NAJWYŻSZA IZBA KONTROLI
Delegatura we Wrocławiu

LWR-4101-013-02/2014
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

Joanna Marczyk, główny specjalista kontroli państwowej, upoważnienie do kontroli nr 89783 z dnia 9 czerwca 2014 r.

(dowód: akta kontroli str. 1-2)

Jednostka kontrolowana

Urząd Miasta w Dzierżoniowie, ul. Rynek 1, 58-200 Dzierżoniów (dalej: Urząd)

Kierownik jednostki kontrolowanej

Marek Piorun – Burmistrz Miasta Dzierżoniowa

(dowód: akta kontroli str. 3-4)

Akty prawne

1. Ustawa z dnia 29 sierpnia 1997 r. *o ochronie danych osobowych*[1] (dalej: ***ustawa o ochronie danych osobowych***).
2. Rozporządzenie 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*[2] (dalej: ***rozporządzenie w sprawie instrukcji kancelaryjnej***).
3. Rozporządzenie Rady Ministrów z dnia 12 kwietnia 2012 r. *w sprawie Krajowych Ram Interoperacyjności, minimalnych wymagań dla rejestrów publicznych i wymiany informacji w postaci elektronicznej oraz minimalnych wymagań dla systemów teleinformatycznych*[3] (dalej: ***rozporządzenie KRI***).

Słownik pojęć

„**Instrukcja kancelaryjna**" – załącznik nr 1 do rozporządzenia w sprawie instrukcji kancelaryjnej; „**SZRLD**" – Strategia Zrównoważonego Rozwoju Lokalnego Dzierżoniowa; „**EPUAP**" – Elektroniczna Platforma Usług Administracji Publicznej; „**BIP**" – Biuletyn Informacji Publicznej; „**PBDO**" – Polityka Bezpieczeństwa Danych Osobowych; „**SIP**" – System Informacji Przestrzennej; „**ELUD**" – System Ewidencji Ludności; „**WIP+**" – System Windykacji Opłat i Podatków; „**CEPIK**" – Centralna Ewidencja Pojazdów i Kierowców.

II. Ocena kontrolowanej działalności

Ocena ogólna[4]

Burmistrz Miasta Dzierżoniów, 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,* w okresie od 31 maja 2012 r. do 17 lipca 2014 r.:

---

[1] Dz. U. z 2002 r. nr 101, poz.926 ze zm.
[2] Dz. U. Nr 14, poz. 67.
[3] Dz. U. z 2012 r., poz. 526.
[4] 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.

1. zapewnił współpracę zbadanych w toku kontroli systemów informatycznych z innymi systemami Urzędu w sposób spełniający minimalne wymogi w zakresie interoperacyjności, w szczególności poprzez wzajemną komunikację oraz udostępnianie danych w formatach określonych w *rozporządzeniu KRI*;
2. rzetelnie zarządzał bezpieczeństwem informacji w Urzędzie poprzez: (a) opracowanie, wdrożenie i aktualizację Polityki bezpieczeństwa danych osobowych, w której m.in. wprowadzono regulacje dotyczące zgłaszania incydentów naruszenia bezpieczeństwa informacji, (b) prowadzenie i bieżącą aktualizację ewidencji sprzętu komputerowego, zawierającą informacje o jego rodzaju i konfiguracji, umożliwiającą jej odtworzenie po ewentualnej katastrofie lub zdarzeniu losowym, (c) uniemożliwienie użytkownikom systemów informatycznych, niebędących pracownikami służb informatycznych, samodzielnej instalacji oprogramowania na komputerach służbowych, (d) analizę ryzyk w zakresie sprawności i bezpieczeństwa infrastruktury IT, (e) dopuszczanie do pracy w systemach IT osób posiadających stosowne uprawnienia, adekwatne do realizowanych czynności zapisanych w ich zakresach obowiązków, (f) blokowanie dostępu do systemów IT osób zatrudnionych w przeszłości w Urzędzie, (g) przeprowadzanie audytów z zakresu bezpieczeństwa informacji, (h) opracowanie, wdrożenie i stosowanie zasad tworzenia kopii zapasowych danych i oprogramowania;
3. uruchomił dla klientów Urzędu świadczenie czterech usług elektronicznych.

Ustalenia kontroli wykazały również następujące nieprawidłowości przy realizacji zadań określonych w *rozporządzeniu KRI*:

1. zamiast Polityki Bezpieczeństwa Informacji (obejmującej wszystkie dane przetwarzane w Urzędzie) opracowano i wdrożono Politykę Bezpieczeństwa Danych Osobowych,
2. dokonano zmian w treści Strategii Zrównoważonego Rozwoju Lokalnego 2010-2016 w zakresie zadań dostosowania Urzędu do elektronicznego świadczenia usług publicznych bez zachowania adekwatnej formy wprowadzenia w życie, tj. uchwały Rady Miasta,
3. nie zapewniono szkoleń w zakresie bezpieczeństwa informacji osobom zaangażowanym w proces przetwarzania informacji, innym niż informatycy, co było niezgodne z § 20 ust. 2 pkt 6 *rozporządzenia KRI*,
4. zamiast zasad (procedur) gwarantujących bezpieczną pracę przy przetwarzaniu mobilnym i pracy na odległość, wprowadzono w tym zakresie regulacje dotyczące tylko danych osobowych, co było niezgodne z § 20 ust. 2 pkt 8 *rozporządzenia KRI*,
5. w trzech umowach (dotyczących systemów: eDIOM, SIDAS Repozytorium oraz NDZ+) dostawcy nie zostali zobowiązani do zachowania tajemnicy informacji, do której mogli mieć dostęp w związku ze świadczeniem serwisu gwarancyjnego, co było niezgodne z postanowieniami § 20 ust. 2 pkt 8 *rozporządzenia KRI*.

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 obowiązujących w badanym okresie Strategiach Zrównoważonego Rozwoju Lokalnego Dzierżoniowa na lata 2010-2016 i 2014-2020 ujęto m.in. zagadnienia dotyczące dostosowania Urzędu do elektronicznego świadczenia usług publicznych.

Zgodnie z zapisami ww. dokumentów Urząd planował rozwój e-usług (SZRLD na lata 2010-2016 i 2014-2020)[5] oraz wdrażanie nowych systemów usprawniających obsługę klienta wewnętrznego i zewnętrznego (SZRLD na lata 2014-2020[6]. W żadnym z ww. dokumentów nie określono terminu wdrożenia tych działań, przy czym w obu ustalono mierniki jego realizacji:

a) **SZRLD na lata 2010-2016:** *poziom satysfakcji klienta UM, *poziom satysfakcji klienta jednostek UM, *liczba spraw, które można załatwić elektronicznie, *liczba klientów korzystających z e-usług, *poziom satysfakcji e-klienta;
b) **SZRLD na lata 2014-2020:** *ilość e-usług, *ilość komputerów udostępnianych mieszkańcom, *ilość darmowych punktów dostępu do internetu, *poziom satysfakcji klienta wewnętrznego i zewnętrznego.

(dowód: akta kontroli str. 46, 146)

Z-ca Burmistrza Miasta Dzierżoniowa Wanda Ostrowska wyjaśniła, że w Strategii Rozwoju Lokalnego Dzierżoniowa na lata 2010-2016 zostały przedstawione jedynie propozycje wskaźników do monitoringu i ewaluacji dla celu operacyjnego „Podnoszenie poziomu usług świadczonych przez Urząd Miasta i jego jednostki organizacyjne". Wartości wskaźników do monitoringu rocznego przyjmowano wynikowo za dany rok, ponieważ proponowane wskaźniki nigdy nie były mierzone (nie została określona ich wartość początkowa). Podała również, że w 2011 r. w wyniku Przeglądu procesów został zidentyfikowany proces pn. „Zarządzanie informacją i technologią IT", który zastąpił dotychczasowe zadanie Rozwój e-usług. Dla ww. procesu określono dwa wskaźniki: Sprawność działania infrastruktury IT oraz Bezpieczeństwo infrastruktury IT. Zmiany podejścia podyktowane były znikomą liczbą mieszkańców korzystających z usług, co wynikało z konieczności posiadania przez nich podpisu elektronicznego. Ponadto, posługiwanie się typowym nazewnictwem e-usługi utożsamiane było z możliwością załatwiania spraw za pośrednictwem platformy EPUAP, do czego społeczeństwo nie było w ówczesnym czasie przygotowane. W związku z tym trudno byłoby określić stopień realizacji tak postawionego sobie celu czy zadania. Dodała również, że SZRLD na lata 2014-2020 jest na etapie wdrażania tj. określania mierników i zadań a w związku z tym brak jest jakichkolwiek danych z ich realizacji oraz stanowiących wyznacznik.

(dowód: akta kontroli str. 181-187)

W badanym okresie, Urząd nie dokonywał analiz potrzeb w zakresie działań promocyjnych tzn. nie przeprowadzono ankiet oraz nie podjęto innych działań w celu zidentyfikowania potrzeb mieszkańców co do ilości oraz treści materiałów promocyjnych dotyczących komunikacji elektronicznej z Urzędem. W ww. okresie jedynym działaniem promocyjnym jakie podjął Urząd były publikacje na stronie internetowej Urzędu oraz w miejskim informatorze samorządowym („Goniec Dzierżoniowski) dotyczące uruchomienia wyszukiwarki umożliwiającej sprawdzenie przez klientów statusu wniesionej sprawy.

(dowód: akta kontroli str. 203-210, 236)

Urząd, u nie zwracał się do Ministra Administracji i Cyfryzacji ani z problemami, ani z prośbą o pomoc w zakresie dostosowania swoich systemów/rejestrów informatycznych do wymogów KRI.

(dowód: akta kontroli str. 146, 188-189)

---

[5] Cel strategiczny nr 2 „Tworzenie miasta przyjaznego", cel operacyjny nr 5 „Podnoszenie poziomu usług świadczonych przez Urząd Miasta i jego jednostki organizacyjne", zadanie pn. „Rozwój e-usług" (SZRLD na lata 2010-2016) oraz cel strategiczny nr 6 „Rozwój społeczeństwa cyfrowego, innowacyjności oraz gospodarki opartej na wiedzy", cel operacyjny nr 6.2 „Rozwój e-usług" (SZRLD na lata 2014-2020).

[6] Cel strategiczny nr 6 „Rozwój społeczeństwa cyfrowego, innowacyjności oraz gospodarki opartej na wiedzy", cel operacyjny nr 6.5 „Wdrażanie nowych systemów usprawniających obsługę klienta wewnętrznego i zewnętrznego" (SZRLD na lata 2014-2020).

W Urzędzie zasady obiegu, dokumentowania i doręczania korespondencji określone zostały w badanym okresie w instrukcji obiegu, dokumentowania i doręczania korespondencji z dnia 23 kwietnia 2012 r.[7], a następnie z dnia 9 września 2013 r.[8]. W obu ww. dokumentach przyjęto, że podstawowym sposobem dokumentowania przebiegu i rozpatrywania spraw w Urzędzie jest system tradycyjny (tzn. papierowy), wspomagany elektronicznym obiegiem dokumentów a przyjmowanie i obieg dokumentacji odbywa się wg zasad opisanych w Rozdziale 3 Instrukcji kancelaryjnej. Ponadto, w obu ww. procedurach określono zasady postępowania z korespondencją przesłaną pocztą elektroniczną i funkcjonowania elektronicznej skrzynki podawczej, przy czym w żadnej z nich nie zawarto zapisów wprowadzających obowiązek przypisywania/powiązania wszystkich (wchodzących i wychodzących) dokumentów do konkretnych spraw, tak aby przegląd poszczególnych spraw pozwalał na zidentyfikowanie wszystkich nadesłanych i wysłanych dokumentów.

(dowód: akta kontroli str. 5-45, 47-55)

Badanie sześciu losowo wybranych dokumentów, które wpłynęły do Urzędu (cztery dokumenty w postaci papierowej oraz dwa w formie elektronicznej) wykazało, że: (a) rejestracja ww. dokumentów odbywa się w systemie SIDAS EZD ver.3.0.6, (b) dokumenty w postaci papierowej[9] przetwarzane były na postać elektroniczną w drodze skanowania, (c) wszystkie skany dokumentów wprowadzano jako załącznik do zarejestrowanej w ww. systemie sprawy, (d) dokumenty wytwarzane przez Urząd w związku z dokumentami zarejestrowanymi (np. odpowiedzi Urzędu): *nie były procedowane (np. akceptowane) jako dokumenty elektroniczne, lecz jako dokumenty papierowe, *nie były załączane do systemu w formie skanów a *ich rejestracji dokonywano w module (rejestrze) pism wychodzących bez powiązania ze sprawą, do której przypisano dokument wpływający do Urzędu.

(dowód: akta kontroli str. 56-60)

W okresie od 31 maja 2012 r. do 31 maja 2014 r. korespondencja Urzędu z obywatelami (osobami fizycznymi), podmiotami gospodarczymi oraz innymi urzędami objęła łącznie 101 290 dokumentów, w tym 40 018 wpłynęło do Urzędu a 61 272 zostało przez Urząd wysłanych. Znaczna część ww. korespondencji (101 094 dokumenty – 99,81%) została dostarczona w formie papierowej[10] a tylko 214 dokumentów[11], tj. 0,21% - drogą elektroniczną. Największy udział w korespondencji elektronicznej miały wnioski o udostępnienie informacji publicznej – 198 dokumentów, w tym 109 wpłynęło do Urzędu[12] a 89 zostało przez Urząd wysłane[13].

(dowód: akta kontroli str. 190)

W procesie zarządzania usługami elektronicznymi Urząd wspierał model usługowy w podstawowym zakresie. W badanym okresie Urząd świadczył dziewięć usług

---

[7] Pismo Okólne Burmistrza Miasta z dnia 23.04.2012 r. nr 54/2012 w sprawie wprowadzenia Instrukcji obiegu, dokumentowania i doręczania korespondencji w Urzędzie Miasta w Dzierżoniowie (wycofane z dniem 09.09.2013 r.).

[8] Pismo Okólne Burmistrza Miasta z dnia 9.09.2013 r. nr 79/2013 w sprawie wprowadzenia Instrukcji obiegu, dokumentowania i doręczania korespondencji w Urzędzie Miasta w Dzierżoniowie.

[9] Oprócz tych zawierających dane wrażliwe (np. kierowane do Urzędu Stanu Cywilnego).

[10] 39.899 dokumentów wpływających do Urzędu oraz 61 195 dokumentów wysyłanych przez Urząd.

[11] 112 dokumentów wpłynęło do Urzędu, w tym 27 zostało wysłanych przez obywateli a 85 przez podmioty gospodarcze oraz 102 dokumenty wysłane przez Urząd, w tym 25 do obywateli i 77 do podmiotów gospodarczych.

[12] 24 przez obywateli (18 za pomocą e-mail, 6 – EPUAP) i 85 przez podmioty gospodarcze (76 – e-mail, 9 – EPUAP).

[13] 19 do obywateli (18 za pomocą e-mail, 1 – EPUAP) i 70 do podmiotów gospodarczych (69 – email, 1 – EPUAP).

elektronicznych poprzez EPUAP[14]: (1) „Bonifikata opłat rocznych z tytułu użytkowania wieczystego nieruchomości gruntowych", (2) „Przyjmowanie zawiadomień o organizacji zgromadzenia publicznego", (3) „Skargi, wnioski, zapytania do urzędu", (4) „Zezwolenie na usunięcie drzew i krzewów", (5) „Wypisy i wyrysy ze studium uwarunkowań i kierunków zagospodarowania przestrzennego", (6) „Objęcie patronatem imprez o charakterze lokalnym i ponadlokalnym", (7) Rozpatrywanie wniosków o wyrażenie zgody na używanie herbu miasta", (8) „Zawiadomienie o odkryciu w trakcie robót budowlanych lub ziemnych przedmiotu, co do którego istnieje przypuszczenie, iż jest zabytkiem", (9) „Dostęp do informacji publicznej". Wszystkie ww. usługi zostały wprowadzone przed 30 maja 2012 r. i wykorzystywały predefiniowane dokumenty/formularze znajdujące się na EPUAP[15] stąd też Urząd nie przekazywał wzorów usług elektronicznych do centralnego repozytorium prowadzonego przez Ministerstwo Administracji i Cyfryzacji. Na dziewięć usług elektronicznych świadczonych przez Urząd, w trzech przypadkach[16] nie zostały one opisane w karatach opisów m.in. publikowanych w BIP. W przypadku sześciu pozostałych[17], w kartach usług (papierowych i publikowanych w BIP): (a) opisy usług były aktualne[18] i zgodne ze świadczoną usługą, (b) umieszczono dane dot. podmiotu/właściciela usługi (jednostki organizacyjnej odpowiedzialnej za realizację świadczonej usługi), miejsce świadczenia usług, aktualną podstawę prawną i sposób realizacji usługi oraz (c) wskazano osoby wprowadzające informacje nt. opisywanych usług (tj. technicznych właścicieli usług). W opisach żadnej z sześciu ww. usług nie zawarto informacji o możliwości załatwienia spraw drogą elektroniczną. Ze względu na fakt, że ww. usługi realizowane były przez portal EPUAP, a Urząd nie ma możliwości technicznej ingerencji w jego funkcjonowanie, w ich opisach nie wskazano również maksymalnego ani dopuszczalnego czasu ich niedostępności, sposobu zgłaszania awarii oraz osób/komórek/podmiotów odpowiedzialnych za usuwanie awarii.

(dowód: akta kontroli str. 76-82, 138-145)

Zakres współpracy systemów informatycznych wewnątrz Urzędu zbadano w oparciu o dobór celowy następujących systemów, zakupionych po 31 maja 2012 r.[19]: (1) SIDAS EZD – Elektroniczny obieg dokumentów, (2) SIDAS REPOZYTORIUM – system do przechowywania dowolnych plików w sposób usystematyzowany umożliwiający łatwe wyszukiwanie (moduł SIDAS EZD), (3) eDIOM, Map View Desktop, eDIOM OR, eDIOM ZPD – ewidencja dróg i obiektów mostowych (eDIOM), program do prezentacji graficznej (Map View Desktop), ewidencja organizacji ruchu

---

[14] W ww. okresie nie świadczono usług elektronicznych dla obywateli z wykorzystaniem własnej strony internetowej.

[15] http://crd.gov.pl/wzor/2010/04/22/357 (usługa pn. „Objęcie patronatem imprez o charakterze lokalnym"), http://crd.gov.pl/wzor/2010/04/22/369 (usługa pn. "Bonifikata opłat rocznych z tytułu użytkowania wieczystego nieruchomości gruntowych"), http://crd.gov.pl/wzor/2010/04/20/343 (usługa pn. "Zawiadomienie o odkryciu w trakcie robót budowlanych lub ziemnych przedmiotu, co do którego istnieje przypuszczenie, iż jest zabytkiem"), http://crd.gov.pl/wzor/2010/04/22/351 (usługa pn."Zezwolenie na usunięcie drzew i krzewów"), http://crd.gov.pl/wzor/2010/04/22/361 (usługa pn. "Przyjmowanie zawiadomień o organizacji zgromadzenia publicznego"), http://crd.gov.pl/wzor/2010/04/22/350 (usługa pn. "Rozpatrywanie wniosków o wyrażenie zgody na używanie herbu miasta"), http://crd.gov.pl/wzor/2010/04/20/339 (usługa pn. "Wypisy i wyrysy ze studium uwarunkowań i kierunków zagospodarowania przestrzennego"), http://crd.gov.pl/wzor/2008/05/09/3 (usługi pn. „Skargi, wnioski, zapytania do urzędu" oraz „Dostęp do informacji publicznej").

[16] „Skargi, wnioski, zapytania do urzędu"; „Rozpatrywanie wniosków o wyrażenie zgody na używanie herbu miasta"; „Zawiadomienie o odkryciu w trakcie robót budowlanych lub ziemnych przedmiotu, co do którego istnieje przypuszczenie, iż jest zabytkiem".

[17] „Bonifikata opłat rocznych z tytułu użytkowania wieczystego nieruchomości gruntowych"; „Przyjmowanie zawiadomień o organizacji zgromadzenia publicznego"; „Zezwolenie na usunięcie drzew i krzewów"; „Wypisy i wyrysy ze studium uwarunkowań i kierunków zagospodarowania przestrzennego"; „Objęcie patronatem imprez o charakterze lokalnym i ponadlokalnym"; Dostęp do informacji publicznej.

[18] Opisu usług były aktualizowane, co było widoczne na stronie internetowej BIP.

[19] Data wejścia w życie *rozporządzenia KRI*.

drogowego (eDIOM OR), ewidencja zajęcia pasa drogowego (eDIOM ZPD), (4) NDZ+ - system naliczania opłat dzierżawnych, (5) iArkusz – internetowe narzędzie pozwalające na przygotowanie projektu arkusza organizacyjnego każdego typu placówki oświatowej, (6) SYSTEmEG[20] – zarządzenie danymi dotyczącymi nieuiszczonych opłat za parkowanie w strefie płatnego parkowania.

W wyniku badania ustalono, że systemy SIDAS EZD, SIDAS REPOZYTORIUM, eDIOM, Map View Desktop, eDIOM OR, eDIOM ZPD oraz NDZ+ spełniają minimalne wymogi interoperacyjności w zakresie współpracy z innymi systemami Urzędu określone w § 5 ust.3 pkt 3 *rozporządzania KRI*[21]. Powyższe systemy komunikują się bowiem z innymi systemami wewnątrz Urzędu na poziomach: (1) transakcyjnym, tzn. wymiana danych pomiędzy systemami następuje bez jakiegokolwiek pośrednictwa pracownika, czyli przekazywanie danych odbywa się w sposób w pełni zautomatyzowany, (2) dwustronnej komunikacji, tzn. dane z systemu A przekazywane są do systemu B, przy czym system B samodzielnie odnotowuje, że oczekują dane które mogą być zaimportowane a rolą pracownika jest udzielenie zgody (zatwierdzenie) w systemie B na wczytanie otrzymanych danych oraz (3) jednostronnej komunikacji, tzn. dane z jednego systemu są przekazywanie do innego systemu za pośrednictwem pracownika (operatora systemu), który dane te importuje ręcznie do systemu. I tak:

- **SIDAS EZD** – komunikuje się na poziomie transakcyjnym z BIP (wymiana danych dotyczy ID sprawy, daty i godziny ostatniej modyfikacji a także statusu i nazwy instytucji, tj. danych nadawane w EZD oraz nr umowy, przedmiotu umowy, wykonawcy i wartości zamówienia brutto, tj. danych z Centralnego Rejestru Umów prowadzonego w EZD),
- **SIDAS REPOZYTORIUM** – komunikuje się na poziomie jednostronnej komunikacji z SIDAS EZD (wymiana danych polega na przekazywaniu do repozytorium dowolnego dokumentu wytworzonego w EZD SIDAS, przy czym czynność ta wymaga stworzenia procesu powiązanego z metryką dokumentu i ręcznego „wydania polecenia" przez pracownika),
- **eDIOM, Map View Desktop, eDIOM OR, eDIOM ZPD** – na poziomie transakcyjnym komunikuje się z SIP (dane z zakresu ewidencji gruntów, budynków i lokali). Systemy SIP i eDIOM potrafią łączyć się do kilku baz danych jednocześnie (bazy rozproszone) i wykorzystywać zawarte w nich dane do swoich potrzeb, np. w eDIOM zdefiniowane jest połączenie do bazy ewidencji gruntów i podczas uruchamiania eDIOM automatycznie łączy się z bazą i pobiera w znajdujące się w niej dane umieszczając je na odpowiednich warstwach stanowiących podkład dla danych gromadzonych w swojej własnej bazie (infrastruktura drogowa zostaje zorientowana w przestrzeni geodezyjnej),
- **NDZ+** - wymiana danych na poziomie transakcyjnym z ELUD+ (dane osobowe z zakresu ewidencji ludności) oraz dwustronnej komunikacji z WIP+ (kwoty przypisanych do kart dzierżawców)[22],

---

[20] System niewdrożony do końca kontroli NIK.

[21] Przepis stanowi, że interoperacyjność na poziomie semantycznym osiągana jest m.in. poprzez stosowanie w rejestrach prowadzonych przez podmioty publiczne odwołań do rejestrów zawierających dane referencyjne w zakresie niezbędnym do realizacji zadań.

[22] Program NDZ+ zasilany jest danymi z ELUD natomiast dane z NDZ zasilają program WIP+(**E – ELUD+** - zasilanie danymi; **W – WIP+** - wysyłanie danych): • NAZWISKO — Nazwisko lub dla osób prawnych nazwa dzierżawcy (płatnika) **E i W**; • IMIE — Imię **E i W**; • IMIE2 — Drugie imię **E i W**; • IMIEOJCA — Imię ojca **E i W**; • IMIEMATKI — Imię matki **E i W**; • PESEL — Numer PESEL **E i W**; • ULIADR — Ulica **E i W**; • NRDOMUADR — Numer domu **E i W**; • NRLOKADR — Numer lokalu **E i W**; • MIEJADR — Miejscowość **E i W**; • KODADR — Kod pocztowy **E i W**; • NAZWISKO — Nazwisko **E i W**; • IMIE — Imię **E i W**; • IMIE2 — Drugie imię **E i W**; • IMIEOJCA — Imię ojca **E i W**; • IMIEMATKI — Imię matki **E i W**; • PESEL — Numer PESEL **E i W**; • NAZWAPELNA — Nazwa pełna **W**; • NAZWASKR — Nazwa skrócona **W**; • UWAGI — Uwagi **W**; • NAZWAREJ — Nazwa rejestrowa **W**; • NRREJ — Numer rejestrowy **W**; • NRDOK — Numer dokumentu **W**; • KRAJKOR —

- **iArkusz i SYSTEmEG** – nie wymieniają danych z innymi systemami wewnątrz Urzędu (brak takiej potrzeby – iArkusz, po wdrożeniu systemu SYSTEmEG będzie wymieniał dane z CEPiK).

(dowód: akta kontroli str. 191-193)

Urząd nie zwracał się do innych jednostek administracji publicznej z propozycją prowadzenia wzajemnej komunikacji wyłącznie w formie elektronicznej. Do Urzędu, z wnioskiem o prowadzenie wzajemnej komunikacji elektronicznej zwrócili się natomiast: (1) Ministerstwo Administracji i Cyfryzacji (dot. ogólnej korespondencji za pośrednictwem platformy EPUAP), (2) Dolnośląski Urząd Wojewódzki (dot. sprawozdań z wykonywania zadań z zakresie opieki nad dziećmi do lat trzech za pomocą komunikatora Quickstat), (3) Kuratorium Oświaty we Wrocławiu (dot. wszystkich dane za pośrednictwem Systemu Informacji Oświatowej oraz danych o ilości sześciolatków w szkołach za pośrednictwem strony internetowej Kuratorium), (4) Ministerstwo Zdrowia (dot. rocznych sprawozdań z zakresu Narodowego Programu Ochrony Zdrowia Psychicznego za pomocą platformy obsługiwanej przez Zespół Badawczy ASM – Centrum Badań i Analiz Rynku), (5) Dolnośląski Urząd Wojewódzki (dot. przekazywania rejestrów wydanych decyzji o ustaleniu inwestycji celu publicznego za pośrednictwem EPUAP).We wszystkich ww. przypadkach Urząd podjął komunikację elektroniczną w proponowanym zakresie.

W badanym okresie elektroniczna komunikacja z innymi jednostkami administracji publicznej odbywała się przy wykorzystaniu następujących portali, systemów Urzędu i/lub narzędzi:

I. portale: (1) EPUAP (m.in. przekazywanie informacji i dokumentów w ramach usług Urzędu oraz innych jednostek publicznych), (2) Portal Urzędu Zamówień Publicznych i (3) Urzędu Publikacji Unii Europejskiej (publikacja ogłoszeń dot. zamówień publicznych), (4) SHRIMP, tj. system harmonogramowania, rejestrowania i monitorowania pomocy publicznej Urzędu Ochrony Konkurencji i Konsumentów (przekazywanie sprawozdań o udzielonej pomocy publicznej i informacji o nieudzieleniu takiej pomocy), (5) System Rejestracji Pomocy Publicznej Ministerstwa Rolnictwa i Rozwoju Wsi (przekazywanie sprawozdań albo informacji dotyczących pomocy publicznej w rolnictwie i rybołówstwie), (6) CEPIK, tj. Centralna Ewidencja Pojazdów i Kierowców (pozyskanie danych osobowych właścicieli pojazdów, którzy nie uiścili opłaty parkingowej w strefie płatnego parkowania[23]), (7) System Sprawozdawczości Budżetowej Dolnośląskiego Urzędu Wojewódzkiego, (8) CEIIODG, tj. Centralna Ewidencja i Informacja o Działalności Gospodarczej (przekazywanie wniosków przedsiębiorców dotyczących wpisów działalności gospodarczej), (9) PIA, tj. Portal Informacyjny Administracji (dwustronna komunikacja z urzędami na terenie kraju, w szczególności w sprawach meldunkowych, tj. przekazywanie aktualizacji Dolnośląskiego Urzędu Wojewódzkiego[24], nadawanie numerów ewidencyjnych pesel do Ministerstwa Spraw Wewnętrznych[25], dane dotyczące zameldowania lub wymeldowania stałego/czasowego oraz dopisania/skreślenia ze spisów wyborców do zainteresowanych adresatów, tj. jednostek publicznych), (10) Platforma wyborcza (rejestr wyborców i komunikacja z Krajowym Biurem

---

Kraj adresu do korespondencji **W**; • WOJKOR — Województwo adresu do korespondencji **W**; • POWKOR — Powiat adresu do korespondencji **W**; • GMIKOR — Gmina adresu do korespondencji **W**; • ULIKOR — Ulica adresu do korespondencji **W**; • NRDOMUKOR — Numer domu adresu do korespondencji **W**; • NRLOKKOR — Numer lokalu adresu do korespondencji **W**; • MIEJKOR — Miejscowość adresu do korespondencji **W**; • KODKOR — Kod pocztowy adresu do korespondencji **W**; • POCZKOR — Poczta adresu do korespondencji **W**.

[23] Komunikacja polega na przesyłaniu danych do CEPiK w formie paczek informacji na odpowiedni serwer.

[24] Dane przekazywane w formie paczek plików z aplikacji Urzędu pn. ELUD.

[25] Dane przekazywane w formie paczek plików z aplikacji Urzędu pn. ELUD.

Wyborczym Delegaturą w Wałbrzychu), (11) portal Ministerstwa Pracy i Polityki Społecznej (przesyłanie do Dolnośląskiego Urzędu Wojewódzkiego sprawozdań rzeczowo-finansowych z wykonywania zadań z zakresu opieki nad dziećmi w wieku od trzech lat), (12) platforma Kuratorium Oświaty (dane w Systemie Informacji Oświatowej), (13) platforma obsługiwana przez Zespół Badawczy ASM – Centrum Badań i Analiz Rynku (sprawozdania do Ministerstwa Zdrowia z realizacji Narodowego Programu Ochrony Zdrowia Psychicznego);

II. systemy Urzędu: (1) POGRUN+ (eksport danych zawartych w ewidencji podatkowej nieruchomości, w celu ich porównania z danymi zawartymi w ewidencji gruntów i budynków, tj. aplikacji Starostwa Powiatowego[26]); (2) LEGISLATOR (przekazywanie uchwały stanowiące prawo miejscowe celem ich ogłoszenia w Dzienniku Urzędowym Województwa – dwustronna komunikacja);

III. narzędzia: (1) skrzynka e-mail - bieżąca komunikacja nieujęta w pozostałych sposobach komunikacji elektronicznej oraz m.in. korespondencja z: (a) Urzędem Marszałkowskim Województwa Dolnośląskiego (informacje o realizacji inwestycji), (b) Dolnośląską Służbą Dróg i Kolei we Wrocławiu (informacje o wspólnych inwestycjach), (c) jednostkami oświatowymi i pomocy społecznej oraz (d) korespondencja USC z Dolnośląskim Urzędem Wojewódzkim w formie przesyłu zeskanowanych dokumentów), (2) APUSC, tj. aplikacja dostarczona do Urzędu przez GUS (sprawozdawczość statystyczna w zakresie urodzeń, małżeństw i zgonów[27] - jednostronna komunikacja), (3) Besti@, tj. aplikacja dostarczona do Urzędu przez Ministerstwo Finansów[28] (dwustronna komunikacja).

Jedynym systemem, który wykorzystywał referencje do danych zewnętrznych, tj. bezpośrednio odwoływał się do danych gromadzonych w innych systemach/rejestrach publicznych był system pn. Besti@ (danymi, z których korzystano były słowniki dotyczące sprawozdań finansowych).

(dowód: akta kontroli str. 261-268)

Ustalone nieprawidłowości

W działalności kontrolowanej jednostki w przedstawionym wyżej zakresie stwierdzono, że zagadnienia dotyczące dostosowania Urzędu do elektronicznego świadczenia usług publicznych, zawarte w obowiązującej w latach 2010-2016 SZRLD, nie były w pełni realizowane. Z wyjaśnień Z-cy Burmistrza Dzierżoniowa wynika bowiem, że w wyniku przeglądu procesów został zidentyfikowany proces pn. „Zarządzanie informacją i technologią IT", który zastąpił dotychczasowe zadanie Rozwój e-usług, tj. zadanie ujęte w SZRLD przyjętej uchwałą Rady Miejskiej Dzierżoniowa[29]. Zmieniono również proponowane wskaźniki realizacji zadania, gdyż zamiast poziomu satysfakcji klienta Urzędu i jego jednostek, liczby spraw, które można załatwić elektronicznie, liczby klientów korzystających z e-usług oraz poziomu satysfakcji e-klienta (miar zadania pn. „Rozwój e-usług") przyjęto sprawność działania infrastruktury IT oraz bezpieczeństwo infrastruktury IT (miary procesu pn. „Zarządzanie informacją i technologią IT"). Kontrola wykazała, że powyższe zmiany nie zostały wprowadzone do treści SZRLD 2010-2016 uchwałą Rady Miasta.

(dowód: akta kontroli str. 46, 146)

[26] Eksport do pliku XML.
[27] Aplikacja wysyła do GUS dane w postaci paczek informacji na odpowiedni serwer.
[28] Aplikacja wysyła dane w postaci paczek informacji na dany serwer Regionalnej Izby Obrachunkowej i Ministerstwa Finansów (sprawozdawczość).
[29] Uchwała nr XLIV/270/09 z dnia 29.06.2009 r.

Uwagi dotyczącej badanej działalności

W ocenie Najwyższej Izby Kontroli poznanie potrzeb obywateli i poznanie ich oczekiwań w zakresie dostępności do usług elektronicznych jest warunkiem zapewnienia sprawnego świadczenia takich usług przez Urząd. Zwiększenie udziału komunikacji elektronicznej w świadczeniach publicznych realizowanych przez Urząd i zorientowanie na rozwój i poszerzenie usług elektronicznych pozwoliłoby na usprawnienie pracy Urzędu.

Zdaniem Najwyższej Izby Kontroli należałoby rozważyć wprowadzenie w nieodległej przyszłości w pełni elektronicznego systemu prowadzenia spraw, jako podstawowego systemu wykonywania czynności kancelaryjnych w Urzędzie. W ocenie NIK w pierwszej kolejności należałoby wprowadzić tą zasadę dla korespondencji wytwarzanej wewnątrz Urzędu (w ramach tzw. procedowania sprawy). Wdrożenie jej mogłoby przyczynić się do przyspieszenia obiegu dokumentów i rozpatrywania spraw oraz do ograniczenia kosztów związanych z ich wytwarzaniem w postaci papierowej.

W ocenie Najwyższej Izby Kontroli zapewnienie przez Urząd sprawnego świadczenia usług elektronicznych wymaga jeszcze podjęcia działań dla jego usprawnienia. W tym celu dla wszystkich świadczonych przez Urząd usług elektronicznych konieczne jest opracowanie kart opisów usług, zawierających m.in. informacje o możliwości załatwienia spraw drogą elektroniczną, sposobie zgłaszania awarii i osobach/komórkach/podmiotach odpowiedzialnych za ich usuwanie.

Ocena cząstkowa

Najwyższa Izba Kontroli ocenia pozytywnie mimo stwierdzonych nieprawidłowości działalność kontrolowanej jednostki w zakresie dostosowania posiadanych systemów teleinformatycznych do współpracy z systemami/rejestrami, używanymi wewnątrz Urzędu oraz przez inne podmioty administracji publicznej.

2. Wdrożenie systemu zarządzania bezpieczeństwem systemów informatycznych

Opis stanu faktycznego

W Urzędzie nie opracowano i nie wdrożono Polityki Bezpieczeństwa Informacji, która jest elementem systemu zarządzania bezpieczeństwem informacji. Zauważyć należy, że w myśl § 20 ust. 3 *rozporządzenia KRI*, wymagania w zakresie systemu zarządzania bezpieczeństwem informacji uznaje się za spełnione, jeżeli została opracowana na podstawie Polskiej Normy: PN-ISO/IEC 27001:2007 *Technika informatyczna. Techniki bezpieczeństwa. Systemy zarządzania bezpieczeństwem informacji*, oraz powiązanej z nią Polskiej Normy PN-ISO/IEC 17799:2007 *Technika informatyczna. Techniki bezpieczeństwa. Praktyczne zasady zarządzania bezpieczeństwem informacji*. W pkt 5.1.1. normy PN-ISO/IEC17799 wskazuje się, aby opracowano i stosowano w Urzędzie dokument polityki bezpieczeństwa informacji. W 2011 r. w Urzędzie opracowano PBDO[30], która nie dotyczyła jednak wszystkich danych jakie są przetwarzane w Urzędzie. Właścicielem PBDO, tj. osobą odpowiedzialną za zarządzanie opracowaniem, przeglądem i oceną ww. dokumentu, był do dnia 12 czerwca 2014 r. Burmistrz Dzierżoniowa (zgodnie z art. 36 ust. 2 i 3 ustawy *o ochronie danych osobowych*) a od 13 czerwca 2014 r. Administrator Bezpieczeństwa Informacji (zarządzenie Burmistrza Dzierżoniowa nr 328/2014 z dnia 13 czerwca 2014 r.).

(dowód: akta kontroli str. 146, 194-197, 243-244)

W badanym okresie, w Urzędzie, do ewidencji sprzętu komputerowego i oprogramowania, oprócz książki inwentarzowej, prowadzonej dla potrzeb rachunkowości, wykorzystywany był program pn. „Ewidencja sprzętu

[30] Wprowadzoną Zarządzeniami Burmistrza Miasta Dzierżoniowa: nr 252/2011 z dnia 18.05.2011 r., nr 382/2012 z dnia 13.07.2012 r. oraz zmienione Zarządzeniem Burmistrza Miasta Dzierżoniowa nr 47/2014 z dnia 20.01.2014 r.

komputerowego i oprogramowania dla przedsiębiorców i instytucji publicznych" ver.1.12.0, zakupiony 10 września 2008 r.[31]. Z badania 14 komputerów (10 wybranych losowo i czterech wybranych celowo[32]) oraz jednego serwera wynika, że ww. program do inwentaryzacji sprzętu IT zawierał co najmniej następujące dane: nazwa komputera, nr ewidencyjny, nr seryjny, stan techniczny, nazwa dostawcy, nazwa producenta, nazwa serwisanta, imię i nazwisko pracownika odpowiedzialnego za sprzęt, cena, nr dowodu zakupu, data zakupu, data odbioru, wartość bieżąca, opis, rodzaj procesora, płyty głównej, obudowy, karty sieciowej i graficznej oraz rodzaj i wielkość pamięci RAM a także rodzaj i pojemność dysku twardego. Ponadto, ww. badanie wykazało, że Urząd skutecznie uniemożliwiał użytkownikom systemów informatycznych (pracownikom Urzędu), niebędących pracownikami służb informatycznych, samodzielną instalację oprogramowania na komputerach służbowych.

(dowód: akta kontroli str. 86-104, 146, 246-251)

W latach 2012-2013, stosownie do § 20 ust. 2 pkt 3 *rozporządzenia KRI* oraz zgodnie z wymogiem zawartym w Procedurze zarządzania ryzykiem[33], dokonywano analizy ryzyk występujących w poszczególnych wydziałach i jednostkach organizacyjnych Urzędu. W ww. okresie Wydział Informatyzacji, ustalając ryzyka w zakresie sprawności działania infrastruktury[34], bezpieczeństwa infrastruktury IT[35] oraz rozwoju i wdrażania nowych systemów informatycznych[36], zidentyfikował także konieczne działania je minimalizujące. Kwartalnie sporządzano również sprawozdania z występowania ww. ryzyk, przy czym w żadnym z nich nie stwierdzono utraty poufności i integralności informacji.

(dowód: akta kontroli str. 146, 258-260)

Na 15 wybranych pracowników mających dostęp do objętych badaniem systemów IT, wszyscy posiadali stosowne uprawnienia adekwatne do realizowanych czynności zapisanych w ich zakresach obowiązków, co było zgodne z § 20 ust. 2 pkt 4 *rozporządzenia KRI*.

(dowód: akta kontroli str. 146, 159-180)

Na 11 osób, które w okresie od 31 maja 2012 r. do 31 maja 2014 r. zakończyły zatrudnienie w Urzędzie Miasta Dzierżoniów (w tym czterech posiadających dostęp do jednego z systemów objętych badaniem, tj. SIDAS EZD):

- w dwóch przypadkach (N[...] G[...] i M[...] D[...]) w momencie zatrudnienia ww. osób, do Wydziału Informatyzacji Urzędu nie złożono wniosku o zarejestrowanie użytkownika systemów informatycznych,
- w jednym przypadku (A[...] C[...]-Sz[...]) nie zablokowano dostępu pracownika do poczty elektronicznej, mimo iż umowa wiążąca Urząd z tym pracownikiem wygasła 31 grudnia 2013 r.[37] (nieprawidłowość ta została usunięta w trakcie kontroli NIK).

---

[31] Faktura VAT 1031729-01-4-R z dnia 10.09.2008 r.

[32] Cztery komputery przekazane do użytkowania przez MSWiA na mocy porozumienia z dnia 5.11.2010 r. w ramach realizacji projektu indywidualnego pl.ID – „Polska ID karta" z 7. osi priorytetowej „Społeczeństwo informacyjne – budowa elektronicznej administracji" Programu Operacyjnego Innowacyjna Gospodarka 2007-2013.

[33] Zarządzenia Burmistrza Dzierżoniowa nr 26/2012 z 29.02.2012 r. oraz 14/2013 z 01.02.2013 r.

[34] Awarie zasilania, sprzętu, systemów, baz danych i/lub aplikacji.

[35] Wpływ danych z systemów, włamania do systemów, infekcje wirusowe, kradzież danych przez pracownika, świadome niepożądane działania pracowników.

[36] Trudność wymiany informacji z systemami już działającymi, wymagania systemowe i sprzętowe oraz brak rozwoju oprogramowania i wsparcia technicznego dla wdrażanej aplikacji.

[37] Uprawnienie to zlikwidowano w trakcie kontroli NIK, tj. 14.07.2014 r.

W pozostałych przypadkach, tj. pracowników, którzy byli a aktualnie nie są zatrudnieni, Urząd usunął lub zablokował ich dostęp do systemów IT i poczty elektronicznej.

(dowód: akta kontroli str. 146, 152-158, 237, 240-242)

Główny specjalista informatyki Urzędu wyjaśnił, że wniosek o zarejestrowanie użytkownika systemów informatycznych nie jest obligatoryjny bowiem w Instrukcji zarządzania systemem informatycznym służącym do przetwarzania danych osobowych Urzędu (w § 7 pkt 5) ustalono, że Administrator Systemów Informatycznych, na wniosek kierownika komórki organizacyjnej użytkownika powinien zdefiniować poziom uprawnień określony w § 7 pkt 3. Według Głównego specjalisty informatyki Urzędu w ww. Instrukcji brak jest precyzyjnego zapisu co do formy powyższego wniosku a zasadę pisemności wprowadzono dla usprawnienia pracy Administratora Systemów Informatycznych i to tylko w przypadku użytkowników, którzy pracują w systemach służących do przetwarzania danych osobowych. Ponadto Główny specjalista informatyki Urzędu wyjaśnił, że nie zablokowano dostępu do poczty elektronicznej A[...] C[...]-S[...] *„z uwagi na możliwość kontynuacji spraw na tym stanowisku"*.

(dowód: akta kontroli str. 237)

W badanym okresie, stosownie do § 20 ust. 2 pkt 6 *rozporządzenia KRI*, przeprowadzono 20 szkoleń pracowników zaangażowanych w proces przetwarzania informacji, w którym wzięło udział od jednej do 16 osób. Wszystkie ww. szkolenia adresowane były do informatyków, przy czym 12 z nich poświęcono m.in. stosowaniu środków zapewniających bezpieczeństwo informacji. W niektórych z ww. 12 przypadków, temat szkolenia rozszerzono o wiedzę nt. zagrożeń bezpieczeństwa informacji (trzy szkolenia) oraz skutków naruszenia bezpieczeństwa informacji, w tym odpowiedzialności karnej (jedno szkolenie).

(dowód: akta kontroli str. 146, 198-200)

Z uwagi na przyjętą w Urzędzie praktykę, w okresie od 31 maja 2012 r. do 14 lipca 2014 r. nie stosowano pracy poza Urzędem. Jednak w Urzędzie ustalono minimalne zasady w zakresie bezpiecznej pracy użytkowników przy wykorzystaniu komputerów przenośnych.

W dniu 15 lipca 2014 r., tj. w trakcie trwania kontroli, pismem okólnym nr 71/2014 Burmistrz Miasta Dzierżoniowa wprowadził do stosowania Regulamin korzystania z urządzeń mobilnych poza obszarem przetwarzania danych osobowych Urzędu. W powyższym regulaminie ustalono m.in., że: (1) urządzenie mobilne może być udostępniane pracownikowi w celu związanym z wykonywaniem przez niego obowiązków służbowych, wynikających z jego zakresu obowiązków i może być wykorzystywane przez pracownika wyłącznie do celów służbowych, (2) obowiązuje całkowity zakaz posługiwania się oprogramowaniem nielegalnym, (3) nie należy podłączać urządzeń mobilnych, zawierających dane osobowe do sieci bezprzewodowych poza Urzędem oraz (4) użytkownik urządzenia mobilnego z systemem Windows powinien co najmniej raz na 14 dni podłączać urządzenie do sieci Urzędu, celem pobrania niezbędnych poprawek i aktualizacji do oprogramowania zainstalowanego na urządzeniu oraz utrzymania relacji zaufania i zmiany hasła komputera.

(dowód: akta kontroli str. 146, 201-202, 269-273)

Dla prawidłowego funkcjonowania wybranych systemów informatycznych w umowach ich zakupu, zawartych z dostawcami lub producentami, zapewniono serwis gwarancyjny związany z ich utrzymaniem (SIDAS EZD do 27 listopada 2012 r., SIDAS Repozytorium do 14 marca 2014 r., eDIOM do 24 marca 2014 r., NDZ+ do 17 kwietnia 2014 r., iArkusz do 31 grudnia 2014 r. oraz SYSTEmEG –

12 m-cy licząc od dnia sporządzenia i podpisania protokołu zdawczo-odbiorczego wdrożenia Programu[38]). Z uwagi na zakup tylko oprogramowania, w żadnej z ww. umów nie zawarto zapisu dotyczącego demontażu nośników w przypadku serwisu komputerów. Ponadto, w trzech ww. umowach (eDIOM, SIDAS Repozytorium oraz NDZ+) dostawcy nie zostali zobowiązani do zachowania tajemnicy informacji, do której mogli mieć dostęp w związku ze świadczeniem serwisu gwarancyjnego.

W przypadku SIDAS EZD oraz SIDAS Repozytorium Urząd podpisał umowę, której przedmiotem był serwis ww. systemów (do 29 listopada 2014 r.), a w której, podobnie jak w umowach zakupu, zawarto zapisy zobowiązujące firmę serwisującą do zachowania tajemnicy informacji przetwarzanych w ww. systemach.

(dowód: akta kontroli str. 146, 252-257)

W Urzędzie, stosownie do § 20 ust. 2 pkt 13 *rozporządzenia KRI*, w rozdziale V Polityki bezpieczeństwa danych osobowych, wprowadzono regulacje dotyczące zgłaszania incydentów naruszenia bezpieczeństwa informacji. Z ww. regulacjami zapoznano pracowników Urzędu[39], co zostało odnotowane i potwierdzone w ich aktach osobowych.

(dowód: akta kontroli str. 146-151)

W latach 2012-2014, stosownie do § 20 ust. 2 pkt 14 *rozporządzenia KRI*, przeprowadozno trzy audyty z zakresu bezpieczeństwa inforamcji (z których sporządzono raporty w dniu 14 lutego 2012 r., 21 października 2013 r. oraz 30 kwietnia 2014 r.).

Sformułowane wnioski w ramach przeprowadzonego audytu, z którego sporządzono raport w dniu 14 lutego 2012 r. zostały zrealizowane. W przypadku wniosków z audytu z 30 kwietnia 2014 r. - wnioski 2 i 3 zrealizowano a wniosek nr 1 jest nadal w realizacji (nie wszystkie karty stanowiskowe zostały uzupełnione[40]).

(dowód: akta kontroli str. 146, 211-235)

Zasady tworzenia kopii zapasowych danych i oprogramowania aplikacyjnego, w którym przetwarzane są dane ustalono w Instrukcji zarządzania systemem informatycznym służącym do przetwarzania danych osobowych[41]. Zgodnie z pkt 1 i 2 załącznika nr 4 do ww. instrukcji kopie zapasowe m.in. badanych systemów informatycznych tworzono w Urzędzie codziennie (bazy danych) oraz raz w tygodniu (oprogramowanie aplikacyjne). Ponadto, stosownie do pkt 3 ww. załącznika, powyższe kopie raz w miesiącu deponowano w sejfie na nośnikach zewnętrznych (magnetycznych lub optycznych). Wszystkie kopie zapasowe (tworzone codziennie, raz w tygodniu oraz raz miesiącu) tworzono i przechowywano, stosownie do § 29 ww. instrukcji, w odpowiednio zabezpieczonych pomieszczeniach, odrębnych od pomieszczeń, w których przechowywane były zbiory danych eksploatowanych na bieżąco. Dodatkowo, kontrolę poprawności wykonania kopii zapasowych losowo wybranych baz danych i serwerów dokonywano raz w miesiącu, przed utworzeniem kopii miesięcznej deponowanej w sejfie. W ten sposób ww. system spełniał wymogi § 20 ust. 2 pkt 12 lit. b *rozporządzenia KRI*, dzięki czemu minimalizowano ryzyko utraty informacji w wyniku awarii.

(dowód: akta kontroli str. 105-137, 146)

Badane systemy informatyczne udostępniały dane w następujących formatach: (1) SIDAS EZ i SIDAS REPOZYTORIUM - pdf, xls, csv, html lub xml, (2a) eDIOM –

---

[38] Program SYSTEmEG nie został jeszcze wdrożony.

[39] Badaniu poddano akta osobowe 19 pracowników spośród 98 zatrudnionych w okresie od 31.05.2012 r. do 31.05.2014 r.

[40] Termin realizacji wniosku ustalono na dzień 31.07.2014 r.

[41] Wprowadzonej w badanym okresie zarządzeniami Burmistrza Dzierżoniowa nr 252/2011 z dnia 18.05.2011 r. i nr 382/2012 z dnia 13.07.2012 r.

xls, OpenOffice Calk, QPR, (2b) eDIOM ZPD – xls, OpenOffice Calk, xml, (2c) MapView Desktop i eDIOM OR – xls, OpenOffice Calk, dbf, html, txt, shp, dxf, dgn, geobase, pdf, png, jpg, tiff, bmp, dmp, (3) NDZ – rtf, xml, txt, (4) iArkusz – pdf, xml, (5) SystemEG – xml, csv, pdf, xls. Tym samym spełniony został warunek określony w załączniku nr 2 do *rozporządzenia KRI* o możliwości zapisywania danych w co najmniej w jednym z formatów wymienionych w KRI.

(dowód: akta kontroli str. 146)

Ustalone nieprawidłowości

W działalności kontrolowanej jednostki w zakresie wdrożenia systemu zarządzania bezpieczeństwem systemów informatycznych stwierdzono następujące nieprawidłowości:

- nie opracowano i nie wdrożono Polityki Bezpieczeństwa Informacji obejmującej swym zakresem wszystkie informacje przetwarzane w Urzędzie,
- nie zablokowano konta użytkownika systemu poczty elektronicznej, pomimo iż nie był on pracownikiem Urzędu od dnia 1 stycznia 2014 r., co było niezgodne z § 20 ust. 2 pkt 5 *rozporządzenia KRI*, w myśl którego zarządzanie bezpieczeństwem informacji realizowane jest w szczególności poprzez niezwłoczną zmianę uprawnień w przypadku zmiany zadań pracowników,
- nie zapewniono szkoleń w zakresie bezpieczeństwa informacji osobom zaangażowanym w proces przetwarzania informacji, innym niż informatycy, co było niezgodne z § 20 ust. 2 pkt 6 *rozporządzenia KRI*,
- nie ustalono zasad (procedur) gwarantujących bezpieczną pracę przy przetwarzaniu mobilnym i pracy na odległość, co było niezgodne z § 20 ust. 2 pkt 8 *rozporządzenia KRI*,
- w trzech umowach (eDIOM, SIDAS Repozytorium oraz NDZ+) dostawcy nie zostali zobowiązani do zachowania tajemnicy informacji, do której mogli mieć dostęp w związku ze świadczeniem serwisu gwarancyjnego, co było niezgodne z postanowieniami z § 20 ust. 2 pkt 10 *rozporządzenia KRI*.

Ocena cząstkowa

Najwyższa Izba Kontroli ocenia pozytywnie mimo stwierdzenia nieprawidłowości[42] działalność kontrolowanej jednostki w zakresie wdrożenia systemu zarządzania bezpieczeństwem systemów informatycznych.

3. Zapewnienie dostępności informacji dla osób niepełnosprawnych

Opis stanu faktycznego

W toku kontroli dokonano weryfikacji zgodności strony internetowej Urzędu Miejskiego w Dzierżoniowie[43] oraz strony BIP[44] Urzędu ze standardem WCAG 2.0 (służącym dostosowaniu treści na stronie internetowej do potrzeb osób niepełnosprawnych). W jej wyniku ustalono, że na stronie internetowej Urzędu wystąpiło sześć błędów i dwa ostrzeżenia (w badaniu z wykorzystaniem narzędzia dostępnego na stronie http://validator.w3.org) oraz 35 błędów i 170 ostrzeżeń (w badaniu z wykorzystaniem narzędzia dostępnego na stronie http://jigsaw.w3.org/css-validartor/). Na stronie BIP Urzędu wystąpiły dwa błędy (http://validator.w3.org) oraz osiem błędów i jedno ostrzeżenie (http://jigsaw.w3.org/css-validartor/).

(dowód: akta kontroli str. 61-75)

Z-ca Burmistrza Miasta Dzierżoniowa wyjaśnił, że strona internetowa Urzędu jest dziś dostosowana do potrzeb osób niepełnosprawnych pod kątem najważniejszych

[42] Najwyższa Izba Kontroli stosuje 3-stopniową skalę ocen: pozytywna, pozytywna mimo stwierdzonych nieprawidłowości, negatywna.
[43] http://www.dzierzoniow.pl
[44] http://bip.um.dzierzoniow.pl/

zasad i funkcjonalności ułatwiających korzystanie z serwisu[45]. Zaznaczył jednak, że prace dostosowujące serwis do potrzeb osób niepełnosprawnych prowadzone są w oparciu o cykliczny przegląd, w którego trakcie sprawdzany jest również stopień dostosowania do takich potrzeb. Prace te zakończą się przed upływem wymaganego terminu (31 maja 2015 r.), natomiast czynności eliminujące błędy dotyczące m.in. właściwości progid, błędu parsowania są w toku i część z nich zakończy się przed zakończeniem kontroli NIK.

(dowód: akta kontroli str. 83-85)

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[46], wnosi o:

1. Podjęcie działań na rzecz opracowania i wdrożenia Polityki Bezpieczeństwa Informacji określającej zasady bezpieczeństwa wszystkich informacji przetwarzanych w Urzędzie.
2. Podjęcie skutecznych działań organizacyjnych celem zapobiegania dokonywania zamian w dokumentach strategicznych Urzędu w formie innej niż zostały uchwalone.
3. Identyfikację potrzeb mieszkańców w zakresie promocji komunikacji elektronicznej, tj. potrzeb dotyczących m.in. treści ewentualnych reklam usług elektronicznych świadczonych przez Urząd.
4. Podjęcie działań na rzecz promocji komunikacji elektronicznej z Urzędem.
5. Wprowadzenie, w przypadku korespondencji wytwarzanej wewnątrz Urzędu (w ramach tzw. procedowania sprawy), w pełni elektronicznego systemu prowadzenia spraw.
6. Opracowanie, dla wszystkich świadczonych przez Urząd usług elektronicznych, kart ich opisów, zawierających informacje o możliwości załatwienia sprawy drogą elektroniczną, oraz o sposobie zgłaszania awarii i o osobach/komórkach/ podmiotach odpowiedzialnych za ich usuwanie.
7. Przeprowadzanie dla wszystkich pracowników zaangażowanych w proces przetwarzania informacji szkoleń poświęconych stosowaniu środków zapewniających bezpieczeństwo informacji.
8. Wprowadzenie, w przypadku nowych umów serwisu komputerowego i/lub oprogramowania, klauzuli zobowiązujących dostawcę/producenta/serwisanta do zachowania tajemnicy informacji, do której będą mieli dostęp w trakcie wykonywania prac serwisowych, jak również wprowadzenie zapisów dotyczących demontażu nośników w przypadku prac serwisowych poza Urzędem.

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

[45] tj.m.in. korzystanie z opcji „wersji tekstowej", „wysokiego kontrastu", zwiększenia czcionki i samego rozmiaru strony oraz obsługi programów pozwalających na czytanie treści przy użyciu programów czytających, którymi posługują się osoby niewidome i niedowidzące

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

pokontrolnego, w terminie 21 dni od dnia jego przekazania. Zastrzeżenia zgłasza się do dyrektora Delegatury NIK we Wrocławiu.

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:
Joanna Marczyk
Główny specjalista k.p.

Podpis

Dyrektor

DYREKTOR
Delegatura Najwyższej Izby Kontroli
we Wrocławiu
z up.
Zenon Fiderkowski
Wicedyrektor