



NAJWYŻSZA IZBA KONTROLI

Delegatura we Wrocławiu

LWR-4101-013-01/2014

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.
Jednostka przeprowadzająca kontrolę	Najwyższa Izba Kontroli Delegatura we Wrocławiu
Kontroler	Waldemar Zimoch, starszy inspektor kontroli państwowej, upoważnienie do kontroli nr 89788 z dnia 12 czerwca 2014 r. <i>(dowód: akta kontroli str. 1-2)</i>
Jednostka kontrolowana	Urząd Miasta Legnicy, Plac Słowiański 8, 59-220 Legnica (dalej: Urząd)
Kierownik jednostki kontrolowanej	Tadeusz Krzakowski – Prezydent Miasta Legnicy <i>(dowód: akta kontroli str. 3-4)</i>

II. Ocena kontrolowanej działalności

Ocena ogólna

Najwyższa Izba Kontroli ocenia pozytywnie¹ działania Prezydenta Miasta Legnicy w zakresie wdrożenia minimalnych wymagań nałożonych na systemy informatyczne przez rozporządzenie Rady Ministrów z dnia 12 kwietnia 2012 r. *w sprawie Krajowych Ram Interoperacyjności oraz minimalnych wymagań dla rejestrów publicznych i wymiany informacji w postaci elektronicznej oraz minimalnych wymagań dla systemów teleinformatycznych*² (dalej: *rozporządzenie KRI*) w okresie od 31 maja 2012 r. do 8 sierpnia 2014 r.

Uzasadnienie
oceny ogólnej

Powyższą ocenę ogólną uzasadniają ustalenia kontroli dotyczące przede wszystkim:

- ✓ zapewnienia współpracy pomiędzy systemami informatycznymi w sposób spełniający minimalne wymogi w zakresie interoperacyjności, w szczególności poprzez wzajemną komunikację oraz udostępnianie danych w formatach określonych w *rozporządzeniu KRI*;
- ✓ wdrożenia i udostępnienia przez narzędzia i systemy informatyczne klientom Urzędu usług elektronicznych³;
- ✓ rzetelnego opracowania, wdrożenia i zarządzania polityką bezpieczeństwa informacji w Urzędzie;
- ✓ prowadzenia i bieżącej aktualizacji ewidencji sprzętu komputerowego, zawierającej informacje o jego rodzaju i konfiguracji umożliwiającej odtworzenie po ewentualnej katastrofie lub zdarzeniu losowym;
- ✓ wcześniejszego przygotowania stron internetowych Urzędu do zapewnienia dostępności informacji dla osób niedowidzących, zgodnie z wymaganiami WCAG 2.0, wynikającymi z § 19 *rozporządzenia KRI*⁴,

¹ Najwyższa Izba Kontroli stosuje 3-stopniową skalę ocen: pozytywna, pozytywna mimo stwierdzonych nieprawidłowości, negatywna.

² Dz. U. z 2012 r., poz. 526.

³ Usługą elektroniczną, w myśl art. 2 pkt 4 ustawy z dnia 18 lipca 2002 r. o świadczeniu usług drogą elektroniczną (Dz. U. z 2013 r., poz. 1422), jest usługa świadczona bez jednoczesnej obecności stron (na odległość), poprzez przekaz danych na indywidualne żądanie usługobiorcy, przesyłanej i otrzymywanej za pomocą urządzeń do elektronicznego przetwarzania.

⁴ Zgodnie z rozporządzeniem KRI, ostateczny termin wprowadzenia tych wymagań to 1 czerwca 2015 r.

- ✓ zapewnienia skutecznego i efektywnego planowania, realizacji i nadzorowania procesów usług elektronicznych obowiązujących w Urzędzie.

III. Opis ustalonego stanu faktycznego

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

Opis stanu faktycznego

W Strategii Rozwoju Miasta Legnica na lata 2004-2014 uwzględniono zadania dotyczące dostosowania Urzędu do elektronicznego świadczenia usług publicznych. Polegały one na: [1] utworzeniu Systemu Informacji Przestrzennej Obszarów Inwestycyjnych (termin realizacji – lata 2005-2006); [2] przystąpieniu gminy do projektu informatycznego „Rozbudowa Zintegrowanego Systemu Informatycznego dla Zrównoważonego Rozwoju Regionu Dolnego Śląska” (termin – lata 2008-2014); [3] zakupie i wdrożeniu systemu wspomaganego Zarządzania Miastem, w tym integracji rozwiązań z zakresu mapy numerycznej z pozostałymi bazami danych i rejestrami Urzędu oraz rozbudowy infrastruktury teleinformatycznej w celu upowszechnienia elektronicznego dostępu do Urzędu (termin – lata 2004-2012); [4] budowie miejskiej szerokopasmowej i bezpiecznej sieci teleinformatycznej LEGMAN w Legnicy (termin – lata 2008-2013); [5] współpracy z dostawcami mediów celem zapewnienia dostępu do komunikacji telefonicznej i internetowej (termin – lata 2004-2014).

Urząd zrealizował większość zaplanowanych zadań, a do najważniejszych należało: [1] wdrożenie produkcyjne Elektronicznego Systemu Obiegu Dokumentów (ESOD) – system przetwarzający elektronicznie dokumenty; [2] zakup i wdrożenie Zintegrowanego Systemu Wspomagającego Zarządzanie Miastem – Ksat2000i – system klasy ERP⁵, realizujący funkcjonalności m.in. z obszaru: ewidencji, naliczania podatków i zobowiązań, szeroko rozumianej obsługi Urzędu; [3] zakup, wdrożenie i serwis systemu do Gospodarowania Odpadami GOP; [4] zakup i wdrożenie systemu eDIOM, wspomagającego ewidencjonowanie i zarządzanie drogami i elementami organizacji ruchu drogowego; [5] uruchomienie, w ramach szerokopasmowej i bezpiecznej sieci LEGMAR, „hot-spotów” świadczących bezpłatny dostęp do Internetu. Połączono wszystkie lokalizacje Urzędu korzystające z zasobów informatycznych, tj. biblioteki, Zarządu Gospodarki Mieszkaniowej, Zarządu Dróg Miejskich, spółdzielni mieszkaniowych, Państwowej Straży Pożarnej.

Ponadto w Urzędzie w dniu 20 lipca 2009 r. wdrożono Zintegrowany System Zarządzania (dalej: ZSZ), oparty na wymaganiach normy PN-EN ISO 9001:2009 oraz normy PN-ISO/IEC 27001:2007, w skład którego wchodziły: polityka bezpieczeństwa informacji i polityka ciągłości działania.

(dowód: akta kontroli str. 8-62)

Promowanie komunikacji elektronicznej pomiędzy mieszkańcem a Urzędem odbywało się wieloetapowo⁶. Kampania na temat usług z obszaru IT⁷, w tym świadczonych przez Internet usług elektronicznych, odbywała się za pomocą: ulotek, billboardów, czy radia, a także kanałami dystrybucji internetowej jak: strony internetowej Urzędu, profile Urzędu na portalach społecznościowych. Promowano

⁵ Planowanie zasobów przedsiębiorstwa (ang. *enterprise resource planning - ERP*).

⁶ I etap - grudzień 2010 r., a II etap - marzec 2014 r.

⁷ Techniki informatyczne (ang.: *information technology*).

np. uruchomienie usługi – rezerwacja terminu ślubu, uruchomienie portalu GIS⁸ (sip.legnica.eu), sprawdzenie adresu siedziby lokalu wyborczego (usługa aktywowana na czas wyborów), udostępnienie bezpłatnego dostępu do Internetu poprzez sieć „hot-spotów”, czy też usług świadczonych za pomocą ePUAP.

(dowód: akta kontroli str. 63-86)

W przeprowadzonych przez Urząd badaniach ankietowych, kierowanych do mieszkańców Legnicy w ramach ZSZ, nie zadano wprost pytań dotyczących chęci, potrzeby korzystania z usług Urzędu przy użyciu środków elektronicznych. Respondenci mieli możliwość wyrazić w tej kwestii swoją opinię odpowiadając na ogólnie sformułowane pytania otwarte, np.: „Czego oczekuje Pan/Pani od Urzędu?”. Ostatnie badania przeprowadzono na przełomie lutego i marca tego 2014 r. Łącznie pozyskano i poddano analizie 912 ankiet. Zawierały one trzy adnotacje, uwagi dotyczące pośrednio lub bezpośrednio usług świadczonych drogą elektroniczną, np. „Więszczego dostępu elektronicznego do wypełnionych dokumentów – możliwości załatwiania spraw elektronicznie”.

(dowód: akta kontroli str. 87-93)

Po wejściu w życie rozporządzenia KRI nie zwracano się do Ministra Administracji i Cyfryzacji z problemami, bądź z prośbą o pomoc w zakresie dostosowania swoich systemów/rejestrów informatycznych do wymogów KRI.

(dowód: akta kontroli str. 94)

Zarządzeniem nr 70/UM/2011 z dnia 30 grudnia 2011 r. Prezydent Miasta Legnicy wprowadził system ESOD służący do przetwarzania dokumentów i spraw w formie elektronicznej. Zobowiązał on użytkowników tego systemu do rejestracji i przetwarzania w formie elektronicznej dokumentów i spraw wskazanych w wykazie stanowiącym załącznik do zarządzenia⁹. Poszczególne etapy procesów elektronicznego obiegu dokumentów w Urzędzie zawierały: wpływ dokumentu, rejestrację, dekretację, rozpatrywanie, akceptację odpowiedzi, wysłanie dokumentu do odbiorcy. W ramach tego samego zarządzenia Prezydent Miasta Legnicy podtrzymał obowiązywanie papierowego obiegu dokumentów. W Regulaminie Organizacyjnym Urzędu nie było zapisów dotyczących przepływu dokumentów drogą elektroniczną.

(dowód: akta kontroli str. 95-111)

W okresie od 31 maja 2012 r. do 31 maja 2014 r. korespondencja Urzędu z osobami fizycznymi, podmiotami gospodarczymi oraz innymi urzędami obejmowała łącznie 360 745 dokumentów, z czego 126 749 wpłynęło do Urzędu, a 233 996 zostało wysłanych przez Urząd. Przeważająca część tej korespondencji, bo 359 110 dokumentów (99,55%) została dostarczona w formie papierowej, a tylko 1 635 dokumentów (0,45%) drogą elektroniczną. Największy udział w korespondencji elektronicznej stanowiły wnioski o udostępnienie informacji publicznej - 362 dokumenty (22,1%), z czego 180 wpłynęło do Urzędu, a 182 zostało przez Urząd wysłanych.

(dowód: akta kontroli str. 112)

Usługi świadczone przez Urząd drogą elektroniczną były realizowane w dwóch obszarach: [a] usługi świadczone w ramach e-PUAP (13 usług); [b] usługi ułatwiające dostęp do Urzędu (pięć usług np.: internetowa rezerwacja terminu ślubu, system komunikacji niewerbalnej – umawianie wizyty z tłumaczem, umawianie wizyty w biurze obsługi klienta).

⁸ System Informacji Przestrzennej (ang. Geographic Information System).

⁹ Np. wypis czy wyrys z miejscowego planu..., wniosek o ustalenie warunków zabudowy, wszystkie dokumenty przychodzące z Biura Geodety Miejskiego, wniosek o wydanie decyzji dot. gospodarki odpadami (wszystkie rodzaje).

Na dzień 16 czerwca 2014 r. Urząd świadczył drogą elektroniczną 18 usług. Przed wejściem w życie *rozporządzenia KRI*, tj. przed 30 maja 2012 r., Urząd świadczył drogą elektroniczną pięć usług. Dynamika przyrostu liczby świadczonych usług elektronicznych w badanym okresie wyniosła ponad 250%.

Urząd nie przekazywał wzorów dokumentów elektronicznych do centralnego repozytorium na ePUAP, prowadzonego przez Ministerstwo Administracji i Cyfryzacji. Na potrzeby realizacji e-usług Urząd zaadoptował istniejące formularze, dostępne na stronie ww. Ministerstwa.

Analiza kontrolna pięciu wybranych usług elektronicznych świadczonych przez Urząd, tj.: [1] wniosku o udzielenie 50% bonifikaty od opłaty rocznej z tytułu użytkowania wieczystego nieruchomości gruntowej, [2] wniosku o przeprowadzenie egzaminu w zakresie transportu drogowego taksówką, [3] wniosku o wydanie wypisu z Miejscowego Planu Zagospodarowania Przestrzennego (dalej: MPZP) lub ze Studium Uwarunkowań i Kierunków Zagospodarowania Przestrzennego (dalej: SUIKZP), [4] wniosku o wydanie wrysu z MPZP lub ze SUIKZP, [5] wniosku o wydanie zezwolenia na usunięcie drzewa - wykazała, iż:

- zamieszczone na stronach internetowych Urzędu i ePUAP opisy ww. usług elektronicznych świadczonych przez Urząd były zgodne ze świadczoną usługą,
- na stronie internetowej Biuletynu Informacji Publicznej Urzędu zamieszczono informacje odnośnie obowiązujących procedur w zakresie załatwiania spraw drogą elektroniczną,
- wszystkie opisy wybranych usług zawierały: dane dotyczące podmiotu, miejsca świadczenia usługi, aktualną podstawę prawną, sposób realizacji usługi.

Powyższe ustalenia wskazują na rzetelne działania Urzędu w zakresie zgodności opisów objętych badaniem usług z faktycznie świadczonymi. Należy podkreślić, iż w procesie zarządzania usługami elektronicznym, Urząd wspierał model usługowy, zgodnie z definicją zawartą w § 2 pkt 8 *rozporządzenia KRI*¹⁰.

(dowód: akta kontroli str. 113-143)

W okresie objętym kontrolą Urząd zakupił lub zmodernizował 12 systemów, programów komputerowych. Kontrolą objęte zostały cztery funkcjonujące w Urzędzie systemy IT:

- GOP – Gospodarka odpadami komunalnymi (program do obsługi deklaracji i należności). System bazodanowy – online. Wymiana informacji z innymi modułami lub programami odbywała się automatycznie – system jest transakcyjny¹¹. Program korzysta z danych osobowych i adresowych z programu KSAT2000i. Kontrola powierzchni opodatkowanej dla danej nieruchomości odbywa się poprzez integrację z modułem Podatki-POD. Ponadto system generuje dokumenty księgowe, które przekazuje do oprogramowania NZ – Należności i Zobowiązania (moduł oprogramowania księgowego);
- eDIOM – system do prowadzenia ewidencji dróg i obiektów mostowych wraz z modułem projektowania i zatwierdzania organizacji ruchu. System korzystał z zewnętrznych źródeł danych przestrzennych, które stanowiły dla niego warstwy podkładowe. System eDiom wykorzystuje dane „EGBiL” (z ewidencji gruntów budynków i lokali), które pobierane były w trybie wsadowym z częstotliwością – raz dziennie. System jest otwarty w kontekście możliwości wymiany danych oraz

¹⁰ Model usługowy jest modelem architektury systemu informatycznego, w którym dla użytkowników zdefiniowano stanowiące odrębną całość funkcje systemu teleinformatycznego (usługi sieciowe) oraz opisano sposób korzystania z tych funkcji.

¹¹ Transakcyjny – wymiana danych pomiędzy systemami odbywa się bez jakiegokolwiek pośrednictwa pracownika, przekaz danych automatyczny.

współpracy z innymi systemami z obszaru GIS. Do wymiany danych wykorzystuje takie formaty tekstowe jak „wms”, czy spopularyzowany wśród aplikacji GIS format „shp”. System posiada klasę dwustronnej komunikacji¹²;

- PB_USC – aplikacja dziedzinowa z zakresu informatycznej obsługi Urzędu Stanu Cywilnego. Tworzy lokalną bazę danych aktów stanu cywilnego. Współpracuje ściśle z aplikacją internetową – usługą – „*Terminarz ślubów*”, posiada mechanizm eksportów danych do innych systemów. Współpracuje automatycznie z aplikacją KSAT2000i-EWD – ewidencja ludności. Współpraca polega na zaimplementowaniu funkcji przenoszenia danych między dwiema bazami – system transakcyjny;
- BIP – Biuletyn Informacji Publicznej – wykorzystywany w Urzędzie oraz w 63 jednostkach organizacyjnych Gminy Miejskiej Legnica – narzędzie do udostępniania informacji publicznej. Spełnia wymogi Krajowych Ram Interoperacyjności, m.in.: wprowadzono nawigację za pomocą klawiatury, zadbano o poprawność kodu HTML¹³, wprowadzono mechanizm zwiększania rozmiaru czcionki, wprowadzono przycisk zwiększenia kontrastu. W BIP używane były wyłącznie formaty plików wyszczególnione w zał. nr 2 do *rozporządzenia KRI*. System zastąpił wcześniejsze oprogramowanie, które nie spełniało warunków *rozporządzenia KRI* i przysparzało Urzędowi problemów technicznych.

W ocenie NIK zbadane systemy spełniały minimalne wymogi interoperacyjności w zakresie współpracy z innymi systemami, funkcjonującymi w kontrolowanej jednostce, o których mowa w § 5 ust. 3 pkt 3 *rozporządzenia KRI*.

(dowód: akta kontroli str. 144-162)

Współpraca „bez papieru” z innymi jednostkami administracji publicznej odbywała się na zasadzie przekazywania korespondencji w postaci elektronicznej poprzez ESP¹⁴ na platformie ePUAP. Dotyczyło to korespondencji z urzędami skarbowymi¹⁵. Poprzez platformę ePUAP przekazywano również korespondencję do Dolnośląskiego Urzędu Wojewódzkiego i Krajowego Biura Wyborczego Delegatury w Legnicy, zgodnie z art. 39 ustawy z dnia 14 czerwca 1960 r. *Kodeks postępowania administracyjnego*¹⁶. Ponadto Ministerstwo Spraw Wewnętrznych zaproponowało Urzędowi wykorzystywanie Portalu Informacyjnego Administracji (PIA) do przesyłania pomiędzy urzędami gmin zawiadomień meldunkowych. W trakcie kontroli współpraca między gminami odbywała się wyłącznie przez portal PIA.

(dowód: akta kontroli str. 163-168)

Ustalone
nieprawidłowości

W działalności Urzędu w zakresie dostosowania posiadanych systemów teleinformatycznych do współpracy z systemami/rejestrami używanymi wewnątrz Urzędu oraz przez inne podmioty administracji publicznej, nie stwierdzono nieprawidłowości.

Najwyższa Izba Kontroli pozytywnie ocenia działalność kontrolowanej jednostki w zakresie dostosowania posiadanych systemów teleinformatycznych do

Ocena cząstkowa

¹² Dwustronna komunikacja – dane z systemu A przekazywane są do systemu B poprzez akceptację pracownika.

¹³ Hipertekstowy język znaczników, obecnie szeroko wykorzystywany do tworzenia stron internetowych (ang. *HyperText Markup Language*).

¹⁴ Elektroniczna Skrzynka Podawcza (ESP) to dostępny publicznie środek komunikacji elektronicznej służący do przekazywania informacji w formie elektronicznej do podmiotu publicznego przy wykorzystaniu powszechnie dostępnej sieci teleinformatycznej.

¹⁵ W Wodzisławiu Śląskim, Złotoryi, Górze, Głogowie, Kujawsko Pomorski Urząd Skarbowy w Bydgoszczy oraz Dolnośląski Urząd Skarbowy we Wrocławiu.

¹⁶ Dz. U z 2013 r., poz. 267 ze zm.

współpracy z systemami, rejestrami używanymi wewnątrz Urzędu oraz przez inne podmioty administracji publicznej.

2. Wdrożenie systemu zarządzania bezpieczeństwem systemów informatycznych

Opis stanu faktycznego

Od dnia 21 października 2009 r. Urząd posiada i stosuje System Zarządzania Bezpieczeństwem Informacji, zgodny z normą PN-ISO/IEC 27001:2007, w którym opisano cele zastosowania zabezpieczeń oraz zabezpieczenia. Osobą odpowiedzialną za wszelkie zmiany procedur, związanych z bezpieczeństwem informacji, jest Pełnomocnik ds. ZSZ. W okresie objętym kontrolą Polityka Bezpieczeństwa Informacji dwukrotnie poddawana była przeglądowi przez audytorów zewnętrznych. Wszelkie uwagi adresowane do Urzędu przez osoby weryfikujące były uwzględniane, co odnotowywano w protokołach z audytu.

(dowód: akta kontroli str. 169-272)

Kontrola 10 szt. komputerów, jednego wybranego serwera i kont użytkowników funkcjonujących na tych urządzeniach wykazała, iż: wszystkie komputery wraz z serwerem posiadały tabliczki znamionowe i były odnotowane w ewidencji środków trwałych. Infrastruktura IT i monitoring pracy komputerów odbywał się za pomocą specjalistycznego narzędzia informatycznego „Statlook” poprzez wykorzystanie m.in. następującej funkcjonalności: [1] inwentaryzacja sprzętu komputerowego; [2] audyt oprogramowania; [3] monitoring zmian oprogramowania; [4] analiza aktywności użytkownika; [5] blokowanie niepożądanych aplikacji. Najwyższa Izba Kontroli stwierdza, iż Urząd dysponuje aktualnymi informacjami w zakresie posiadanego sprzętu informatycznego oraz jego konfiguracji.

Na 33 poddanych kontroli komputerach (w tym 23 komputerach przekazanych przez Ministerstwo Spraw Wewnętrznych w ramach projektu „pl.ID – Polska ID karta”), żaden z użytkowników nie posiadał praw administratora.

(dowód: akta kontroli str. 273-295)

W Urzędzie została wdrożona i była stosowana Polityka Ciągłości Działania. Zapewnia ona ciągłość kluczowych procesów działalności usługowej, minimalizuje straty ponoszone w wyniku zaistnienia sytuacji kryzysowych. W toku kontroli stwierdzono, iż Urząd przeprowadzał okresowe analizy ryzyka utraty integralności, dostępności lub poufności informacji, co było zgodne z § 20 ust. 2 pkt 3 *rozporządzenia KRI*. W raportach z audytów w okresie objętym kontrolą nie stwierdzono zagrożeń utraty integralności, poufności lub dostępności informacji.

(dowód: akta kontroli str. 296-316)

W wyniku kontroli losowo wybranych 15 pracowników Urzędu, wykonujących zadania na systemach informatycznych (zgodne z realizowanymi czynnościami zapisanymi w zakresach obowiązków) – ustalono, iż pracownicy ci posiadali stosowne uprawnienia dla zapewnienia bezpieczeństwa informacji, stosownie do przepisów § 20 ust. 2 pkt 4 i 5 *rozporządzenia KRI*. W trakcie kontroli dokonano sprawdzenia zablokowania dostępu do systemów IT Urzędu dla 10 pracowników, którzy zakończyli pracę w Urzędzie w badanym okresie. Zgodnie z wypełnionymi przez przełożonych kartami Z1/PB-4/I-12 (*wniosek o nadanie, zmianę i cofnięcie uprawnień do systemów i urządzeń*), konta w systemach informatycznych byłych pracowników były blokowane lub usuwane.

(dowód: akta kontroli str. 317-358)

W badanym okresie, stosownie do § 20 ust. 2 pkt 6 *rozporządzenia KRI*, przeprowadzono cztery szkolenia, adresowane do wszystkich pracowników zaangażowanych w proces przetwarzania informacji. Szkolenia te miały charakter

usystematyzowany, odbywały się według ściśle określonych harmonogramów w danym roku kalendarzowym. Szkolenia uwzględniały takie zagadnienia jak:

- Zintegrowany System Zarządzania (w 2012 r. przeszkolono 157 pracowników, w 2013 r. przeszkolono 164 pracowników) – jednym z podejmowanych tematów był system ochrony informacji i ochrony danych osobowych;
- ochronę danych osobowych i udostępnianie informacji publicznej w praktyce (w 2012 r. przeszkolono 183 pracowników);
- obowiązki stosowania środków zapobiegawczych w komunikacji elektronicznej w postępowaniach prowadzonych przez organy administracji publicznej (w 2012 r. przeszkolono 229 pracowników).

(dowód: akta kontroli str. 359-413)

W ramach polityki bezpieczeństwa informacji, w okresie objętym kontrolą, z Referatu Informatyki wysyłane były, drogą mailową, zasady i informacje dotyczące prawidłowej eksploatacji systemów IT i zabezpieczeń, w tym m.in.:

- ciągłości prac i uprawnień, dostępów(dla spraw danego użytkownika);
- poczty elektronicznej;
- dodawania i usuwania informacji na stronach internetowych;
- pracy użytkowników z systemami;
- sprawdzania systemu programem antywirusowym.

W Urzędzie w ramach Procedury Pb-4 „*Monitorowanie i utrzymanie bezpieczeństwa informacji*” wprowadzono instrukcję dotyczącą komputerów przenośnych. Dokument określał zasady pracy, przechowywania i metody ochrony sprzętu, danych oraz ochrony informacji przy jego pomocy przetwarzanych, co było zgodne § 20 ust. 2 pkt 8 *rozporządzenia KRI*. Użytkownicy, w ramach przekazywania sprzętu, byli zapoznawani z ww. procedurą i zobowiązani do jej stosowania. Na komputerach mobilnych o dużym znaczeniu dla Urzędu zastosowano mechanizmy szyfrujące zawartość całych dysków twardej, lub wyznaczonych katalogów.

(dowód: akta kontroli str. 237-242)

Kontrola 11 umów serwisowych, zakupu oprogramowania, czy też zakupu sprzętu informatycznego wykazała, że Urząd zawarł w nich zapisy gwarantujące odpowiedni poziom bezpieczeństwa informacji, zgodnie z § 20 ust. 2 pkt 10 *rozporządzenia KRI*. Wyżej wymienione umowy posiadały m.in. następujące, przykładowe zapisy:

- „*zleceniodawca zastrzega sobie możliwość pozostawienia dysków twardej u siebie...*”;
- „*wykonawca zobowiązuje się przestrzegać bezwzględnie ... przepisów ustawy o ochronie danych osobowych, ... zachowania tajemnicy służbowej*”;
- „*... umowa przy wykorzystaniu wdrożonego ZS BIP odbywa się zgodnie z Rozporządzeniem ... w sprawie KRI, minimalnych wymagań dla rejestrów publicznych...*”;
- „*każda ze stron zobowiązuje się traktować jako poufne informacje, ... uzyskane w formie ustnej, pisemnej, graficznej...*”;
- „*wykonawca zobowiązuje się do utrzymania tajemnicy handlowej o przetwarzanych danych i nie ujawnianiu danych osobom trzecim zarówno w czasie trwania umowy jak i po jej wygaśnięciu*”.

(dowód: akta kontroli str. 414-620)

W Urzędzie obowiązywała procedura zarządzania incydentami, określająca zasady postępowania w przypadku ich wystąpienia. W ramach tej procedury zapewniono możliwość bezzwłocznego zgłaszania incydentów naruszenia bezpieczeństwa

informacji przez pracowników, a tym samym zrealizowano obowiązek określony w § 20 ust. 2 pkt 13 rozporządzenia KRI.

(dowód: akta kontroli str. 621-677)

W październiku 2012 r. i 2013 r. przeprowadzono w Urzędzie zewnętrzny audyt Systemu Zarządzania Bezpieczeństwem Informacji (SZBI). Systematycznie przeprowadzano również w zaplanowanych terminach audyty wewnętrzne dla sprawdzenia prawidłowości przebiegu realizowanych procesów i oceny skuteczności funkcjonowania SZBI. Z audytów tych sporządzana była dokumentacja poaudytowa.

(dowód: akta kontroli str. 678-723)

We wszystkich objętych badaniem serwerowniach stwierdzono, że posiadały one właściwe zabezpieczenia. Kopie zapasowe systemów informatycznych były tworzone zgodnie z zapisami PBI i harmonogramem (sporządzane były regularnie i testowo odtwarzane). Testowanie polegało na sprawdzeniu, czy wykonana kopia zapasowa nie zawierała błędów oraz czy dane odtworzone były prawidłowe. Kopie tworzone na serwerach przechowywane były wirtualnie w innej lokalizacji, a tworzone na nośnikach danych przechowywane były fizycznie w szafie pancerniej poza miejscem ich wytworzenia. W miejscu przechowywania znajdował się monitoring, instalacja p.poż., wzmocnione drzwi i szyby. Dostęp do szafy posiadali tylko upoważnieni pracownicy.

(dowód: akta kontroli str. 724-763)

Ustalone
nieprawidłowości

W działalności kontrolowanej jednostki w zakresie wdrożenia systemu zarządzania bezpieczeństwem systemów informatycznych nie stwierdzono nieprawidłowości.

Ocena cząstkowa

Najwyższa Izba Kontroli ocenia pozytywnie działalność Urzędu w zakresie wdrożenia systemu zarządzania bezpieczeństwem systemów informatycznych.

3. Zapewnienie dostępności informacji dla osób niepełnosprawnych

Opis stanu
faktycznego

Urząd zamieszczał na swoich stronach internetowych deklarację dostępności strony BIP, zawierającą informację o poprawnej walidacji HTML oraz o tym, że strona spełnia wymogi standardów WCAG¹⁷ 2.0 (podwójne A). Ponadto monitorował dostępność swoich stron za pomocą darmowego narzędzia Got Site Monitor (<http://www.gotsitemonitor.com/>). Pozwalało to na monitorowanie przerw w dostępie użytkowników do stron internetowych.

W kwietniu 2012 r. uruchomiono system komunikacji niewerbalnej pn. „Równość Człowieka Głuchego”. System umożliwiał osobom niedosłyszącym i niesłyszącym komunikację z Urzędem w prosty i bezstresowy sposób. System „Równość Człowieka Głuchego” wykorzystywał środki wspomagające komunikację, m.in. pocztę elektroniczną, SMS, MMS czy też komunikator internetowy do umówienia wizyty czy załatwienia sprawy.

W toku kontroli za pomocą walidatorów dostępnych na stronie <http://validator.w3.org>, <http://jigsaw.w3.org/css-validator/> dokonano (z wykorzystaniem oględzin) porównania zgodności stron internetowych Urzędu (www.portal.legnica.eu, um.bip.legnica.eu) ze standardem służącym dostosowaniu treści strony internetowej do potrzeb osób niepełnosprawnych - WCAG 2.0 w zakresie zasady 4 - Kompatybilność z uwzględnieniem poziomu A. W wyniku tej weryfikacji ustalono, że na stronach internetowych Urzędu wystąpiły dwa błędy, które nie miały wpływu na prezentację treści dla osób niepełnosprawnych.

(dowód: akta kontroli str. 764-782)

¹⁷ Standard służący dostosowaniu wyświetlanej treści na stronie internetowej do potrzeb osób niedowidzących.

IV. Uwagi i wnioski

Wnioski pokontrolne

Przedstawiając powyższe oceny i uwagi wynikające z ustaleń kontroli, Najwyższa Izba Kontroli odstępuje od formułowania wniosków pokontrolnych.

V. Pozostałe informacje i pouczenia

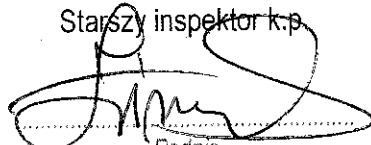
Prawo zgłoszenia
zastrzeżeń

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.

Wrocław, dnia 30 września 2014 r.

Kontroler:
Waldemar Zimoch
Starszy inspektor k.p.



Podpis

Najwyższa Izba Kontroli
Delegatura we Wrocławiu

Dyrektor

DYREKTOR
Delegatura Najwyższej Izby Kontroli
we Wrocławiu
z up.



Ziemowit Florowski
Wicedyrektor