenę opisową, bądź uzupełnia ocenę ogólną o dodatkowe objaśnienie.
[2] Dz. U. z 2012 r., poz. 526.

byłych pracowników Urzędu; **[4]** braku procedur gwarantujących bezpieczną pracę przy przetwarzaniu mobilnym i pracy na odległość; **[5]** niezamieszczeniu wzorów dokumentów elektronicznych w centralnym repozytorium ePUAP.

III. Opis ustalonego stanu faktycznego

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

Opis stanu faktycznego

1.1. Zagadnienia dotyczące dostosowania Urzędu do elektronicznego świadczenia usług publicznych zostały zawarte w dokumencie „E-Głogów – strategia budowy i rozwoju społeczeństwa informacyjnego w Głogowie"[3], obejmującym okres do 2020 r. Projekt ten obejmuje 26 inicjatyw związanych z wdrożeniem w Głogowie usług elektronicznych w obszarach m.in. administracji, edukacji, zdrowia, biznesu, transportu. W dokumencie tym zdefiniowano następujące cele:

- *zapewnienie dostępności obywateli do administracji publicznej za pomocą budowy i rozbudowy sieci telekomunikacyjnych, jak również w wyniku informatyzacji urzędu;*
- *zapewnienie dostępu do placówek edukacyjnych i kulturalnych umożliwiając studiowanie przez Internet, a także wysokiej jakości materiałów, zajęć i szkoleń;*
- (rozwój) *usług medycznych dających lekarzom i pracownikom ochrony zdrowia sprawne narzędzie do przesyłania danych o pacjentach, rejestracjach wizyt i porad;*
- *zmiany modelu zarządzania przedsiębiorstw poprzez szerokie wykorzystywanie środków komunikacji elektronicznej;*
- *rozwój usług inteligentnego transportu.*

(Dowód: akta kontroli str. 584-590 i 647-648)

Dodatkowo, na mocy zarządzenia Prezydenta Miasta[4] z dnia 19 stycznia 2010 r., Urząd przyjął do realizacji projekt o charakterze strategicznym na lata 2007-2013 pn. „E-Głogów – rozwój usług elektronicznych na rzecz mieszkańców Gminy Miejskiej Głogów", którego głównym celem było *przygotowanie Gminy Miejskiej Głogów do świadczenia e-usług na rzecz mieszkańców Gminy, powiatu głogowskiego, regionu (w tym odbiorcy indywidualni i przedsiębiorcy)*. Projekt ten został zrealizowany.

(Dowód: akta kontroli str. 16 i 565- 583)

1.2. Urząd, w ramach promocji komunikacji elektronicznej, zamieszczał informacje na lokalnych portalach internetowych oraz w drukowanych materiałach reklamowych, a także wykorzystywał portale społecznościowe.

(Dowód: akta kontroli str. 31 i 564)

1.3. Urząd nie przeprowadzał badań potrzeb mieszkańców w zakresie korzystania z usług elektronicznych oraz elektronicznej komunikacji z Urzędem. Naczelnik Wydziału Komunikacji Społecznej Urzędu wyjaśnił, że zastosowano w tym zakresie inne mierniki zainteresowania e-usługami, tj. głównie statystyki ilości wejść na strony internetowe Urzędu.

(Dowód: akta kontroli str. 31; 737)

---

[3] Uchwała Rady Miejskiej w Głogowie nr XXXVIII/325/206 z dnia 7 lutego 2006 w sprawie przyjęcia programu 'E-Głogów – strategia budowy i rozwoju społeczeństwa informacyjnego w Głogowie".

[4] Zarządzenie Prezydenta Miasta Głogowa nr 19/2010 z dnia 19 stycznia 2010r. w sprawie powołania Zespołu ds. Realizacji Projektu w związku z realizacją zadania pod nazwą „E-Głogów – rozwój usług elektronicznych na rzecz mieszkańców Gminy Miejskiej Głogów".

1.4. Urząd nie zwracał się do Ministerstwa Administracji i Cyfryzacji (dalej: MAiC) z problemami, jak również z prośbą o pomoc w zakresie dostosowania swoich systemów/rejestrów informatycznych do wymogów *rozporządzenia w sprawie KRI.*

(Dowód: akta kontroli str. 31)

1.5. Proces obiegu dokumentacji oraz zarządzania dokumentami regulowała Instrukcja Elektronicznego Obiegu Dokumentów (dalej: Instrukcja EOD), wprowadzona zarządzeniem Prezydenta Miasta nr 23/2013 z dnia 1 sierpnia 2013 r. Dodatkowo w Regulaminie Organizacyjnym Urzędu z dnia 10 października 2013 r.[5] opisano kwestię opiniowania oraz elektronicznej autoryzacji zarządzeń Prezydenta włączanych do obiegu elektronicznego, a także wskazano, że *sprawy wniesione przez Obywateli do Urzędu są ewidencjonowane i wprowadzane do elektronicznego systemu EZD (tj. zarządzania dokumentami).* Instrukcja EOD opisuje szczegółowo obieg pism wpływających w formie papierowej oraz elektronicznej, definiuje zadania poszczególnych pracowników Urzędu w procesie obiegu dokumentów oraz precyzuje jaki rodzaj spraw realizowanych przez poszczególne Wydziały oraz komórki organizacyjne nie podlega procedowaniu w obiegu elektronicznym.

(Dowód: akta kontroli str. 548 – 554)

EOD w Urzędzie był oparty o system informatyczny Intradok[6]. System ten spełnia wymagania 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*[7].
Opis działania EOD przedstawiał się następująco: *Proces elektronicznego obiegu dokumentów inicjowany jest w Biurze Obsługi Mieszkańca (dalej: BOM). Dokumenty wpływające do Urzędu w formie elektronicznej*[8] *są importowane do systemu Intradok*[9]*. Pracownik BOM po zapoznaniu się z treścią każdego dokumentu, rejestruje go, a następnie dekretuje do odpowiedniego Wydziału lub komórki organizacyjnej Urzędu*[10]*. Dokumenty zarejestrowane w systemie pojawiają się na kontach poszczególnych pracowników Urzędu, którzy po jego otrzymaniu zakładają odpowiednią „Sprawę"*[11]*. Realizując kolejne etapy załatwiania sprawy, dołączają oni do sprawy kolejne dokumenty w formie elektronicznej. W przypadku, gdy wymagane jest przygotowanie odpowiedzi, pracownik umieszcza jej wersję elektroniczną w systemie Intradok, a następnie przesyła ją do akceptacji przełożonego*[12]*. Finalnie powstaje odpowiedź, która jest sygnowana podpisem elektronicznym Prezydenta Miasta lub osoby upoważnionej. Następnie odpowiedź jest drukowana w jednym egzemplarzu, podpisywana przez osobę upoważnioną i przesyłana do zainteresowanego.* W Urzędzie pozostaje wyłącznie dokumentacja elektroniczna,

---

[5] Załącznik do Zarządzenia Nr 31/2013 Prezydenta Miasta Głogowa z dnia 10 października 2013 r. - § 21 ust. 1 i ust. 3.

[6] Jest to pakiet oprogramowania do zarządzania dokumentami, korespondencją, sprawami oraz poleceniami. Umożliwia on sprawny dostęp do dokumentów, informacji, kontroluje drogę ich obiegu oraz stan realizacji, usprawnia obsługę klientów oraz wspomaga kontrolę terminowości załatwianych spraw. Umożliwia także ewidencję dokumentów, pism przychodzących i wychodzących, poleceń służbowych oraz regulacji wewnętrznych. System posiada także funkcje identyfikacji i autoryzacji, pozwalając na rejestrowanie wszystkich operacji wykonywanych przez użytkowników umożliwiając tym samym prześledzenie ścieżki którą pismo przebyło od wejścia, aż do wyjścia.

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

[8] Np. za pośrednictwem platformy ePUAP, www.glogow.pl.

[9] System wszystkie pobrane w danym dniu wnioski prezentuje w dedykowanym folderze jako „Nowe".

[10] Dokumenty zaadresowane imiennie do Sekretarza, Wiceprezydenta Prezydenta, lub konkretnego pracownika są przez BOM rejestrowane i przekierowywane do wskazanej osoby. Jeśli BOM ma kłopot z dekretacją lub dokument ma charakter ogólny, zostaje on przekierowany do Sekretarza lub osoby go zastępującej. Sekretarz lub osoba go zastępująca, Prezydent lub Wiceprezydent decyduje o finalnej dekretacji i przekierowuje sprawę do właściwej komórki organizacyjnej.

[11] Formę elektronicznych akt dla dokumentów które będą sprawie towarzyszyć.

[12] Pismo na każdym etapie akceptacji może być zwrócone do projektującego z prośbą o dokonanie stosownej korekty.

zgromadzona w archiwum systemu Intradok. W przypadku dokumentów wpływających do Urzędu w formie tradycyjnej (papierowej), pracownik BOM skanuje dokumentację i wprowadza do systemu Intradok. Następnie postępuje się z nimi tak, jak z dokumentacją wpływającą do Urzędu w formie elektronicznej.
Dokumenty, które nie podlegały procedowaniu za pośrednictwem systemu Intradok[13] były w nim wyłącznie rejestrowane jako przychodzące. Resztę procesu, tj. dekretacja, procedowanie, przygotowanie odpowiedzi, jej opiniowanie i akceptacja realizowane były w formie tradycyjnej. Odpowiedź, która wychodziła z Urzędu podlegała rejestracji w systemie.

(Dowód: akta kontroli str. 731-732)

1.6. W okresie od 31 maja 2012 r. do 31 maja 2014 r. do Urzędu wpłynęło 54 614 dokumentów, w tym 678 w formie elektronicznej, tj. 1,24%. W tym samym okresie z Urzędu wysłano 175 242 dokumentów, przy czym formę elektroniczną zastosowano w odniesieniu do 0,08% przypadków (142 razy)[14].

(Dowód: akta kontroli str. 512)

1.7. Urząd świadczył 141[15] usług za pośrednictwem platform ePUAP, BIP oraz www.glogow.pl, a w czasie kontroli NIK udostępniał:
- 16 usług w pełni elektronicznych[16],
- 125 usług częściowo elektronicznych[17].

Od 31 maja 2012 r. przybyło siedem usług na platformie ePUAP (przyrost ilości usług - 39%), oraz po cztery na pozostałych serwisach (przyrost ilości usług - 3%).

(Dowód: akta kontroli str. 13-16, 502-504, 507-511)

Szczegółową kontrolą poprawności opisów objęto pięć usług elektronicznych świadczonych przez Urząd[18]. Opisy wszystkich sprawdzanych usług były zgodne z usługami faktycznie świadczonymi.

(Dowód: akta kontroli str. 479-481)

1.8. Każda z badanych pięciu usług elektronicznych posiadała w karcie opisu usługi informacje dotyczące m.in.: aktualnej podstawy prawnej, celu, adresata usługi, miejsca świadczenia usługi, opłat, terminu realizacji, trybu odwoławczego oraz danych kontaktowych do osoby lub osób udzielającej merytorycznych informacji nt. usług.

(Dowód: akta kontroli str. 479-506)

Urząd nie wydawał oraz nie publikował na stronach internetowych (ePUAP, BIP i www.glogow.pl) ogólnych procedur obowiązujących przy realizacji spraw w trybie elektronicznym

Dowody: Akta kontroli str. 479-506

1.9. Urząd do dnia zakończenia czynności kontrolnych (14 sierpnia 2014 r.) nie opublikował wzorów dokumentów elektronicznych w centralnym repozytorium ePUAP, dostępnym pod adresem www.crd.gov.pl.

(Dowód: akta kontroli str. 288-290)

---

[13] Wymienione w Instrukcji EOD, są to m.in. publikacje, dokumenty księgowe, kadrowe, dotyczące zamówień publicznych, zastrzeżone, wymienione wnioski i sprawy itp.
[14] Wychodzące dokumenty są rejestrowane lub znajdują się w systemie informatycznym.
[15] Łącznie Urząd udostępniał 141 usług: 21 na wszystkich portalach, trzy tylko na ePUAP, a 117 na innych portalach niż ePUAP.
[16] Zawierających co najmniej dedykowany formularz elektroniczny, w tym dziewięć umożliwiających wykonanie elektronicznie opłaty.
[17] Zawierających dołączony formularz w formacie pdf lub doc lub opis usługi.
[18] 1). Odpis i zaświadczenie z ksiąg stanu cywilnego, 2). Wniosek o wydanie dowodu osobistego, 3). Zameldowanie na pobyt stały, 4). Wnioski w sprawie ulg w spłacie zobowiązań podatkowych, 5). Wypis i wyrys ze studium i planu miejscowego.

1.10. Wszystkie, poddane szczegółowej kontroli, pięć usług elektronicznych świadczonych przez Urząd posiadało karty opisu usługi. Ich ostatnia aktualizacja nastąpiła w 2011 r. i 2012 r. w serwisie ePUAP oraz w 2013 i 2014 r. w serwisie BIP i www.glogow.pl. We wszystkich kartach określony został właściciel usługi oraz wskazywano czas dostępności usługi[19]. Dla usług świadczonych za pośrednictwem administrowanych przez Urząd stron BIP oraz www.glogow.pl nie określono dopuszczalnych, ani maksymalnych czasów niedostępności usługi. W przypadku problemów z serwisem, na stronach tych pojawia się ogólny komunikat o jego niedostępności. W kontekście powyższego, należy stwierdzić, że Urząd w procesie zarządzania usługami wspierał model usługowy w podstawowym zakresie.

(Dowód: akta kontroli str. 479-506)

1.11. Zakres współpracy systemów informatycznych wewnątrz Urzędu zbadano w oparciu o cztery systemy zakupione po 31 maja 2012 r.[20]:

1) system informatyczny „Intradok". wspierający elektroniczny obieg dokumentów Urzędu;
2) moduły systemu Ratusz[21]:
   a. „Firmy" – program służy do obsługi wymiaru i księgowości podatku od nieruchomości, rolnego i leśnego osób prawnych;
   b. „Posesja" - służy do obsługi wymiaru i księgowości podatku od nieruchomości, rolnego i leśnego osób fizycznych;
   c. „Pojazdy" - służy do obsługi podatku od środków transportowych pojazdów powyżej 3,5 tony;
   d. „Rejestr opłat" - służy do kompleksowej obsługi przyjmowania dowolnych opłat niepodatkowych od osób fizycznych i prawnych.
3) „Odpady Komunalne" - wspierający zarządzanie odpadami komunalnymi[22];
4) „Użytkowanie Wieczyste" - wspierający obsługę umów użytkowania wieczystego[23].

(Dowód: akta kontroli str. 736)

Poziom współpracy (interoperacyjności) tych systemów można sklasyfikować jako:

- jednostronnej komunikacji[24] – moduły aplikacji Ratusz:
  - „Odpady Komunalne" - jako jedyny z modułów Systemu Ratusz komunikuje się z platformą ePUAP oraz usługami udostępnionymi na www.glogow.pl - istnieje możliwość złożenia elektronicznej deklaracji podatkowej. Jeśli klient złoży deklarację w formie tradycyjnej, system wymaga ręcznego zasilania danymi z deklaracji;
  - „Użytkowanie Wieczyste" - system wymaga ręcznego zasilania danymi z aktów notarialnych otrzymywanych od osób fizycznych, dodatkowo wymaga ręcznego zasilania informacjami z Powiatowego Ośrodka Dokumentacji Geodezyjnej i Kartograficznej w Głogowie. Moduł posiada funkcję komunikowania się z rejestrem centralnym PESEL, ale komunikacja ta wymuszana jest ręcznie – jeden raz w miesiącu dane aktualizuje firma dostarczająca oprogramowanie;
  - „Firmy" - system wymaga ręcznego zasilania danymi z deklaracji podatkowych. Moduł wymienia informację jedynie pomiędzy częścią, w której wyliczany jest wymiar podatku, a częścią księgową;

---

[19] Wskazanie kiedy klient może zrealizować usługę.
[20] Data wejścia w życie rozporządzenia KRI.
[21] Zakupione 24 kwietnia 2014 r.
[22] Moduł systemu Ratusz zakupiony 21 grudnia 2012 r.
[23] Moduł systemu Ratusz zakupiony 20 czerwca 2013 r.
[24] Dane z jednego systemu są przekazywane do innego systemu za pośrednictwem pracownika (operatora systemu), który dane te importuje ręcznie do systemu.

- „Posesja" - system wymaga ręcznego zasilania danymi z deklaracji podatkowych oraz ksiąg wieczystych. Moduł wymienia informację jedynie pomiędzy częścią w której wyliczany jest wymiar podatku, a częścią księgową;
- „Pojazdy" - system wymaga ręcznego zasilania danymi z deklaracji podatkowych;

- dwustronnej komunikacji[25] - system Intradok nie jest zintegrowany z żadnym systemem użytkowanym w Urzędzie. System ten umożliwia dołączanie dokumentów opracowanych z wykorzystaniem oprogramowania biurowego. Dane wymieniane są w sposób transakcyjny, wyłącznie pomiędzy jego użytkownikami. System komunikuje się z systemem usług udostępnionych na www.glogow.pl, ePUAP oraz BIP, ale komunikacja ta musi zostać wymuszona przez użytkownika poprzez funkcję importu lub eksportu. Klient może podglądnąć status sprawy na portalu BIP – pod warunkiem, że zna numer sprawy, a klient posiadający konto na www.glogow.pl lub ePUAP otrzymuje odpowiedzi w formie elektronicznej logując się do portalu;
- transakcyjny[26] - moduł aplikacji Ratusz „Rejestr Opłat" - komunikuje się transakcyjnie z modułem „Użytkowanie Wieczyste" oraz „Posesja" i „Firmy" (częścią-modułem „Wymiar"), widoczne są dane osobowe, dotyczące umów (numer działki, rodzaj gruntu) oraz kwoty należności.

W ocenie NIK badane 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. 518 i 734-735)

1.12. Wszystkie jednostki Gminy Miejskiej Głogów[27] zostały, na podstawie pisma Prezydenta Miasta[28], zobowiązane do stosowania elektronicznej formy komunikacji za pośrednictwem platformy ePUAP. Dodatkowo, włączono je do EOD za pośrednictwem systemu Intradok oraz przeszkolono z zakresu korzystania z tego systemu i portalu ePUAP[29]. Działania te wynikały z realizacji projektu „E-Głogów – rozwój usług elektronicznych na rzecz mieszkańców gminy miejskiej Głogów".

(Dowód: akta kontroli str. 519-520, 544-547)

Urząd zwrócił się także do 19 innych instytucji i jednostek, w tym administracji publicznej, z prośbą[30] o możliwość wymiany korespondencji za pośrednictwem skrzynek ePUAP. W wyniku tego działania sześć jednostek wyraziło gotowość wymiany informacji w formie elektronicznej i częściowo z niej korzysta[31].

(Dowód: akta kontroli str. 521-542)

W okresie objętym kontrolą do Urzędu wpłynęło jedno pismo od Wojewody Dolnośląskiego[32] z prośbą o przesyłanie rejestrów wydanych decyzji za pośrednictwem ePUAP. Urząd dostosował się do tej prośby.

(Dowód: akta kontroli str. 543)

---

[25] Dane z jednego systemu informatycznego przekazywane są do innego systemu, wymagane jest zatwierdzenie wyników przez operatora, odpowiedź z systemu jest przekazywana analogicznie.
[26] Wymiana danych pomiędzy systemami bez jakiegokolwiek pośrednictwa pracownika, czyli przekazywanie danych odbywa się w sposób w pełni zautomatyzowany.
[27] Przedszkola, Szkoły Podstawowe, Gimnazja, Spółki oraz Instytucje i Zakłady.
[28] Z dnia 21 listopada.2012 r.
[29] Część korespondencji mimo to wysyłana jest w dalszym ciągu drogą tradycyjną.
[30] Pismo Wydziału Administracyjno-Gospodarczego UM w Głogowie z dnia 20 lutego 2013 r.
[31] Korespondencja z Urzędem Skarbowym w Głogowie, Kuratorium Oświaty we Wrocławiu, ZUS Oddziałem w Legnicy Inspektoratem w Głogowie, Urzędem Marszałkowskim Województwa Dolnośląskiego, Dolnośląskim Urzędem Wojewódzkim i Urzędem Gminy Głogów.
[32] Z dnia 7 listopada 2012 znak:IF-PP.740.12.2012-1.KK.

Urząd prowadził elektronicznie ponadto:
- bieżącą wymianę danych statystycznych za pośrednictwem dedykowanego Portalu Sprawozdawczego Głównego Urzędu Statystycznego,
- wysyłkę sprawozdań budżetowych do Regionalnej Izby Obrachunkowej za pośrednictwem portalu BESTIA.

(Dowód: akta kontroli str. 519-520)

Badane systemy Urzędu nie pobierały bezpośrednio danych z rejestrów centralnych, tj. CEIDG oraz PESEL. Tylko jeden z modułów systemu Ratusz – „Użytkowanie Wieczyste" oferował możliwość pobierania danych z rejestru PESEL. Funkcja ta wykorzystywana była jeden raz w miesiącu - dostawca oprogramowania aktualizował bazę z rejestrem PESEL.

(Dowód: akta kontroli str. 734-735)

W kontekście powyżej opisanych sposobów wymiany danych z innymi jednostkami, poziom współpracy systemów można sklasyfikować jako dwustronnej komunikacji, spełniający w minimalnym stopniu wymogi interoperacyjności określone w § 5 ust.3 pkt 3 *rozporządzenia w sprawie KRI*.

Ustalone nieprawidłowości

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

1. Urząd do dnia kontroli NIK nie umieścił wzorów dokumentów elektronicznych w centralnym repozytorium ePUAP, dostępnym pod adresem www.crd.gov.pl, co było niezgodne z art. 19b ust. 3 ustawy z dnia 17 lutego 2005 r. *o informatyzacji działalności podmiotów realizujących zadania publiczne*[33], w myśl której, organy administracji publicznej przekazują do centralnego repozytorium wzory dokumentów dotyczących świadczonych przez jednostkę usług elektronicznych. Jako przyczynę tego stanu główny specjalista, pełniący obowiązki informatyka oraz Administratora Systemów Informatycznych (dalej: ASI) wskazał na mylną interpretację zapisów ww. ustawy (art. 19b ust. 3), według której umieszczanie wzorów w repozytorium zinterpretowano jako zadanie fakultatywne, a nie jako obowiązek, który powinna realizować jednostka.

(Dowód: akta kontroli str. 288-290)

Uwagi dotyczące badanej działalności

NIK zwraca uwagę, że Urząd nie wykorzystywał w pełni funkcji automatycznej wymiany danych udostępnionej w modułach aplikacji Ratusz („Firmy", „Posesja" oraz „Pojazd"), które oferują możliwość wczytywania do systemu danych z deklaracji i załączników złożonych przez podatników za pomocą platformy ePUAP.

(Dowód: akta kontroli str. 734-735)

Ocena cząstkowa

Najwyższa Izba Kontroli ocenia pozytywnie działalność Urzędu w zakresie wdrażania wymogów *rozporządzenia w sprawie KRI*, dotyczących współpracy systemów informatycznych i ich dostosowania do wymiany danych z innymi systemami oraz podmiotami. Stwierdzona nieprawidłowość nie miała istotnego wpływu na wdrażanie wymogów *rozporządzenia w sprawie KRI*, dotyczących współpracy systemów informatycznych i ich dostosowania do wymiany danych z innymi systemami i podmiotami oraz nie spowodowała obniżenia oceny. Podstawę pozytywnej oceny stanowi w szczególności: [1] zapewnienie współpracy pomiędzy wybranymi do kontroli systemami informatycznymi w sposób zapewniający minimalne wymogi w zakresie interoperacyjności; [2] korzystanie z elektronicznego obiegu dokumentów wewnątrz Urzędu; [3] udostępnienie mieszkańcom 141 usług

[33] Dz. U. z 2014 r., poz. 1114.

elektronicznych; [4] wprowadzanie Elektronicznego Obiegu Dokumentów do jednostek Gminy Miejskiej Głogów.

2. Wdrożenie systemu zarządzania bezpieczeństwem systemów informatycznych

Opis stanu faktycznego

2.1. Urząd posiadał opracowaną i wdrożoną Politykę Bezpieczeństwa Informacji (dalej: PBI), ustanowioną i zatwierdzoną przez Prezydenta Miasta[34]. Dokument ten został przyjęty jako Polityka bezpieczeństwa przetwarzania danych osobowych, a od 11 czerwca 2014 r. ma także zastosowanie do innych systemów IT w celu zapewnienia ich poufności, dostępności i integralności informacji z uwzględnieniem takich atrybutów, jak: autentyczność, rozliczalność, niezaprzeczalność i niezawodność[35]. Zmiany do PBI proponują kierownicy komórek organizacyjnych Urzędu, ich wnioski podlegają przeanalizowaniu pod względem zasadności przez Administratora Bezpieczeństwa Informacji (dalej: ABI). Stosownie do § 20 ust. 1 *rozporządzenia w sprawie KRI*, w okresie objętym kontrolą, Urząd dokonał (trzykrotnie[36]) przeglądu PBI. W wyniku dokonanych przeglądów przeprowadzono dwukrotnie zmiany PBI.

(Dowód: akta kontroli str. 17-31; 231-258; 297; 311-381, 649-730)

2.2. Kontrola wykazała, że inwentaryzacja zasobów informatycznych w Urzędzie była realizowana przy wykorzystaniu aplikacji Symantec Management Console[37]. Kontrolerzy NIK przeprowadzili oględziny zapisów zawartych w ww. programie na podstawie 10 losowo wybranych komputerów oraz jednego urządzenia pełniącego rolę centralną[38]. Wyniki oględzin wykazały, że program Symantec Management Console zawierał szczegółowe informacje o dziewięciu komputerach i urządzeniu centralnym, w tym o ich konfiguracji.

(Dowód: akta kontroli str. 382-384)

W trakcie przeprowadzonych oględzin 15 komputerów Urzędu stwierdzono, że w przypadku 14 z nich nie było możliwości zainstalowania dowolnego oprogramowania przez użytkowników niebędących pracownikami służb informatycznych Urzędu.

(Dowód: akta kontroli str. 382-384)

2.3. Urząd w badanym okresie przeprowadził trzy analizy ryzyka bezpieczeństwa informacji[39], co było zgodne z § 20 ust. 2 pkt 3 *rozporządzenia w sprawie KRI*. W ich wyniku Urząd nie stwierdził utraty poufności, dostępności oraz integralności informacji.

(Dowód: akta kontroli str. 31-32; 74-105)

2.4. Kontrolerzy NIK dokonali przeglądu uprawnień do systemów i zasobów informatycznych dla 18 losowo wybranych pracowników Urzędu. Stwierdzono, iż wszyscy oni posiadali uprawnienia adekwatne do realizowanych zadań

---

[34] Zarządzenie Prezydenta Miasta Nr 197/2009 z dnia 8 września 2009 r. w sprawie w sprawie wprowadzenia do użytku służbowego polityki bezpieczeństwa i instrukcji zarządzania systemami informatycznymi w Urzędzie Miejskim w Głogowie (z późniejszymi zmianami).

[35] Zarządzenie Prezydenta Miasta Głogowa z dnia 11 czerwca 2014 r. w sprawie: Polityki Bezpieczeństwa Informacji w Urzędzie Miejskim w Głogowie.

[36] Dwukrotnie przeglądy kierowników komórek organizacyjnych/ABI – maj 2013 i maj 2014 oraz audyt 1/2014 dokonujący przeglądu PBI o którym mowa w pkt. 2.9 niniejszego Wystąpienia pokontrolnego.

[37] Za pomocą tej aplikacji w czasie rzeczywistym (online) zbierane są m.in. informacje na temat cech identyfikacyjnych komputera, logowań i pracujących na nim użytkowników, sieci w której działa komputer, dane na temat konfiguracji technicznej, tj. sprzętu (urządzeń) składowych, alertów wykorzystania pamięci, oprogramowania które jest na komputerze zainstalowane, licencji oraz aktualizacji oprogramowania.

[38] Serwer centralny na którym działały 4 aplikacje o charakterze bazodanowym.

[39] W 2013 r. przez Administratora Systemów Informatycznych (dalej: ASI) oraz w 2013 r. i 2014 r. przez Biuro Audytu.

określonych w zakresach obowiązków, lecz tylko pięciu z nich (28% próby) miało sporządzone formalne wnioski o nadanie uprawnień do systemów IT zgodnie z obowiązującą procedurą[40].

(Dowód: akta kontroli str. 591-621)

Nadawanie/modyfikowanie/odbieranie uprawnień w systemach informatycznych odbywało się w oparciu o funkcjonujące w Urzędzie procedury[41]. O uprawnieniach pracowników w systemach informatycznych decydują kierownicy komórek organizacyjnych we wniosku złożonym do ABI. Kontrolerzy dokonali sprawdzenia zablokowania dostępu do systemów informatycznych dla 10 byłych pracowników, którzy ostatnio zakończyli pracę w Urzędzie. Badaniem objęto dostęp do systemów „Intradoc", „Ratusz", „Użytkowanie wieczyste" i „Odpady komunalne". W tej grupie dla pięciu pracowników sporządzono niezbędne wnioski, a dostęp do kont dziewięciu osób nie budził zastrzeżeń[42].

(Dowód: akta kontroli str. 393-478, 622-646)

2.5. W Urzędzie, stosownie do § 20 ust. 2 pkt 6 *rozporządzenia w sprawie KRI* zapewniono szkolenia osób zaangażowanych w proces przetwarzania informacji. Zakres tematyczny szkolenia obejmował m.in. zagrożenia bezpieczeństwa informacji, skutki naruszenia bezpieczeństwa informacji oraz odpowiedzialność prawną[43]. Według wyjaśnień Sekretarza Gminy szkolenia takie były przeprowadzane przed majem 2012 r., a szkolenie z bezpieczeństwa informacji jest przewidziane w tym roku po okresie wakacyjnym. Ponadto w sieci wewnętrznej pracownicy mają dostęp do materiałów szkoleniowych i prezentacji w tym zakresie.

(Dowód: akta kontrolistr. 42, 44-61, 107, 297)

2.6. Zgodnie z obowiązującą PBI, laptopy wynoszone poza siedzibę Urzędu były zaszyfrowane i zabezpieczone hasłem, a ich użytkownicy mają podpisane umowy o indywidualnej odpowiedzialności za powierzone mienie.

(Dowód: akta kontroli str. 25-30; 34-42; 106-137; 229-230

2.7. Serwisowania komputerów Urzędu dokonują dostawcy w ramach gwarancji, a bieżącą konserwację i naprawy pozostałych urządzeń wykonują pracownicy Urzędu. W pojedynczych przypadkach zlecana jest naprawa urządzeń pogwarancyjnych do serwisu. Zgodnie z obowiązującą procedurą urządzenia lub elektroniczne nośniki informacji, przeznaczone do napraw w firmach zewnętrznych, pozbawia się w trwały sposób, przed ich naprawą, informacji na nich zawartych, albo naprawia się je pod nadzorem pracownika Urzędu[44].

(Dowód: akta kontroli str. 12, 34-42,138-166, 297)

W okresie po 31 maja 2012 r. Urząd zawarł 13 umów na dostawę lub serwisowanie urządzeń IT oraz na dostawę i serwisowanie wybranych czterech systemów IT[45]. Trzy z tych umów dotyczyły sprzętu IT nierodzącego ryzyka utraty poufności informacji; sześć umów na dostawę i serwis oprogramowania zawierało zapisy wprowadzające obowiązek zachowania przez dostawcę/serwisanta

---

[40] Instrukcja zarządzania systemami informatycznymi, służącymi do przetwarzania danych osobowych oraz postępowania w sytuacji naruszenia ochrony danych osobowych w Urzędzie Miejskim w Głogowie - Załącznik nr 2 do Zarządzenia nr 197/2009 Prezydenta Miasta Głogowa z dnia 8 września 2009 r.

[41] Instrukcja zarządzania systemami informatycznymi, służącymi do przetwarzania danych osobowych oraz postępowania w sytuacji naruszenia ochrony danych osobowych w Urzędzie Miejskim w Głogowie - Załącznik nr 2 do Zarządzenia nr 197/2009 Prezydenta Miasta Głogowa z dnia 8 września 2009 r.

[42] Konta były zablokowane lub konta były aktywne, gdy zwolnieni pracownicy ponownie zostali zatrudnieni i w momencie kontroli byli pracownikami Urzędu.

[43] W ramach szkolenia „Audyt wewnętrzny w zakresie bezpieczeństwa informacji w jsfp".

[44] Instrukcja zarządzania systemami informatycznymi, służącymi do przetwarzania danych osobowych oraz postępowania w sytuacji naruszenia ochrony danych osobowych w Urzędzie Miejskim w Głogowie - Załącznik nr 2 do Zarządzenia nr 197/2009 Prezydenta Miasta Głogowa z dnia 8 września 2009 r.

[45] IntraDoc; Odpady komunalne; Moduły systemu Ratusz; Użytkowanie wieczyste.

oprogramowania poufności informacji, a w czterech umowach na dostawy sprzętu komputerowego nie zawarto zapisów gwarantujących zachowanie poufności informacji przez dostawcę, zdobytych podczas serwisowania tych urządzeń IT. Według wyjaśnień udzielonych przez Sekretarza Gminy działania w przypadku naruszenia poufności informacji zostały opisane w procedurze[46] i polegały na powiadomieniu ABI, powołaniu przez niego doraźnego zespołu do zbadania naruszenia, a w przypadku stwierdzenia zaniedbania ze strony użytkownika zastosowania konsekwencji wynikających z właściwych przepisów prawa.

(Dowód: akta kontroli str. 12; 34-42;138-166; 297, 622-646)

2.8. W Urzędzie stosownie do § 20 ust. 2 pkt 13 *rozporządzenia w sprawie KRI*, wprowadzono procedurę nakazującą pracownikom niezwłoczne zgłaszanie incydentów naruszenia bezpieczeństwa informacji w sposób umożliwiający podjęcie działań korygujących[47]. Z procedurą tą zostali zapoznani pracownicy Urzędu. W badanej próbie 18 pracowników, w ich teczkach osobowych znajdowały się podpisane stosowne oświadczenia.

(Dowód: akta kontroli str. 34-42; 197-199)

2.9. W okresie objętym kontrolą Urząd przeprowadził jeden audyt (w 2014 r.)[48] obejmujący część Systemu Zarządzania Bezpieczeństwa Informacji. W jego wyniku sformułowano cztery rekomendacje[49], które według stanu na 12 sierpnia 2014 r. znajdują się w trakcie realizacji.

(Dowód: akta kontroli str. 231-281)

2.10. W Urzędzie wprowadzono procedurę tworzenia i przechowywania kopii bezpieczeństwa danych[50], w której określono zasady sporządzania i testowania kopii zapasowych danych oraz oprogramowania aplikacyjnego. Kopie zapasowe badanych systemów były tworzone raz dziennie (kopia przyrostowa) oraz raz w miesiącu (kopia całego zasobu) i zapisywane w określonych katalogach na dwóch serwerach. Testowanie prawidłowości sporządzania wykonanych kopii zapasowych następowało co najmniej raz na pół roku. Dodatkowo na bieżąco była weryfikowana prawidłowość tworzenia plików kopii zapasowych. Kopie zapasowe były przechowywane w siedzibie Urzędu w szafie pancernej poza miejscem ich wytworzenia. Stan taki spełniał wymogi określone w § 20 ust. 2 pkt 12 lit. b *rozporządzenia w sprawie KRI*, dzięki czemu minimalizowano ryzyko utraty informacji w wyniku awarii.

(Dowód: akta kontroli str. 8-11; 34-42; 167-188)

2.11. Badane systemy informatyczne udostępniały dane w następujących formatach:

- „Intradok" generuje pliki w formatach: pdf, xls, rtf, doc,
- „Odpady komunalne" generuje pliki w formatach: xls, doc, docx, odt,

---

[46] Rozdział 13 Instrukcji zarządzania systemami informatycznymi, służącymi do przetwarzania danych osobowych oraz postępowania w sytuacji naruszenia ochrony danych osobowych w Urzędzie Miejskim w Głogowie - Załącznik nr 2 do Zarządzenia nr 197/2009 Prezydenta Miasta Głogowa z dnia 8 września 2009 r.

[47] Rozdział 13 Instrukcji zarządzania systemami informatycznymi, służącymi do przetwarzania danych osobowych oraz postępowania w sytuacji naruszenia ochrony danych osobowych w Urzędzie Miejskim w Głogowie - Załącznik nr 2 do Zarządzenia nr 197/2009 Prezydenta Miasta Głogowa z dnia 8 września 2009 r.

[48] „Polityka bezpieczeństwa informacji" zrealizowany przez pracowników Biura Audytu UM Głogów w dniach 14.01 – 16.03.2014 r.

[49] 1. Wdrożenia kompleksowego dokumentu – Polityki Bezpieczeństwa Informacji; 2. Uzupełnienia istniejących przepisów o brakujące zapisy, tak aby kompleksowo wypełniały warunki opisane w przepisach prawa oraz stosownych normach; 3. Eliminacji uchybień związanych z brakiem realizacji wymagań bezpieczeństwa; 4. Zakup norm PN-ISO/IEC27001, 17799 oraz 27005.

[50] Rozdział 6 Instrukcji zarządzania systemami informatycznymi, służącymi do przetwarzania danych osobowych oraz postępowania w sytuacji naruszenia ochrony danych osobowych w Urzędzie Miejskim w Głogowie - Załącznik nr 2 do Zarządzenia nr 197/2009 Prezydenta Miasta Głogowa z dnia 8 września 2009 r. oraz „Procedura wykonywania kopii awaryjnej baz danych".

- „Użytkowanie wieczyste" generuje pliki w formatach: txt, xls,
- „Ratusz":
  - moduł „Posesja" generuje pliki w formatach: raf, txt, xls, wk1, wq1, htm, rtf, prn, pdf,
  - moduł „Pojazd" generuje pliki w formatach: txt, rtf, xls, htm, pdf, jpg,
  - moduł „Rejestr Opłat" generuje pliki w formatach: raf, txt, xls, wk1, wq1, htm, rtf, prn, pdf, csv,

tj. zgodnie z wymogami określonymi w § 18 ust. 1 *rozporządzenia w sprawie KRI.*

(Dowód: akta kontroli str. 189-196)

Ustalone nieprawidłowości

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

1. Obowiązująca w Urzędzie Polityka Bezpieczeństwa Informacji, wprowadzona zarządzeniem Prezydenta Miasta Nr 197/09 z dnia 8 września 2009 r., została opracowana na podstawie rozporządzenia Ministra Spraw Wewnętrznych i Administracji z dnia 29 kwietnia 2004 r. *w sprawie dokumentacji przetwarzania danych osobowych oraz warunków technicznych i organizacyjnych, jakim powinny odpowiadać urządzenia i systemy informatyczne służące do przetwarzania danych osobowych*[51]. Rozporządzenie to określa sposób prowadzenia i zakres dokumentacji opisującej sposób przetwarzania danych osobowych oraz środki techniczne i organizacyjne zapewniające ochronę przetwarzanych danych osobowych, odpowiednią do zagrożeń oraz kategorii danych objętych ochroną. Natomiast zgodnie z § 20 ust. 1 *rozporządzenia w sprawie KRI*, podmiot publiczny opracowuje i ustanawia system zarządzania bezpieczeństwem informacji (dalej: SZBI). W myśl § 20 ust. 3 ww. *rozporządzenia* wymagania w zakresie SZBI uznaje się za spełnione, jeżeli zostały opracowane na podstawie Polskiej Normy PN-ISO/IEC 27001. Wymogi powołanej normy oraz powiązanej z nią normy PN-ISO/IEC 17799 jasno wskazują, iż Polityka Bezpieczeństwa Informacji dotyczy wszystkich informacji jakie są przetwarzane w Urzędzie, a nie wyłącznie danych osobowych. Takie też stanowisko zajął Audytor wewnętrzny Urzędu w sprawozdaniu z zadania audytowego 1/2014 „Polityka Bezpieczeństwa Informacji" z 16 marca 2014 r., wskazując na szereg odstępstw i braków w obowiązującym dokumencie PBI w stosunku do wymagań normy PN-ISO/IEC 27001, oraz wydając zalecenie nr 1 w zakresie *„opracowania jednego kompleksowego dokumentu PBI zawierającego niezbędne, wymagane przepisami regulacje pozwalające na uznanie przedmiotowej polityki za zgodną z wymaganiami określonymi w obowiązujących aktach prawnych i normach*".
   Jak wyjaśnił Sekretarz Gminy uznano, że spośród 130 zidentyfikowanych wymagań przez audytorów wewnętrznych Urzędu tylko 21 pozostało niespełnionych, przy czym niezgodności te były według informatyków Urzędu w praktyce spełnione, więc PBI jest zgodne z normą PN-ISO/IEC 27001. Dodatkowo rozszerzono w czerwcu 2014 r. zakres stosowania PBI, tzn. nie tylko do danych osobowych, ale do wszystkich informacji przetwarzanych w UM w Głogowie. Według Sekretarza Gminy w bieżącym roku planowana jest również aktualizacja PBI, podczas której zostaną doprecyzowane niektóre rozdziały związane z bezpieczeństwem.
   W ocenie NIK wydanie Zarządzenia Prezydenta Miasta Nr 10/2014 z dnia 11 czerwca 2014 r. w sprawie Polityki Bezpieczeństwa Informacji w Urzędzie Miasta w Głogowie i oparcie się w niej na aktach wewnętrznych z 2009 r. nie zapewniło realizacji cytowanego powyżej zalecenia z audytu i zgodności PBI z normą PN-ISO/IEC 27001. Nie dokonano bowiem żadnych zmian w PBI,

[51] Dz. U. z 2004 r. Nr 100, poz. 1024.

rozszerzając tylko jej stosowanie na inne systemy informatyczne, nie obejmując zakresem wszystkich obszarów określonych w *rozporządzeniu w sprawie KRI*.

(Dowód: akta kontroli str. 17-31; 231-258; 297; 311-381, 622-646; 649-730)

2. W oprogramowaniu Symantec Management Console, inwentaryzującym strukturę informatyczną Urzędu, nie był ujęty jeden z 10 komputerów sprawdzanych przez kontrolerów NIK, a także dwa serwery oraz siedem stacji roboczych z systemem Windows 8.1. Było to niezgodne z przepisami § 20 ust. 2 pkt 2 *rozporządzenia w sprawie KRI*, w myśl którego Urząd jest zobowiązany do utrzymywania aktualności inwentaryzacji sprzętu i oprogramowania służącego do przetwarzania informacji, obejmującej ich rodzaj i konfigurację. Jak wyjaśnił główny specjalista Urzędu (pełniący funkcję informatyka oraz ASI) badany komputer nie był widoczny w oprogramowaniu ze względu na blokadę agenta oprogramowania przez firewall, a w trakcie kontroli dokonano jego odblokowania zapewniając widoczność tego komputera w oprogramowaniu. W pozostałych przypadkach powodem braku widoczności 11 urządzeń były problemy ze współpracą agenta oprogramowania inwentaryzującego z wersjami systemów operacyjnych tych urządzeń.

(Dowód: akta kontroli str. 382-384)

3. Na jednym spośród 15 skontrolowanych komputerów można było dokonać instalacji oprogramowania z poziomu użytkownika niebędącego pracownikiem służb informatycznych Urzędu. Miał on nadane prawa administracyjne do używanego przez siebie urządzenia. Było to niezgodne z przepisami § 20 ust. 2 pkt 4 *rozporządzenia w sprawie KRI*, w myśl którego Urząd jest zobowiązany do podejmowania działań zapewniających, że osoby zaangażowane w proces przetwarzania informacji posiadają stosowne uprawnienia i uczestniczą w tym procesie w stopniu adekwatnym do realizowanych przez nie zadań oraz obowiązków mających na celu zapewnienie bezpieczeństwa informacji. Według wyjaśnień głównego specjalisty Urzędu (pełniący funkcję informatyka oraz ASI) wynika to z faktu, że na komputerze tym było kiedyś zainstalowane oprogramowanie wymagające praw administracyjnych użytkownika i nie zostało to zmienione po zaprzestaniu jego używania. W trakcie kontroli pozbawiono tego użytkownika praw administracyjnych i możliwości samodzielnej instalacji oprogramowania.

(Dowód: akta kontroli str. 382-384)

4. Trzynastu z 18 sprawdzanych pracowników Urzędu nie posiadało w aktach osobowych formalnych wniosków o nadanie uprawnień do kontrolowanych systemów IT zgodnie z obowiązującą procedurą[52]. Było to niezgodne z przepisami § 20 ust. 2 pkt 4 *rozporządzenia w sprawie KRI*, w myśl którego Urząd jest zobowiązany do podejmowania działań zapewniających, że osoby zaangażowane w proces przetwarzania informacji posiadają stosowne uprawnienia i uczestniczą w tym procesie w stopniu adekwatnym do realizowanych przez nie zadań oraz obowiązków mających na celu zapewnienie bezpieczeństwa informacji. Sekretarz Gminy wyjaśnił, że kierownicy komórek organizacyjnych nie wystąpili o dostęp do systemu „Ratusz" i „Odpady komunalne" dla pięciu pracowników, a w przypadku pozostałych uznano, że upoważnienia do przetwarzania danych osobowych wydane przez Urząd przed 2010 r. były nadal aktualne. W ocenie NIK

[52] Instrukcja zarządzania systemami informatycznymi, służącymi do przetwarzania danych osobowych oraz postępowania w sytuacji naruszenia ochrony danych osobowych w Urzędzie Miejskim w Głogowie - Załącznik nr 2 do Zarządzenia nr 197/2009 Prezydenta Miasta Głogowa z dnia 8 września 2009 r.

powyższe wyjaśnienia nie zasługują na uwzględnienie, gdyż kontroli zostały poddane systemy zakupione i wdrożone przez Urząd po dniu 31 maja 2012 r.

(Dowód: akta kontroli str. 591-646)

5. Obowiązująca w Urzędzie procedura nadawania uprawnień do systemów informatycznych[53] nie obejmowała nadawania uprawnień do kont użytkowników sieciowych, dostępu do poczty elektronicznej, zasobów sieciowych[54] i uprawnień użytkownika do lokalnego systemu operacyjnego. Nie sporządzano wniosków o dostęp do tych zasobów. Zgodnie z załącznikiem A normy PN-ISO/IEC 27001:2007, punkt A.11.2.1, zarządzanie uprawnieniami powinno być realizowane w oparciu o formalną procedurę rejestrowania i wyrejestrowywania użytkowników. Jak wyjaśnił Sekretarz Gminy, kierownicy komórek występują z wnioskiem o dostęp do przetwarzania danych do odpowiedniego systemu. Na podstawie tego wniosku oczywiste jest, że należy założyć konto na stacji roboczej lub domenowe, a e-mail zakładany jest także automatycznie po telefonicznym uzgodnieniu z kierownikiem komórki.

(Dowód: akta kontroli str. 393-478, 622-646)

6. W badanej próbie 10 byłych pracowników Urzędu, z którymi w ostatnim okresie rozwiązano umowę o pracę, nie sporządzono pięciu wniosków o odebranie upoważnień do systemów informatycznych. W przypadku jednej osoby nie odebrano uprawnień - konto po ustaniu zatrudnienia nadal pozostawało aktywne. Wystąpił także jeden przypadek, kiedy już po ustaniu stosunku pracy na konto byłego pracownika dokonano logowania. Było to niezgodne z § 20 ust. 2 pkt 5 *rozporządzenia w sprawie KRI*, w myśl którego zarządzanie bezpieczeństwem informacji jest realizowane w szczególności przez bezzwłoczną zmianę uprawnień w przypadku zmiany zadań pracowników. Sekretarz Gminy wyjaśnił, że dla dwóch pracowników nie sporządzono wniosków, ponieważ zostali oni na nowo zatrudnieni, a dla trzech kolejnych kierownicy komórek przeoczyli ten obowiązek. Stwierdzone aktywne konto nie było zablokowane, ponieważ kierownik zapomniał sporządzić wniosek o zamknięcie konta zmarłego pracownika, zostało ono zablokowane w czasie kontroli. Natomiast logowania na konto zwolnionego pracownika dokonał Administrator Systemu by nadać uprawnienia do sprawy niezałatwionej przez zwolnionego pracownika innemu pracownikowi Urzędu. W ocenie NIK w momencie rozliczania zwalnianego pracownika należało dopilnować rozliczenia wszystkich realizowanych zadań i spraw, a w przypadku dwóch pracowników, którzy zostali przyjęci ponownie do pracy, okres od ustania zatrudnienia do ponownego ich zatrudnienia wyniósł odpowiednio 16 dni i 3,5 miesiąca, zatem zasadnym było sporządzenie wniosków o pozbawienie uprawnień.

(Dowód: akta kontroli str. 393-478, 622-646)

7. W Urzędzie nie opracowano procedur gwarantujących bezpieczną pracę przy przetwarzaniu mobilnym i pracy na odległość, określających m.in. zasady pracy i minimalizacji ryzyka kradzieży urządzenia oraz danych poza siedzibą jednostki, a także zasady korzystania z ogólnodostępnych sieci bezprzewodowych, zasady aktualizacji programowania urządzeń przenośnych. Było to niezgodne z § 20 ust. 2 pkt 8 i 11 *rozporządzenia w sprawie KRI*,

---

[53] Instrukcja zarządzania systemami informatycznymi, służącymi do przetwarzania danych osobowych oraz postępowania w sytuacji naruszenia ochrony danych osobowych w Urzędzie Miejskim w Głogowie - Załącznik nr 2 do Zarządzenia nr 197/2009 Prezydenta Miasta Głogowa z dnia 8 września 2009 r.

[54] Zasoby istniejące na innym komputerze w sieci. Przykładem tego typu zasobów są dyski twarde serwera, drukarki sieciowe, a także wszystkie urządzenia, z których można korzystać w internecie - np. dysk twardy serwera FTP.

w myśl którego Urząd miał obowiązek ustanowienia podstawowych zasad gwarantujących bezpieczną pracę przy przetwarzaniu mobilnym i pracy na odległość oraz ustalenia zasad postępowania z informacjami, zapewniających minimalizację wystąpienia ryzyka kradzieży informacji i środków przetwarzania informacji, w tym urządzeń mobilnych. Zaistnienia stwierdzonej nieprawidłowości nie uzasadniają, w ocenie NIK, argumenty przedstawione przez Sekretarza Gminy, iż dotychczasowe regulacje są wystarczające, a połączenia przy pracy na odległość są szyfrowane.

(Dowód: akta kontroli str. 25-30; 34-42; 106-137; 229-230, 622-646)

8. W przypadku czterech z 13 umów[55] (31% próby) na dostawy sprzętu komputerowego nie zawarto zapisów gwarantujących zachowanie poufności informacji przez dostawcę, zdobytych podczas serwisowania gwarancyjnego urządzeń IT. Było to niezgodne z § 20 ust. 2 pkt 10 *rozporządzenia w sprawie KRI*, w myśl którego Urząd jest zobowiązany do zawierania w umowach serwisowych podpisanych ze stronami trzecimi zapisów gwarantujących odpowiedni poziom bezpieczeństwa informacji. Według wyjaśnień Prezydenta Miasta kwestia ta jest uregulowana w PBI, a *„dodatkowe klauzule w umowach powodują wzrost ceny zakupu sprzętu"*. NIK nie zgadza się z taką argumentacją, ponieważ klauzule takie są powszechne w obrocie gospodarczym i nie powodują dodatkowych kosztów, a zapisy PBI nie gwarantują odpowiedniego zabezpieczenia bezpieczeństwa informacji w relacjach z dostawcą.

(Dowód: akta kontroli str. 12; 34-42; 138-166; 297)

9. W roku 2013 nie przeprowadzono w Urzędzie audytu wewnętrznego z zakresu bezpieczeństwa informacyjnego, mimo że zgodnie z zapisami § 20 ust. 2 pkt 14 *rozporządzenia w sprawie KRI* okresowe audyty wewnętrzne w zakresie bezpieczeństwa informacji należało przeprowadzać nie rzadziej niż raz na rok. Stwierdzonej nieprawidłowości nie tłumaczą argumenty Kierownika Biura Audytu, iż wynika to z ograniczonych zasobów komórki audytu, monitorowania tego obszaru w ramach innych procesów oraz wykonywania zadań audytowych o podobnej tematyce w poprzednich latach.

(Dowód: akta kontroli str. 231-281)

Ocena cząstkowa

Najwyższa Izba Kontroli ocenia negatywnie działalność Urzędu w obszarze wdrożenia systemu zarządzania bezpieczeństwem systemów informatycznych. Na negatywną ocenę wpływ miały skala, waga i charakter stwierdzonych w wyniku kontroli nieprawidłowości polegających na: [1] braku Polityki Bezpieczeństwa Informacyjnego, spełniającej wymogi *rozporządzenia w sprawie KRI*; [2] nieobjęciu niektórych systemów i zasobów IT procedurą nadawania uprawnień w Urzędzie; [3] braku sporządzenia wniosków o nadanie/cofnięcie uprawnień w kontrolowanych systemach dla ok. 50% badanej próby pracowników; [4] braku procedur gwarantujących bezpieczną pracę przy przetwarzaniu mobilnym i pracy na odległość; [5] braku realizacji audytów o których mowa w *rozporządzeniu w sprawie KRI*.

3. Zapewnienie dostępności informacji dla osób niepełnosprawnych

Opis stanu faktycznego

W toku kontroli przeprowadzono weryfikację stron internetowych Urzędu pod kątem ustalenia czy spełniają one wymagania dotyczące prezentacji zasobów zgodnie ze

[55] 1) 91/WAG/162/2014 z 31 stycznia 2014 r. – brak jakichkolwiek zapisów, 2) UM/240/WAG/578/13 z 26.04.2013 r., 3) 680/WAG/1742/2012 z 3 grudnia 2012 r., 4) 521/WAG/1248/2012 z 03.09.2012 r. – brak zagwarantowania poufności przy naprawach gwarancyjnych dokonywanych w Urzędzie.

standardem WCAG 2.0. w zakresie Zasady 4 – Kompatybilność, służącym dostosowaniu wyświetlanej treści na stronie internetowej do potrzeb osób niedowidzących[56].
W wyniku walidacji narzędziem http://validator.w3.org/ ustalono, że strona: http://glogow.bip.info.pl/ zawierała 43 błędy, natomiast strona www.glogow.pl. zawierała 155 błędów. Błędy pogrupowane były w sześć kategorii. Natomiast badanie za pomocą narzędzia http://jigsaw.w3.org/css-validator/ ujawniło cztery błędy i pięć ostrzeżeń na stronie http://glogow.bip.info.pl/ oraz 17 błędów i 20 ostrzeżeń na stronie www.glogow.pl.

(Dowód: akta kontroli str. 202-228)

IV. Wnioski

Wnioski pokontrolne

Przedstawiając powyższe oceny i uwagi wynikające z ustaleń kontroli, Najwyższa Izba Kontroli, na podstawie art. 53 ust. 1 pkt 5 ustawy z dnia 23 grudnia 1994 r. o Najwyższej Izbie Kontroli[57], wnosi o:

1. Umieszczenie wzorów obowiązujących dokumentów elektronicznych w centralnym repozytorium ePUAP dostępnym pod adresem www.crd.gov.pl.
2. Rozważenie wdrożenia automatycznego zasilania modułów aplikacji „Ratusz", tj. „Firmy", „Posesja" oraz „Pojazd", danymi za pośrednictwem formularzy elektronicznych udostępnionych na platformie www.glogow.pl i/lub ePUAP.
3. Opracowanie i wdrożenie Polityki Bezpieczeństwa Informacji, określającej zasady bezpieczeństwa informacji zgodnej z normą PN-ISO/IEC 27001 oraz wykonywanie corocznych audytów w tym zakresie.
4. Objęcie oprogramowaniem inwentaryzującym wszystkich podłączonych do sieci Urzędu komputerów i urządzeń centralnych.
5. Objęcie procedurą nadawania/modyfikowania/odbierania uprawnień do systemów informatycznych kont użytkowników sieciowych, dostępu do poczty elektronicznej, zasobów sieciowych i uprawnień użytkownika do lokalnego systemu operacyjnego.
6. Opracowanie i wdrożenie procedur gwarantujących bezpieczną pracę przy przetwarzaniu mobilnym i pracy na odległość, określających m.in. zasady pracy i minimalizacji ryzyka kradzieży urządzenia oraz danych poza siedzibą jednostki, a także zasady korzystania z ogólnodostępnych sieci bezprzewodowych i zasady aktualizacji programowania urządzeń przenośnych.
7. Przeprowadzanie co najmniej raz w roku audytu wewnętrznego w zakresie bezpieczeństwa informacji w formie zadania zapewniającego.

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 we Wrocławiu.

---

[56] Weryfikację przeprowadzono z wykorzystaniem narzędzi dostępnych na stronie internetowej http://validator.w3.org/ oraz http://jigsaw.w3.org/css-validator/.
[57] Dz. U. z 2012 r., poz. 82 ze zm.

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.

Wrocław, dnia 30 września 2014 r.

Najwyższa Izba Kontroli
Delegatura we Wrocławiu

Kontroler:
Małgorzata Grudowska
Starszy inspektor k.p.

Podpis

Dyrektor

DYREKTOR
Delegatura Najwyższej Izby Kontroli
we Wrocławiu
z up.
Zbigniew Torkowski
Wicedyrektor