NAJWYŻSZA IZBA KONTROLI
Delegatura w Łodzi

LLO. 410.009.03.2020

Pan
Jacek Lipiński
Burmistrz Aleksandrowa Łódzkiego
Plac Kościuszki 2,
95-070 Aleksandrów Łódzki

WYSTĄPIENIE POKONTROLNE

P/20/004 – Realizacja usług publicznych dla obywateli z wykorzystaniem platformy ePUAP

NAJWYŻSZA IZBA KONTROLI
Delegatura w Łodzi
ul. Kilińskiego 210, 90-980 Łódź
T +48 42 239 32 00, F +48 42 239 32 90
llo@nik.gov.pl

I. Dane identyfikacyjne

Jednostka kontrolowana	Urząd Miejski w Aleksandrowie Łódzkim[1], Plac Kościuszki 2, 95-070 Aleksandrów Łódzki
Kierownik jednostki kontrolowanej	Jacek Lipiński, Burmistrz Aleksandrowa Łódzkiego[2] od dnia 22 listopada 2002 r.
Zakres przedmiotowy kontroli	Świadczenie przez urzędy j.s.t. e-usług. Rozwiązania organizacyjne i techniczne w zakresie zapewnienia bezpieczeństwa przetwarzania informacji w urzędzie i ich stosowanie.
Okres objęty kontrolą	Lata 2016-2020 (do dnia zakończenia kontroli).
Podstawa prawna podjęcia kontroli	Art. 2 ust. 2 ustawy z dnia 23 grudnia 1994 r. o Najwyższej Izbie Kontroli[3]
Jednostka przeprowadzająca kontrolę	Najwyższa Izba Kontroli Delegatura w Łodzi
Kontroler	Agnieszka Tomalska, główny specjalista kontroli państwowej, upoważnienie do kontroli nr LLO/102/2020 z 1 lipca 2020 r.

(dowód: akta kontroli str.1-2)

II. Ocena ogólna[4] kontrolowanej działalności

OCENA OGÓLNA

Najwyższa Izba Kontroli ocenia, że w latach 2016-2020 (I połowa) Urząd Miejski w Aleksandrowie Łódzkim sprawnie realizował usługi, w sprawie których obywatele składali wnioski za pośrednictwem platformy ePUAP[5] oraz przyjął rozwiązania techniczne, dzięki którym zapewnił w wymaganym stopniu bezpieczeństwo przetwarzania informacji.

Uzasadnienie oceny ogólnej

Prowadzona w Urzędzie ewidencja sprzętu i oprogramowania komputerowego, przedstawiała bieżącą informację o zasobach informatycznych, a użytkownicy systemów informatycznych nie posiadali uprawnień administracyjnych. W przypadku większości pracowników, którzy zakończyli zatrudnienie w Urzędzie, dostęp systemów informatycznych blokowany był niezwłocznie po rozwiązaniu stosunku pracy.

Zaangażowani w proces przetwarzania informacji pracownicy Urzędu zostali w okresie dwóch ostatnich lat[6] objęci szkoleniami wymaganymi § 20 ust. 2 pkt 6 rozporządzenia 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[7] (dalej: Rozporządzenie KRI).

---

[1] Dalej: „Urząd".
[2] Dalej „Burmistrz".
[3] Dz. U. z 2020 r. poz. 1200, dalej: „ustawa o NIK".
[4] Najwyższa Izba Kontroli formułuje ocenę ogólną jako ocenę pozytywną, ocenę negatywną albo ocenę w formie opisowej.
[5] Ogólnopolska platforma teleinformatyczna, zapewniająca ustandaryzowaną komunikację m.in. pomiędzy obywatelami a administracją samorządową oraz pomiędzy urzędami administracji publicznej.
[6] Tj. od 1 lipca 2018 r. do 30 czerwca 2020 r.
[7] Dz. U. z 2017 r. poz. 2247.

W działalności Urzędu stwierdzono nieprawidłowości. W szczególności:

- nie ustanowiono i nie wdrożono kompleksowego Systemu Zarządzania Bezpieczeństwem Informacji (dalej: SZBI), wynikającego z § 20 ust. 1, w związku z § 20 ust. 3 rozporządzenia KRI, a obowiązujące w tym zakresie polityki i instrukcje, opracowane były na podstawie przepisów o ochronie danych osobowych i głównie dotyczyły ochrony tych danych oraz regulacji w zakresie dostępu do pomieszczeń;
- w latach 2017-2018 nie przeprowadzano audytu bezpieczeństwa informacji wymaganego na podstawie § 20 ust. 2 pkt 14 Rozporządzenia KRI;
- w jednym przypadku zmiana uprawnień dostępu do zasobów komputera została przeprowadzona z opóźnieniem 11 dni, co stanowiło naruszenie § 20 ust. 2 pkt 5 rozporządzenia KRI.

Ponadto, w dziewięciu przypadkach (z 15 objętych badaniem) zmiany uprawnień dostępu do zasobów komputera dokonano z naruszeniem procedury określonej w wewnętrznych przepisach Urzędu.

III. Opis ustalonego stanu faktycznego

Opis stanu faktycznego

1. Rozwój e-usług stanowił jeden z kierunków działań wymienionych w Strategii rozwoju gminy Aleksandrów Łódzki na lata 2014-2020[8] (cel strategiczny „Poprawa dostępności komunikacyjnej", cel operacyjny „Rozwój społeczeństwa informacyjnego"). W opisie kierunku podano, że cyfryzacja usług publicznych ma na celu wzmocnienie komunikacji jednostek samorządu gminnego z otoczeniem, a wykorzystanie nowoczesnych technologii i Internetu ma na celu usprawnienie procesów administracyjnych, w tym obsługi klientów.

Rozwój e-usług oraz upowszechnianie elektronicznej obsługi ludności publicznych ujęto również w ramach celu strategicznego „Rozwój aktywności społeczności lokalnej" (cel operacyjny: „Wzmacnianie potencjału i skuteczności administracji publicznej", kierunek działania: „Usprawnianie procesów zarządzania w administracji publicznej"). W Strategii nie ustanowiono mierników stopnia realizacji tych celów.

(dowód: akta kontroli str. 11-46)

2. Według stanu na dzień 31 maja 2020 r. za pośrednictwem platformy ePUAP Urząd udostępniał obywatelom łącznie 39 usług, w kategoriach:

- „Sprawy obywatelskie (dowody osobiste, meldunki, wybory)" – łącznie 20 usług[9],
- „Podatki i opłaty" – siedem usług[10],
- „Pismo ogólne, Skargi, wnioski, Zapytania do urzędu" – łącznie trzy usługi[11],
- „Budownictwo, architektura, urbanistyka" – dwie usługi[12],
- „Urodzenia, małżeństwa, zgony" – dwie usługi[13],
- „Geodezja, kartografia" – jedną usługę[14],
- „Gospodarka komunalna" – jedną usługę[15],
- „Bezpieczeństwo i zarządzanie kryzysowe" – jedną usługę[16].

---

[8] Przyjętej Uchwałą Nr VIII/77/15 Rady Miejskiej w Aleksandrowie Łódzkim z dnia 30 kwietnia 2015 r.

[9] W tym: dowody osobiste (sześć usług), wybory (dziewięć usług), meldunki (pięć usług).

[10] W tym informacje o: lasach, gruntach, nieruchomościach i obiektach budowlanych oraz deklaracje na podatek: leśny, rolny, od nieruchomości, od środków transportu.

[11] Po jednej z każdego rodzaju.

[12] W tym: wydanie wypisu i wyrysu ze studium uwarunkowań i kierunków zagospodarowania przestrzennego oraz wypisu i wyrysu z miejscowego planu zagospodarowania przestrzennego.

[13] W tym: wnioskowanie o wydaniu odpisu aktu stanu cywilnego oraz zgłoszenie urodzenia dziecka.

[14] Ustalenie numeru porządkowego budynku.

[15] Deklaracja o wysokości opłaty za gospodarowanie odpadami komunalnymi.

[16] Wniosek o zasiłek powodziowy w kwocie do 2 tys. zł.

– „Inne" – dwie usługi.

Ponadto Urząd udostępniał usługi elektroniczne z wykorzystaniem serwisu Elektronicznego Biura Obsługi Interesanta Urzędu (e-BOI), zamieszczonego na stronie internetowej Urzędu[17]. Katalog spraw możliwych do załatwienia na stronie e-BOI obejmował:

– „Moje sprawy", gdzie interesant mógł sprawdzić, na jakim etapie realizacji znajduje się jego konkretna sprawa (dotyczy spraw wyłącznie złożonych za pośrednictwem platformy e-BOI);
– „Do zapłaty" - po powiązaniu konta e-BOI i konta podatkowego (na wniosek interesanta), interesant mógł przeglądać kartotekę podatkową zawierającą informacje dotyczące rozliczeń należności oraz składników stanowiących podstawę naliczenia tych należności[18];
– „Wyślij wniosek", gdzie interesant mógł złożyć wniosek o wypis i wyrys z miejscowego planu zagospodarowania przestrzennego (też w wersji uproszczonej) oraz o wydanie zaświadczenia o przeznaczeniu w miejscowym planie zagospodarowania przestrzennego działki.

Dodatkowo, istniała możliwość skorzystania przez obywateli z usług Urzędu świadczonych przez ePUAP, za pośrednictwem portalu Wrota Regionu Łódzkiego[19].

(dowód: akta kontroli str. 11-17, 47-49, 259-275, 665)

3. W pierwszym półroczu 2020 r. za pośrednictwem e-PUAP w Urzędzie zrealizowano 1.642 usługi elektroniczne, z czego:

– 223 usługi w okresie od 1 stycznia 2020 r. do 28 lutego 2020 r.,
– 584 usługi w okresie od 1 marca 2020 r. do 30 kwietnia 2020 r.,
– 835 usług w okresie od 1 maja 2020 r. do 30 czerwca 2020 r.

Najwięcej spraw dotyczyło: dopisania do spisu wyborców (430 wniosków lub zawiadomień, tj. 26,2% wszystkich e-usług w tym okresie), spraw meldunkowych (253, tj. 15,4%) oraz wydania dowodu osobistego (237, tj. 14,4%). Pozostałe wnioski i zawiadomienia głównie dotyczyły: geodezji[20] (181, tj. 11%), pomocy społecznej (85, tj. 5,2%), gospodarki komunalnej[21] (84, tj. 5,1%) oraz podatków (55, tj. 3,3%).

Istotny wzrost zainteresowania e-usługami świadczonymi przez Urząd, nastąpił w okresie od 1 marca 2020 r. do 30 kwietnia 2020 r., tj. w początkowym okresie epidemii COVID-19 w Polsce (o ok. 162% w porównaniu z pierwszymi dwoma miesiącami roku). W tym czasie znacznie częściej występowano do Urzędu: w sprawach meldunkowych (wzrost o 768%), dotyczących rolnictwa (wzrost o 300%) oraz w sprawach dotyczących aktów stanu cywilnego (wzrost o 229%) i pomocy społecznej (wzrost o 207%). W trakcie kolejnych dwóch miesięcy (maj-czerwiec 2020 r.) liczba spraw kierowanych do Urzędu przez ePUAP była o 274% wyższa od złożonych na początku roku (styczeń-luty 2020 r.) i o 43% wyższa niż w miesiącach marzec-kwiecień 2020 r.

(dowód: akta kontroli str. 11-17, 50-53)

---

[17] https://aleksandrow-lodzki.pl/ dostęp na 8.07.2020 r.

[18] System e-BOI umożliwia integrację tylko z jednym kontem wymiarowym. W przypadku gdy osoba posiada oddzielne konta wymiarowe dla różnego rodzaju opłat, nie ma możliwości powiązania konta EBOI w taki sposób, aby wszystkie konta były dostępne z poziomu e-BOI.

[19] Utworzonego w ramach projektu „Budowa Zintegrowanego Systemu e-Usług Publicznych Województwa Łódzkiego (Wrota Regionu Łódzkiego)"; https://elodzkie.pl/urzad/urzad-miasta-i-gminy-aleksandrow-lodzki (dostęp 8.07.2020 r.).

[20] Dot. m.in. stanu prawnego nieruchomości, wniosków o wypis i wyrys z miejscowego planu zagospodarowania przestrzennego, ewidencji gruntów, nabycia gruntu, przeznaczenia gruntu, numeru porządkowego nieruchomości.

[21] Dotyczy odpadów.

4. Urząd nie prowadził monitoringu poziomu wykorzystania e-usług realizowanych poprzez ePUAP. Jak wyjaśniła Sekretarz Gminy (z up. Burmistrza), dotychczas nie było takiej potrzeby, a wszystkie zgłoszenia procedowane są w sposób analogiczny do wpływających drogą tradycyjną. Aktualnie wykorzystywany system pozwala na sporządzanie statystyk w dowolnym momencie poprzez wygenerowania danych do programu Excel.

(dowód: akta kontroli str. 11-17, 54)

5. W okresie objętym kontrolą do Urzędu nie wpłynęły skargi i wnioski dotyczące świadczenia usług publicznych w formie elektronicznej lub usprawnienia tej formy komunikacji.

(dowód: akta kontroli str. 11-17, 73)

6. Zgodnie z zarządzeniem Burmistrza[22] podstawowym sposobem dokumentowania przebiegu załatwiania i rozstrzygania spraw był system tradycyjny, o którym mowa w § 1 załącznika nr 1 do rozporządzenia w sprawie instrukcji kancelaryjnej[23], wspomagany przez System Elektronicznego Obiegu Dokumentów PROTON. Urząd nie opracował własnej instrukcji kancelaryjnej, a podczas bieżącej pracy stosował zasady określone w ww. rozporządzeniu.

Szczegółowe zasady postępowania z wypływającymi do Urzędu dokumentami, w tym elektronicznymi, określono w procedurze „Nadzór nad dokumentami i zapisami" utworzonej w ramach Systemu Zarządzania Jakością. Zgodnie z jej treścią, dokumenty kierowane do Urzędu drogą pocztową i elektroniczną przyjmowane są przez pracownika sekretariatu Burmistrza, podlegają rejestracji przez pracownika Wydziału Obsługi Mieszkańców w „Dzienniku korespondencji" i przekazywane są do dekretacji, natomiast korespondencja wychodząca z Urzędu wysyłana jest przez odpowiednie komórki organizacyjne pocztą tradycyjną i pocztą elektroniczną, wg zasad określonych w ww. rozporządzeniu w sprawie instrukcji kancelaryjnej.

(dowód: akta kontroli str. 11-17, 74-77)

W stanu na dzień 30 czerwca 2020 r. podpis elektroniczny w urzędzie posiadało 17 osób, a profil zaufany 44 osoby.

W okresie od 1 stycznia 2020 r. do 30 czerwca 2020 r. z wykorzystaniem podpisu elektronicznego do petentów wysłanych zostało łącznie 238 pism: 49 przez Burmistrza, 167 przez Zastępcę Burmistrza, trzy przez Przewodniczącą Rady Miejskiej w Aleksandrowie Łódzkim, a dwa przez Kierownika USC. Ponadto, podpis ten wykorzystywany był przez pracowników Wydziału Finansowego (obsługa systemów: Bestia i Płatnik oraz do wysyłki JPK), Rejestracji Działalności Gospodarczej (obsługa CEIDG) oraz Wydziału Edukacji, Kultury i Sportu (obsługa systemów Empatia i Płatnik).

Z wykorzystaniem profilu zaufanego wysłane zostały łącznie 703 pisma, głównie przez pracowników Wydziału Organizacji i Spraw Obywatelskich (691).

(dowód: akta kontroli str. 11-17, 78-80)

W praktyce korespondencja wpływająca do Urzędu poprzez platformę ePUAP była:

1) rejestrowana przez pracownika sekretariatu,
2) drukowana i przedkładana Zastępcy Burmistrza do dekretacji,

---

[22] Zarządzenie Burmistrza Aleksandrowa Łódzkiego nr 98/2011 z dnia 4 sierpnia 2011 r. w sprawie zasad stosowania w Urzędzie Miejskim w Aleksandrowie Łódzkim 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.

[23] 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 (Dz. U. z 2011 r. Nr 14, poz. 67 ze zm.), zwane dalej rozporządzeniem w sprawie instrukcji kancelaryjnej".

3) Zastępca Burmistrza dekretował korespondencję na Naczelnika Wydziału/kierownika referatu, a ten – na pracownika merytorycznego,
4) pracownik merytoryczny dokonywał analizy sprawy oraz przygotował projekt pisma wychodzącego do akceptacji przez kierownika komórki organizacyjnej, a wersję elektroniczną ostatecznej odpowiedzi na pismo testowe umieścił w zasobie sieciowym (sieci wewnętrznej) w katalogu „Pisma do podpisu",
5) pismo podpisywane było podpisem kwalifikowanym,
6) ostateczna odpowiedź przygotowywana była w systemie PROTON, a do elementów wychodzących elektronicznie załączona była treść pisma oraz plik z ww. podpisem,
7) po wybraniu adresata i zmianie statusu pisma na czystopis, pismo podlegało autoryzacji podpisem zaufanym ePUAP przez osobę wysyłającą (pracownika merytorycznego),
8) po potwierdzeniu otrzymania pisma w systemie ePUAP, system generował Urzędowe Potwierdzenie Doręczenia, widoczne w systemie PROTON,
9) sprawa była skatalogowana wg Jednolitego Rzeczowego Wykazu Akt (JRWA), status sprawy zmieniony na „załatwiona", a pisma w wersji papierowej zostały umieszczone w wydziale merytorycznym.

Otrzymywane dokumenty były procedowane równolegle, tj. pracownik otrzymywał zarówno wersję elektroniczną dokumentu, jak i dokumentację papierową.

(dowód: akta kontroli str. 279-289)

W wyniku przeprowadzonego w 2018 r zadania audytowego „Elektroniczny obieg dokumentów w Urzędzie Miejskim w Aleksandrowie Łódzkim", Audytor Wewnętrzny Urzędu rekomendował zmianę używanego w Urzędzie systemu PROTON, z uwagi na brak stabilnej współpracy z systemem ePUAP oraz z funkcją podpisu elektronicznego. Jak wyjaśnił Audytor Wewnętrzny, po kalkulacji ewentualnych korzyści i kosztów zmiany systemu, zalecenie to nie zostało zrealizowane.

(dowód: akta kontroli str. 564-583)

7. Analiza 20 spraw[24] wpływających do Urzędu przez ePUAP w I półroczu 2020 r. wykazała, że:

- przekazanie wersji elektronicznej dokumentu do pracownika merytorycznego prowadzącego daną sprawę następowało w dniu złożenia dokumentu, kolejnym dniu roboczym lub w pięciu przypadkach[25] – najpóźniej czwartego dnia roboczego, zaś papierowej - najpóźniej piątego dnia roboczego[26];
- w jednym przypadku, w którym badany wniosek nie był kompletny (brak wniesionej opłaty), po wezwaniu przez Urząd Interesant złożył nowy wniosek i załączył niezbędne dokumenty;
- w jednym przypadku (złożony niewłaściwy formularz), Interesant złożył nowy wniosek w wyniku przeprowadzonej z pracownikiem Urzędu rozmowy telefonicznej;

---

[24] Do szczegółowego badania wybrano losowo próbę 20 spraw wnoszonych przez obywateli (osoby fizyczne), w formie elektronicznej poprzez ePUAP, w okresie pomiędzy 1 stycznia 2020 r. a 30 czerwca 2020 r.: trzy deklaracje o wysokości opłaty za gospodarowanie odpadami komunalnymi, deklaracja udziału w programie gromadzenia wód opadowych, cztery wnioski o wydanie wypisu i wyrysu z miejscowego planu zagospodarowania przestrzennego, dwa wioski o kierowanie korespondencji za pośrednictwem ePUAP, wniosek o wydanie zaświadczenia o wielkości użytków rolnych, wniosek o zarejestrowanie kota (program Koci Opiekun), deklaracja DN-1 na podatek od nieruchomości na rok 2020, informacja IN-1 o nieruchomościach i obiektach budowlanych, zapytanie w sprawie wysokości podatku rolnego na rok 2020, wniosek o umorzenie opłaty z tytułu powadzenia działalności gospodarczej, wniosek o dopisanie do spisu wyborców, wniosek o wydanie skróconego odpisu aktu stanu cywilnego, wniosek o wydanie dowodu oraz zgłoszenie zamiaru głosowania korespondencyjnego.

[25] Sprawy zadekretowane w wersji papierowej najpóźniej kolejnego dnia roboczego po dacie wpływu pisma.

[26] Sprawa zadekretowana i przekazana w systemie PROTON w dniu wpływu.

- system elektronicznego obiegu dokumentów w Urzędzie nie komunikował się automatycznie z innymi systemami informatycznymi Urzędu w zakresie przesyłania danych niezbędnych dla załatwienia sprawy. Tym niemniej, dla załatwienia spraw Urząd korzystał z danych gromadzonych zarówno w wewnętrznych[27], jak i zewnętrznych systemach[28] i nie żądał od wnioskodawców dodatkowych informacji w tym zakresie;
- załatwienie 19 badanych spraw nastąpiło w terminach wynoszących od 0 do 38 dni (średnio 10 dni) od daty wpływu kompletnego wniosku/pisma na platformę ePUAP, z czego jednej w terminie przekraczającym 30 dni.
  Sprawa ta dotyczyła złożonej w dniu 17 marca 2020 r. deklaracji o wysokości opłaty za gospodarowanie odpadami komunalnymi. Pismo informujące o zarejestrowaniu deklaracji i wysokości opłat, sporządzone z datą 19 marca 2020 r. i podpisane podpisem elektronicznym przez Zastępcę Burmistrza w dniu 24 marca 2020 r., zajmujący się sprawą pracownik Wydziału Inwestycji, Ochrony Środowiska i Rolnictwa wysłał do Interesanta dopiero w dniu 24 kwietnia 2020 r., tj. po 38 dniach od daty wpływu deklaracji. Wyjaśniając przyczyny opóźnienia, pracownik ten wskazał na utrudnienie w - możliwym wyłącznie w Urzędzie - dostępie do systemu PROTON, spowodowane wykonywaną w tym czasie, z uwagi na warunki pandemii, pracą w systemie rotacyjnym oraz obowiązujące w tym okresie przepisy ustawy z dnia 2 marca 2020 r. o szczególnych rozwiązaniach związanych z zapobieganiem, przeciwdziałaniem i zwalczaniem COVID-19, innych chorób zakaźnych oraz wywołanych nimi sytuacji kryzysowych[29]. Z uwagi na doręczenie pisma przed terminem płatności, powyższe opóźnienie nie miało wpływu na terminowość wniesienia opłaty za gospodarowanie odpadami.
  Jedna z badanych spraw (wydanie decyzji ustalającej wymiar podatku od nieruchomości) nie została zakończona do dnia kontroli z uwagi na nieotrzymanie przez Urząd wykazu zmian od Starosty Powiatowego w Zgierzu, prowadzącego ewidencję gruntów i budynków;
- uzyskanie informacji na temat aktualnego stanu procedowania sprawy możliwe było poprzez kontakt osobisty, mailowy lub telefoniczny, a w przypadku wniosku o dowód osobisty – aktualny stan sprawy dostępny jest na stronie obywatel.gov.pl lub jeśli wnioskodawca poda swój numer telefonu, dostanie powiadomienie smsowe z informacją o możliwości odebrania dowodu. Informacje te nie były udostępniane poprzez system PROTON, stronę bądź platformę internetową, pozwalającą na samodzielne śledzenie postępu sprawy przez obywatela. Żadna z wylosowanych spraw prowadzonych przez Wydział Geodezji i Gospodarki Przestrzennej nie została złożona przy wykorzystaniu systemu e-BOI. Próba sprawdzenia statusu przy użyciu funkcji: „Sprawdź status sprawy bez logowania" we wszystkich czterech przypadkach zwróciła komunikat: „Nie znaleziono sprawy/wniosku o podanym numerze".
  Żaden z interesantów, których sprawy zostały wylosowane do próby i były prowadzone przez Wydział Finansowy, nie posiadał zintegrowanego z systemem podatkowym konta EBOI;
- wszystkie wpływające wnioski zostały zarejestrowane w systemie PROTON, wydrukowane i przekazane do komórek merytorycznych w formie papierowej. Dwie sprawy (wniosek o dodanie do spisu wyborców i wniosek o wydanie dowodu osobistego) były całkowicie procedowane w formie elektronicznej,

---

[27] np. Gospodarka Odpadami Miasta i Gminy, Księgowość Zobowiązań Podatkowych, Podatki.
[28] m.in.: WebEwid, program geoinformacyjny QGIS, Rejestr Stanu Cywilnego, Rejestr PESEL, Rejestr Dowodów Osobistych ŹRÓDŁO, Rejestr Wyborców SELWIN, czy program obsługujący wybory WOW.
[29] Dz.U. z 2020 r. poz. 374 ze zm.

a trzy sprawy załatwiono w wyniku rozmowy telefonicznej. W pozostałych czternastu przypadkach przy prowadzeniu sprawy wspomagano się formą papierową dokumentów.

(dowód: akta kontroli str. 368-382, 665)

8. W latach 2016-2020 (I półrocze) wykorzystywana platforma ePUAP nie zawsze działała sprawnie i bezawaryjnie. Urząd czterokrotnie[30] dokonywał zgłoszeń, drogą mailową, do Centralnego Ośrodka Informatyki, w związku z napotkanymi problemami w funkcjonowaniu ePUAP i czterokrotnie[31] odbywał tą drogą konsultacje, w tym w zakresie wgrania nowego certyfikatu. Zgłaszane problemy zostały usunięte w ciągu od 2 dni do 4,5 miesiąca od daty zgłoszenia.
Z wyjaśnień Zastępcy Burmistrza (z up. Burmistrza) wynika, że powyższy termin usunięcia zgłoszonego problemu nie miał żadnego wpływu na terminowość załatwianej sprawy, bowiem zgłoszenie dotyczyło wygenerowanego dokumentu potwierdzenia. W dniu 18 lipca 2017 r. Urząd otrzymał z Centralnego Ośrodka Informatyki informację, iż przedmiotowe pismo zostało poprawnie dostarczone do użytkownika.

(dowód: akta kontroli str. 11-17, 56-72, 616-619)

9. System Elektronicznego Obiegu Dokumentów PROTON dostarczany był Urzędowi przez podmiot komercyjny. Umowy dotyczące korzystania z oprogramowania zawierane były w sposób zapewniający ciągłość dostępu do systemu. W ich treści określono rodzaje występujących kategorii zgłoszeń oraz czas na usunięcie zaistniałego problemu.
W latach 2016-2020 Urząd dziewięciokrotnie zgłaszał problemy w funkcjonowaniu przyjętego systemu dotyczące m.in. generowania raportów, błędnych statusów wysyłki oraz aktualizacji, synchronizacji i zawieszania się systemu. W ośmiu przypadkach błędy zostały usunięte w czasie do ośmiu dni od daty zgłoszenia, a w jednym – po upływie 5,5 miesiąca, z uwagi na rozwiązanie problemu przy kolejnej aktualizacji systemu.

(dowód: akta kontroli str. 11-17, 55, 290-333)

10. Aktualna na dzień prowadzenia kontroli NIK strona internetowa BIP Urzędu[32] posiadała odnośnik do Systemu Elektronicznej Skrzynki Podawczej[33], kierującego interesanta do ogólnopolskiego portalu ePUAP[34], wraz z informacją o możliwości podpisania dokumentu elektronicznie za pomocą podpisu zaufanego. Z kolei link zamieszczony w BIP Urzędu, w kategorii „Urząd Miejski w Aleksandrowie Łódzkim" w zakładce „Załatw sprawę przez ePUAP"[35] kierował do listy obejmującej wybrane kategorie spraw możliwych do załatwienia przez ePUAP oraz informacji jak korzystać z ePUAPu, w tym jak założyć konto użytkownika, natomiast w zakładce „Informacje ogólne – Dane podstawowe" opublikowany został (w formie linku) adres skrytki na ePUAP Urzędu[36].
Ponadto, jak wyjaśniła Naczelnik Wydziału Obsługi Mieszkańców, informacje o możliwości załatwienia spraw drogą elektroniczną udostępniane były w lokalnej prasie wydawanej przez Urząd i w lokalnej telewizji oraz podczas rozmów telefonicznych z interesantami.
Ostatnia aktualizacja strony miała miejsce 11 lutego 2015 r., co jak wynika z wyjaśnień Zastępcy Burmistrza (z up. Burmistrza), spowodowane było

---

[30] W dniach: 28.01.2017 r., 3.03.2017 r., 6.03.2017 r., 17.07.2018 r. (anulowane 3.09.2018 r.).
[31] W dniach: 17.04.2018 r., 16.01.2019 r., 13.05.2019 r. i 10.04.2020 r.
[32] https://aleksandrowlodzki.bip.net.pl/?c=454 (dostęp 14.07.2020 r.).
[33] https://aleksandrowlodzki.bip.net.pl/# (dostęp 14.07.2020 r.).
[34] https://epuap.gov.pl/wps/portal (dostęp 14.07.2020 r.).
[35] https://aleksandrowlodzki.bip.net.pl/?c=543 (dostęp 14.07.2020 r.).
[36] https://aleksandrowlodzki.bip.net.pl/?c=83 (dostęp 14.07.2020 r.).

niedopatrzeniem i brakiem zgłoszeń o potrzebie wykonania aktualizacji. Jednocześnie Zastępca Burmistrza podał, że prace związane z aktualizacją strony zostały już rozpoczęte.
Informacja o sprawach możliwych do załatwienia przy pomocy dowodu osobistego z warstwą elektroniczną oraz o sposobie uzyskania takiego dokumentu (ulotka „Co to jest e-DOWÓD?" do pobrania w formacie .pdf) zamieszczona była w zakładce „Urząd Miejski w Aleksandrowie Łódzkim » Sprawy w urzędzie » Wydział Organizacji i Spraw Obywatelskich » Dowody Osobiste".
Jak wynika z wyjaśnień Zastępcy Burmistrza (z up. Burmistrza), od 4 marca 2019 r. wszystkie dowody osobiste wydawane obywatelom posiadają warstwę elektroniczną w dowodzie, jest ona wgrywana podczas produkcji dowodu osobistego. Osoba składająca wniosek o wydanie dowodu osobistego, może wyrazić zgodę na zamieszczenie w dowodzie certyfikatu podpisu osobistego. Taką możliwość posiadają wyłącznie osoby, które ukończyły 13 rok życia. W związku z powyższym nie ma możliwości wydania dowodu bez warstwy elektronicznej.
Informacje dotyczące e-dowodu udzielane są przez urzędnika podczas składania wniosku o wyrobienie dowodu osobistego, ponadto dostępne są również ulotki dotyczące e-dowodu.

(dowód: akta kontroli str. 11-17, 81-85, 259-278, 618-660)

11. W badanym okresie pracownicy Urzędu uczestniczyli w szkoleniach w zakresie danych osobowych i bezpieczeństwa informacji. Były to zarówno prowadzone przez firmy zewnętrzne szkolenia zamknięte, jak i szkolenia wewnętrzne, prowadzone przez Administratora Bezpieczeństwa Informacji (ABI) od 6 sierpnia 2018 r przez Inspektora Ochrony Danych Osobowych (IOD). Na przykładzie 20 nowoprzyjętych pracowników stwierdzono, że przed przystąpieniem do pracy i nadaniem uprawnień do systemu informatycznego przeszli oni tzw. szkolenia stanowiskowe, przeprowadzane przez ABI/IOD.
W okresie od 1 lipca 2018 r. do 30 czerwca 2020 r. pracownicy Urzędu uczestniczyli w dziewięciu szkoleniach zewnętrznych z zakresu: ochrony danych osobowych i bezpieczeństwa danych, w tym informacji niejawnych (6 szkoleń), audytu bezpieczeństwa teleinformatycznego i wdrażania zabezpieczeń (1 szkolenie), przeciwdziałania zagrożeniom związanym z obsługą systemów informatycznych (1 szkolenie), czy obsługi platformy ePUAP (1 szkolenie). W powyższych formach podnoszenia kompetencji udział wzięło łącznie 77 pracowników Urzędu.
W ww. okresie IOD przeprowadził również dwa szkolenia wewnętrzne: w szkoleniu z zakresu ochrony informacji niejawnych przeprowadzonym we wrześniu 2019 r. uczestniczyło 27 osób, a w zorganizowanym w grudniu 2019 r. szkoleniu „Realizacja obowiązku informacyjnego wynikającego z RODO" - 90 pracowników.
Ponadto trzech pracowników ukończyło w powyższym okresie studia podyplomowe z zakresu: wykonywania funkcji inspektora ochrony danych (1 osoba w 2018 r.) oraz ochrony danych osobowych (1 osoba w 2018 r. i jedna w 2020 r.).

(dowód: akta kontroli str. 243-249, 383-486)

12. Obowiązujące w Urzędzie: Polityka bezpieczeństwa przetwarzania i ochrony danych osobowych i Instrukcja zarządzania system informatycznym służącym do przetwarzania danych osobowych[37] (dalej: *Polityka bezpieczeństwa* i *Instrukcja zarządzania systemem informatycznym*), ustanowione zostały na podstawie przepisów o ochronie danych osobowych[38].

---

[37] Wprowadzona Zarządzeniami Burmistrza Aleksandrowa Łódzkiego nr 1/2011 z dnia 4 stycznia 2011 r. i nr 146/2018 z dnia 6 sierpnia 2018 r.

[38] Ustawy o ochronie danych osobowych - w brzmieniu z dnia 29 sierpnia 1997 r. (Dz.U. z 2016 r. poz. 922 ze zm.) i z dnia 10 maja 2018 r. (Dz.U. z 2019 r. poz. 1781), rozporządzenia Ministra Spraw Wewnętrznych i Administracji z dnia 29 kwietnia 2004 w sprawie dokumentacji przetwarzania danych osobowych oraz

Innymi dokumentami regulującymi kwestię bezpieczeństwa i dostępu do przechowywanych w Urzędzie danych były:

- „Instrukcja postępowania z kluczami oraz zabezpieczenia pomieszczeń i obiektu Urzędu Miejskiego w Aleksandrowie Łódzkim"[39], obowiązująca od 14 marca 2017 r.,
- „Instrukcja postępowania w sytuacji naruszenia ochrony danych osobowych w Urzędzie Miejskim w Aleksandrowie Łódzkim"[40], obowiązująca od 27 lipca 2018 r.,
- „Polityka rachunkowości dla Gminy Aleksandrów Łódzki oraz jednostki budżetowej Urząd Miejski w Aleksandrowie Łódzkim"[41], określająca m.in. opis programowych zasad ochrony danych, metody zabezpieczenia dostępu do danych i systemu ich przetwarzania.

Dodatkowo w Urzędzie obowiązywały systemowe i procesowe procedury opracowane w ramach Systemu Zarządzania Jakością, w tym dotyczące zarządzania ryzykiem, nadzoru nad dokumentami, czy szkolenia pracowników.

Jak wynika z wyjaśnień Zastępcy Burmistrza (z up. Burmistrza), w Urzędzie każda polityka i instrukcja publikowana jest w Urzędowym serwisie intranetowym. Dużą część informacji pracownicy otrzymują z wykorzystaniem poczty elektronicznej. Ponadto, każdy z naczelników instruowany jest odnośnie nowych dokumentów obowiązujących w Urzędzie, a każdy podległy pracownik zobligowany jest przez swojego przełożonego do zapoznania się z nowymi dokumentami i stosowania ich zapisów.

IOD wyjaśniła, że w intranecie Urzędu zamieszcza materiały ze szkoleń oraz materiały związane z ochroną danych osobowych i bezpieczeństwem informacji, a ostrzeżenia przed atakami hakerskimi wysyła do pracowników za pośrednictwem poczty elektronicznej oraz za pomocą aplikacji Infonet Communicator. Dodatkowo wszelkie ważne informacje dotyczące bezpieczeństwa oraz przetwarzania danych, w tym o podejmowanych działaniach czy szkoleniach, przekazywane są na cotygodniowych naradach z kadrą kierowniczą Urzędu.

(dowód: akta kontroli str. 86-249, 616-618, 622-660)

13. Obowiązek zapewnienia aktualności regulacji wewnętrznych, wynikający z § 20 ust. 2 pkt 1 rozporządzenia KRI, zawarty został w § 4 Polityki bezpieczeństwa, jednak nie zakładał częstotliwości przeglądów dokumentacji. Obowiązek corocznej identyfikacji i oceny ryzyka oraz określenia metody przeciwdziałania ujęto w procedurze PS-4 „Zarządzanie ryzykiem".

Zarządzeniem Burmistrza nr 48/2010 z dnia 22 marca 2010 r. powołano Administratora Bezpieczeństwa Informacji[42] (od 6 sierpnia 2018 r. - Inspektora Ochrony Danych Osobowych[43]), a Zarządzeniem 146/2018 z dnia 6 sierpnia 2018 r. wyznaczono m.in. Administratora Bezpieczeństwa Systemów Informatycznych[44], realizującego zadania w zakresie bezpieczeństwa informatycznego.

(dowód: akta kontroli str. 116-201, 229-232, 243-249)

---

warunków technicznych i organizacyjnych, jakim powinny odpowiadać urządzenia i systemy informatyczne służące do przetwarzania danych osobowych (Dz.U. Nr 100 poz. 1024, uchylone z dniem 6 lutego 2019 r.), Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (Dz.U.UE.L.2016.119.1 ze zm.).

[39] Stanowiąca załącznik nr 1 do zarządzenia nr 22/2017 Burmistrza Aleksandrowa Łódzkiego z dnia 14 marca 2017 r.

[40] Wprowadzona Zarządzeniem nr 142/2018 Burmistrza Aleksandrowa Łódzkiego z dnia 27 lipca 2018 r.

[41] Wprowadzona Zarządzeniem nr 123/2017 2017 Burmistrza Aleksandrowa Łódzkiego z dnia 20 lipca 2017 r.

[42] Zwanego dalej: „ABI".

[43] Zarządzenie nr 147/2018 Burmistrza Aleksandrowa Łódzkiego z dnia 6 sierpnia 2018 r.

[44] Zwanego dalej: „ABSI".

Z dniem 18 października 2017 r. Burmistrz powołał[45] Zespół ds. opracowania systemu zarządzania bezpieczeństwem informacji, w skład którego wchodzili Administrator Bezpieczeństwa Informacji, Sekretarz Miasta i Gminy oraz Administrator Systemu Informatycznego. Zespół zobowiązany był m.in. do:

- dokonania diagnozy stanu organizacji w odniesieniu do spełnienia wymagań prawnych związanych z ochroną danych osobowych, w tym inwentaryzacji funkcjonującej w Urzędzie dokumentacji – w terminie do 30 listopada 2017 r.,
- przeglądu i określenia działań wymagających usprawnień – w terminie do 30 grudnia 2017 r.,
- opracowania niezbędnej dokumentacji bezpieczeństwa informacji – w terminie do 30 stycznia 2018 r.

Do dnia kontroli Zespół zrealizował dwa pierwsze zadania. Na posiedzeniu w dniu 29 grudnia 2017 r. przedstawił wyniki przeglądu i identyfikacji obszarów wymagających wprowadzenia zabezpieczeń technicznych i organizacyjnych oraz wskazał niezbędną do opracowania dokumentację, obejmującą:

- politykę bezpieczeństwa informacji Urzędu oraz - jako załącznik – instrukcję ochrony danych osobowych,
- instrukcję zarządzania bezpieczeństwem informacji w systemie informatycznym,
- instrukcję postępowania w sytuacji naruszenia danych osobowych,
- regulamin użytkownika systemów informatycznych.

Do dnia kontroli spośród ww. czterech pozycji opracowana i wdrożona została tylko Instrukcja postępowania w sytuacji naruszenia ochrony danych osobowych.

Zarządzeniem nr 154/2020 r. z dnia 11 września 2020 r., tj. w trakcie niniejszej kontroli, Burmistrz zmienił skład Zespołu i ostatni punkt harmonogramu jego pracy, wydłużając do 30 czerwca 2021 r. termin opracowania niezbędnej dokumentacji.

(dowód: akta kontroli str. 250-255)

Zarządzeniem 60/2018 z dnia 12 kwietnia 2018 r. Burmistrz powołał Zespół ds. wdrożenia Rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r., zobowiązany „za przygotowanie koncepcji systemu ochrony danych osób fizycznych i przepływu tych danych, w zgodzie z wymaganiami określonymi w RODO". Zespół ten, na początku 2019 r., przystąpił do prac związanych z szacowaniem ryzyka w przetwarzaniu danych osobowych. W tym celu zakupiono dostęp do platformy GDPR RISC Tracker i przeprowadzono w Urzędzie szacowanie ryzyka metodą uproszczonej analizy. Jak wynika z wyjaśnień Naczelnika Wydziału Organizacji w Spraw Obywatelskich, z uwagi na skomplikowany charakter czynności szacowania ryzyka oraz ilość wyodrębnionych czynności przetwarzania danych, zwłaszcza w systemach informatycznych, proces ten jest nadal realizowany (postęp prac szacuje się na 80%).

(dowód: akta kontroli str. 233-242, 256-258)

W 2018 r. dokonano aktualizacji Polityki bezpieczeństwa i – będącej dokumentem powiązanym – Instrukcji zarządzania systemem informatycznym. W treści tych dokumentów uwzględniono potrzebę ich dostosowania do zmienionych przepisów o ochronie danych osobowych oraz realizacji zaleceń Audytora Wewnętrznego. Naczelnicy wydziałów zobligowani zostali do szczegółowego opisu uprawnień, jakie mają być nadane pracownikom w systemie informatycznym oraz wprowadzono kartę obiegową przy zwalnianiu pracownika.

(dowód: akta kontroli str. 152-201, 501-504, 564-566)

---

[45] Zespół ds. opracowania systemu zarządzania bezpieczeństwem informacji w Urzędzie Miejskim w Aleksandrowie Łódzkim powołany Zarządzeniem nr 182/2017 Burmistrza Aleksandrowa Łódzkiego z dnia 18 października 2017 r.

14. Polityka bezpieczeństwa obejmowała zakresem m.in. organizację przetwarzania danych osobowych, w tym uregulowania dotyczące szkolenia w zakresie ochrony danych osobowych, a także: zasady aktualizacji, zadania Administratora systemów informatycznych[46], zadania Administratora bezpieczeństwa systemów informatycznych[47] oraz zasady odpowiedzialności pracowników i użytkowników systemu.

Natomiast w Instrukcji zarządzania systemem informatycznym określono m.in. ogólne zasady:

- dostępu do systemu informacyjnego, w tym zarządzania uprawnieniami użytkowników systemu i mechanizmami uwierzytelniającymi,
- bezpiecznej eksploatacji systemów informatycznych i ochrony przed niebezpiecznym oprogramowaniem,
- postępowania z nośnikami przenośnymi i komputerami przenośnymi,
- wymiany informacji w systemie informatycznym (w tym korzystania z Internetu i prywatnej poczty elektronicznej),
- komunikacji w sieci teleinformatycznej oraz połączenia z zewnętrznymi sieciami teleinformatycznymi,
- zarządzania mechanizmami kryptograficznymi,
- bezpiecznego serwisowania systemu informatycznego,

a także wymagania dotyczące sprzętu i oprogramowania, mechanizmy monitorowania działania składowych systemu oraz zasady wprowadzania zmian w systemie informatycznym.

(dowód: akta kontroli str. 116-201)

15. Prowadzona w Urzędzie ewidencja sprzętu IT w bazie konfiguracji komputerów oraz specjalistyczne oprogramowanie[48] pozwalały na uzyskanie bieżącej informacji o zasobach informatycznych, obejmującej ich rodzaj i konfigurację co było zgodne z § 20 ust. 2 pkt 2 Rozporządzenia KRI. Powyższa baza danych obejmowała wszystkie posiadane przez Urząd elementy IT, a dane o ich szczegółowej konfiguracji podlegały automatycznemu odświeżaniu. Ponadto, w skonfigurowanym na bazie SQL programie „Spis sprzętu" Urząd ewidencjonował m.in. takie informacje, jak: numer ewidencyjny, numer seryjny, miejsce użytkowania, dane osoby lub komórki organizacyjnej, do której przypisano odpowiedzialność za sprzęt, dane faktury, cenę zakupu, numer seryjny, adres IP oraz czy dany sprzęt jest przeznaczony do likwidacji.

Badanie, przeprowadzone na podstawie 15 pozycji zasobów informatycznych[49] wykazało, że powyższe oprogramowanie pozwalało na odnalezienie w nim informacji o danym zasobie informatycznym, a w przypadku komputerów i laptopów również o ich aktualnej konfiguracji. Dane dotyczące konfiguracji serwera były dostępne na stronie internetowej producenta, po podaniu numeru seryjnego sprzętu, zaś w przypadku routera i drukarki – na stronie konfiguracyjnej w sieci lokalnej.

---

[46] Dotyczące m.in. przeciwdziałania próbom naruszeń bezpieczeństwa danych osobowych, wykonywania czynności związanych ze sprawdzaniem systemu pod kątem obecności szkodliwego oprogramowania, monitorowania systemu komunikacji w sieci komputerowej i przesyłania danych za pośrednictwem urządzeń teletransmisji, dokonywanie napraw, konserwacji oraz likwidacji urządzeń komputerowych, na których zapisane są dane osobowe oraz przeglądu uprawnień użytkownikom systemu informatycznego.

[47] W tym: bieżący nadzór oraz zapewnienie optymalnej ciągłości działania systemu informatycznego, w tym opracowywanie procedur określających zarządzanie systemem informatycznym przetwarzającym dane osobowe, koordynacja procesu analizy ryzyka związanego z przetwarzaniem danych w systemie informatycznym, a także merytoryczne przygotowanie i przeprowadzenie szkoleń w zakresie bezpieczeństwa systemu informatycznego.

[48] IT Manager.

[49] W tym: 10 komputerów, dwa laptopy, jeden serwer, jeden router i jedna drukarka, dobrane w sposób celowy spośród łącznie: 146 szt. komputerów stacjonarnych i laptopów, 6 szt. serwerów, 44 szt. drukarek, 46 szt. kserokopiarek i 2 szt. routerów.

(dowód: akta kontroli str. 334-367)

16. Weryfikacja[50] możliwości zainstalowania nieautoryzowanego oprogramowania na komputerach użytkowanych przez pracowników, niebędących pracownikami służb informatycznych Urzędu wykazała, że we wszystkich przypadkach do dokończenia instalacji pliku na komputerach stacjonarnych żądane były uprawnienia administratora, natomiast laptop miał wyłącznie możliwość zdalnego przekierowania do zdalnego pulpitu osoby pracującej na nim (tunel VPN) i brak było na nim możliwości uruchomienia funkcji wymagających uprawnień administratora.

(dowód: akta kontroli str. 334-367)

17. Spośród 15 losowo zweryfikowanych kont pracowników, którzy w latach 2016-2020 rozwiązali stosunek pracy z Urzędem, w 13 przypadkach zmiana uprawnień dostępu do zasobów komputera była zrealizowana zgodnie z § 20 ust. 2 pkt 5 Rozporządzenia KRI – konta zostały wygaszone/zablokowane najpóźniej kolejnego dnia roboczego po rozwiązaniu stosunku pracy z pracownikiem. W jednym przypadku uprawnienia odebrano po upływie 11 dni, a w kolejnym (pracownik zatrudniony do 31 grudnia 2017 r. – brak było potwierdzenia odebrania uprawnień (zarówno w systemie informatycznym, jak i w formie papierowej).

Tym niemniej, w żadnym z kontrolowanych przypadków nie było możliwe zalogowanie na koncie pracownika w ramach domeny @alex.local w usłudze katalogowej Active Directory Windows Server 2012. Konta 13 osób były zablokowane, a dwóch – usunięte.

(dowód: akta kontroli str. 487-515)

Procedura nadawania, modyfikacji i odbierania uprawnień pracownikom określona została w obowiązujących w badanym okresie *Politykach bezpieczeństwa* i *Instrukcjach zarządzania systemem informatycznym*. Zgodnie z ich treścią, wszelkie zmiany winny być poprzedzone stosownymi wnioskami, składanymi do IOD (do 6 sierpnia 2018 r.) i Administratora Bezpieczeństwa Systemów Informatycznych[51] (od 6 sierpnia 2018 r.) przez kierowników poszczególnych komórek organizacyjnych.

Tylko w przypadku dwóch spośród 15 losowo zweryfikowanych kont pracowników, którzy w latach 2016-2020 rozwiązali stosunek pracy z Urzędem, odebranie uprawnień dostępu do zasobów komputera zostało poprzedzone takimi wnioskami. Cztery kolejne osoby miały uprawnienia nadane na czas określony, które wygasły po upływie tego czasu.

(dowód: akta kontroli str. 116-201, 487-515)

18. Audytor Wewnętrzny przeprowadził w 2016 r. zadanie zapewniające: „Realizacja obowiązków w zakresie bezpieczeństwa informacji w Urzędzie Miejskim w Aleksandrowie Łódzkim", ujęte w planie na 2015 r. W jego wyniku wydał 16 zaleceń, których realizację zweryfikowano w 2017 r., w formie czynności sprawdzających.

(dowód: akta kontroli str. 543-566)

W 2019 r., na zlecenie Urzędu, audytorzy firmy zewnętrznej (Elit Partner sp. z o.o.) przeprowadzili audyt IT bezpieczeństwa informacji, w tym danych osobowych. Celem audytu była weryfikacja wypełniania przez Urząd wymogów określonych w rozporządzeniu KRI. Audyt dotyczył głównie zgodności przetwarzanych danych osobowych z wymaganiami rozporządzenia Parlamentu Europejskiego i Rady Unii Europejskiej z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu

---

[50] Do próby wytypowano 10 komputerów, w tym: 9 komputerów stacjonarnych oraz 1 laptop, wybranych w sposób celowy, spośród komputerów będących na stanie Urzędu.

[51] Dalej: „ABSI".

takich danych (...)[52]. Stwierdzone nieprawidłowości dotyczyły m.in.: braku egzekwowania od pracowników pisemnych oświadczeń o zapoznaniu z przepisami o ochronie danych osobowych oraz o zachowaniu poufności, braku dowodów na realizację niektórych procedur, np. analizy ryzyka systemu informatycznego.

(dowód: akta kontroli str. 584-615)

Zaplanowanego na 2018 r. zadania audytowego „Realizacja obowiązków w zakresie bezpieczeństwa informacji" nie przeprowadzono m.in. z uwagi na absencję audytora i decyzję o zleceniu zadania firmie zewnętrznej w 2019 r. W latach 2017 i 2020 nie prowadzono zadań audytowych z zakresu bezpieczeństwa informacji.

(dowód: akta kontroli str. 516-542, 618-621)

Stwierdzone nieprawidłowości

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

1. W Urzędzie nie było opracowanej i wdrożonej polityki bezpieczeństwa informacji, o której mowa w § 20 ust. 1 w związku z ust. 3 rozporządzenia KRI[53]. Obowiązujące w Urzędzie: *Polityka bezpieczeństwa* i *Instrukcja zarządzania systemem informatycznym*, ustanowione zostały na podstawie przepisów o ochronie danych osobowych i - z założenia - ograniczały się do bezpieczeństwa danych osobowych.

   Wprawdzie Burmistrz powołał w dniu 18 października 2017 r. Zespół ds. opracowania systemu zarządzania bezpieczeństwem informacji i określił harmonogram jego zadań, jednak do dnia zakończenia niniejszej kontroli nie wyegzekwował ich pełnej realizacji.

   Wyjaśniając przyczyny tego stanu, Zastępca Burmistrza (z up. Burmistrza) przedstawił wyjaśnienie Naczelnika Wydziału Organizacji i Spraw Obywatelskich, będącej jednocześnie Inspektorem Ochrony Danych w Urzędzie i Przewodniczącą ww. Zespołu. Naczelnik wyjaśniła, że chaos informacyjny i interpretacyjny, jaki powstał w okresie wdrażania RODO spowodował, że w pierwszej kolejności skupiono się na opracowaniu i wdrożeniu zasad przetwarzania danych osobowych oraz ochrony w tym zakresie. Ponadto na Administratora nałożono szereg innych obowiązków, przy których wypełnieniu zaangażowany był Inspektor Ochrony Danych, który m.in. opiniował setki wpływających do niego dokumentów, w tym umów, przeprowadzał szkolenia pracowników, udzielał na bieżąco wyjaśnień pracownikom, przygotowywał i zamieszczał informacje i broszury w intranecie Urzędu. Dodatkowo, w październiku 2017 r. wdrażana była w Urzędzie nowa wersja Systemu Zarządzania Jakością wg normy ISO 9000:2015, w 2018 r. rozpoczęły się przygotowania do wyborów samorządowych, w 2019 r. do Parlamentu Europejskiego oraz do Sejmu i Senatu RP, a w 2020 r. dwa podejścia do wyborów prezydenckich. W procesy te zaangażowani byli również członkowie Zespołu ds. opracowania systemu zarządzania bezpieczeństwem informacji. W związku z powyższym spiętrzeniem obowiązków, dalsze prace nad SZBI – mimo opracowania części dokumentacji w wersji brudnopisu - zostały zawieszone, a termin zakończenia prac w trzecim etapie w zakresie bezpieczeństwa informacji przesunięto, nie dokonując przez przeoczenie zmiany harmonogramu.

   Wyjaśniając dlaczego Burmistrz nie wyegzekwował realizacji tych zadań, Zastępca Burmistrza (z up. Burmistrza) potwierdził przyczyny wskazane przez

[52] Rozporządzenie Parlamentu Europejskiego i Radu Unii Europejskiej z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (Dz.U.UE.L.2016.119.1).

[53] Dz. U. z 2017 r. poz. 2247, zw. dalej „rozporządzeniem KRI".

IOD, w tym zaangażowanie członków Zespołu w proces wyborczy i zapowiedział kontynuację prac, na potwierdzenie czego załączył Zarządzenie nr 154/2020 r. z 11 września 2020 r. zmieniające skład Zespołu i wprowadzające nowy harmonogram, w którym termin opracowania niezbędnej dokumentacji wydłużono do 30 czerwca 2021 r.

(dowód: akta kontroli str. 116-201, 250-255, 618-619, 620-660, 661-664)

2. Analiza kont 15 pracowników, którzy w latach 2016-2020 rozwiązali stosunek pracy z Urzędem wniosków o odebranie uprawnień do systemu informatycznego wykazała, że:
   a. w jednym przypadku zmiana uprawnień dostępu do zasobów komputera została przeprowadzona z opóźnieniem 11 dni, co stanowiło naruszenie § 20 ust. 2 pkt 5 rozporządzenia KRI;
   b. w dziewięciu przypadkach odebranie uprawnień dostępu do zasobów komputera nie zostało poprzedzone wnioskiem, o którym mowa w:
      – § 8 ust. 3 pkt 2 Polityki bezpieczeństwa oraz § 4 pkt 5 Instrukcji zarządzania systemem informatycznym, wprowadzonych Zarządzeniem Burmistrza Aleksandrowa Łódzkiego Nr 1/2011 z dnia 4 stycznia 2011 r.;
      – § 9 pkt 16 Polityki bezpieczeństwa oraz § 11 pkt 3 i 9 Instrukcji zarządzania systemem informatycznym, wprowadzonych Zarządzeniem Burmistrza Aleksandrowa Łódzkiego Nr 146/2018 z dnia 6 sierpnia 2018 r.

   IOD oraz Naczelnik Wydziału Obsługi Informatycznej wyjaśnili m.in., że uprawnienia są odbierane natychmiast po otrzymaniu stosownego wniosku lub informacji z kadr, wobec niektórych osób naczelnicy wydziałów nie wystąpili z wnioskami, ale stanowisko ds. Kadr ustnie przekazało informację o rozwiązaniu stosunku pracy, a w przypadku osób, które przed zakończeniem stosunku pracy składały karty obiegowe, odebranie uprawnień nastąpiło na ich podstawie. Brak wniosku o odebranie uprawnień jednemu z pracowników Wydziału Obsługi Informatycznej, Naczelnik Wydziału wyjaśnił przeoczeniem procedury.

   (dowód: akta kontroli str. 487-515)

3. W latach 2017 i 2018 w Urzędzie nie przeprowadzono audytu z zakresu bezpieczeństwa informacji, co było niezgodne z § 20 ust. 2 pkt 14 rozporządzenia KRI. Zgodnie ze wskazanym przepisem, obowiązkiem kierownictwa podmiotu publicznego było zapewnienie warunków umożliwiających realizację takiego audytu, nie rzadziej niż raz na rok.
   Wyjaśniając przyczyny tego stanu, Zastępca Burmistrza (z up. Burmistrza) przedstawił wyjaśnienie Audytora Wewnętrznego Urzędu, który podał, że w latach 2017 i 2018 obowiązek wynikający z KRI był przedmiotem rozważań i analizy kosztów dla ewentualnych korzyści, po czym podjęto decyzję o wstrzymaniu planowania audytu bezpieczeństwa informacji w związku z zapowiedzią wprowadzenia RODO i zmian w przepisach. Zdecydowano najpierw wprowadzić zmiany organizacyjne i regulacje wewnętrzne spełniające wymogi RODO, a następnie potwierdzić je audytem. Natomiast w 2020 r. podjęto decyzję o ponownym przeprowadzeniu specjalistycznego audytu informatycznego przez firmę zewnętrzną, jednak zamówienie tej usługi zostało wstrzymane ze względu na ograniczenia związane z wybuchem epidemii. Procedurę zamówienia wszczęto w dniu 23 września 2020 r.

   (dowód: akta kontroli str. 516-621)

IV. Uwagi i wnioski

W związku ze stwierdzonymi nieprawidłowościami, Najwyższa Izba Kontroli, na podstawie art. 53 ust. 1 pkt 5 ustawy o NIK, przedstawia następujące uwagi i wnioski:

Wnioski

1) Opracować i wdrożyć system zarządzania bezpieczeństwem informacji, zgodnie z § 20 ust. 1, w zw. z ust. 3 rozporządzenia KRI.
2) Niezwłocznie dokonywać zmiany uprawnień do systemów informatycznych pracownikom, którzy zakończyli zatrudnienie w Urzędzie oraz dokumentować zmiany w sposób określony w wewnętrznych przepisach.
3) Zapewnić okresowy audyt wewnętrzny w zakresie bezpieczeństwa informacji, o którym mowa w § 20 ust. 2 pkt 14 rozporządzenia KRI.

Uwagi

Najwyższa Izba Kontroli nie formułuje uwag.

V. Pozostałe informacje i pouczenia

Wystąpienie pokontrolne zostało sporządzone w dwóch egzemplarzach; jeden dla kierownika jednostki kontrolowanej, drugi do akt kontroli.

Prawo zgłoszenia zastrzeżeń

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 Najwyższej Izby Kontroli w Łodzi. Prawo zgłaszania zastrzeżeń, zgodnie z art. 61 b ust. 2 ustawy o NIK, nie przysługuje do wystąpienia pokontrolnego zmienionego zgodnie z treścią uchwały w sprawie zastrzeżeń.

Obowiązek poinformowania NIK o sposobie wykorzystania uwag i wykonania wniosków

Zgodnie z art. 62 ustawy o NIK należy poinformować Najwyższą Izbę Kontroli, w terminie 21 od otrzymania wystąpienia pokontrolnego, o sposobie 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.

Łódź, 19 października 2020 r.

Najwyższa Izba Kontroli
Delegatura w Łodzi

Kontroler
Agnieszka Tomalska
Główny specjalista k.p.

podpis

Dyrektor
Przemysław Szewczyk

Podpis