NAJWYŻSZA IZBA KONTROLI
Delegatura w Łodzi

LLO.410.009.01.2020

Pan
Tomasz Jachymek
Burmistrz
Urząd Miejski w Zelowie
ul. Żeromskiego 23
97-425 Zelów

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 Zelowie, ul. Stefana Żeromskiego 23, 97-425 Zelów
Kierownik jednostki kontrolowanej	Tomasz Jachymek, Burmistrz Zelowa od 22 listopada 2018 r. W okresie objętym kontrolą funkcję kierownika jednostki poprzednio pełniła: Urszula Świerczyńska, Burmistrz Zelowa w okresie od 6 grudnia 2010 r. do 21 listopada 2018 r.
Zakres przedmiotowy kontroli	Świadczenie przez urzędy jednostek samorządu terytorialnego e-usług. Rozwiązania organizacyjne i techniczne w zakresie zapewnienia bezpieczeństwa przetwarzania informacji w urzędzie i ich stosowanie.
Okres objęty kontrolą	Od 1 stycznia 2016 r. do 20 sierpnia 2020 r.
Podstawa prawna podjęcia kontroli	Art. 2 ust. 2 ustawy z dnia 23 grudnia 1994 r. o Najwyższej Izbie Kontroli[1]
Jednostka przeprowadzająca kontrolę	Najwyższa Izba Kontroli Delegatura w Łodzi
Kontroler	Ewa Tworkowska, inspektor kontroli państwowej, upoważnienie do kontroli nr LLO/81/2020 z 9 czerwca 2020 r. (akta kontroli str. 1-3)

[1] Dz. U. z 2020 r. poz. 1200, dalej: ustawa o NIK.

II. Ocena ogólna[2] kontrolowanej działalności

OCENA OGÓLNA

Najwyższa Izba Kontroli ocenia, że w latach 2016-2020 (I połowa) Urząd Miejski w Zelowie (dalej: Urząd) sprawnie realizował usługi publiczne na rzecz obywateli, wpływające poprzez ePUAP[3], jednak - z uwagi na przyjęcie niewystarczających rozwiązań organizacyjnych i technicznych - nie zapewnił w wymaganym stopniu bezpieczeństwa przetwarzania informacji. Stwierdzone w trakcie kontroli nieprawidłowości wynikały głównie z braku spełnienia wymogów wynikających z 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*[4] (dalej: Rozporządzenie KRI):

- 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 zawężały się do ochrony danych osobowych oraz regulacji w zakresie monitoringu wizyjnego i dostępu do pomieszczeń.
- w przypadku pięciu z 15 poddanych weryfikacji kont pracowników, którzy zakończyli zatrudnienie w Urzędzie, wbrew § 20 ust. 2 pkt. 5 rozporządzenia KRI, nie został zablokowany dostęp do systemów informatycznych, natomiast dla dziewięciu kont czynności blokowania dostępu dokonywane były w sposób opieszały i trwały od 20 dni do nawet 17 miesięcy od dnia rozwiązania stosunku pracy;
- nie wszyscy pracownicy Urzędu, zaangażowani w proces przetwarzania informacji, zostali w okresie dwóch ostatnich lat[5] objęci szkoleniami wymaganymi § 20 ust. 2 pkt. 6 Rozporządzenia KRI. W tym czasie, w zorganizowanej w 2019 r. formie podnoszenia wiedzy z zakresu bezpieczeństwa informacji w systemach informatycznych, udział wzięło czterech z 66 pracowników;
- w niewystarczającym stopniu ustanowiono zabezpieczenia systemów informatycznych, gwarantujące adekwatne uprawnienia użytkowników, względem realizowanych przez nich zadań. Wbrew § 20 ust. 2 pkt 4 Rozporządzenia KRI, w przypadku dwóch z dziesięciu zweryfikowanych komputerów możliwym było samodzielne dokonywanie instalacji nieautoryzowanego oprogramowania przez osoby niebędące pracownikami służb informatycznych;
- w latach 2018-2020 nie przeprowadzano corocznego audytu bezpieczeństwa informacji, wymaganego § 20 ust. 2 pkt 14 Rozporządzenia KRI.

W wyniku nierzetelnego ewidencjonowania sprzętu i oprogramowania oraz wbrew § 20 ust. 2 pkt 2 Rozporządzenia KRI, Urząd nie posiadał bieżącej informacji o zasobach informatycznych, a rozbieżności w tym zakresie stwierdzono w przypadku 10 spośród 15 poddanych weryfikacji sprzętów. Ponadto widniejące na stronie internetowej Urzędu informacje o rodzaju spraw możliwych do załatwienia drogą elektroniczną, a także wymogach z tym związanych, były nieaktualne i niekompletne.

Realizacja usług elektronicznych przez Urząd, pomimo ograniczonych działań informacyjnych, przebiegała prawidłowo i sprawnie.

---

[2] Najwyższa Izba Kontroli formułuje ocenę ogólną jako ocenę pozytywną, ocenę negatywną albo ocenę w formie opisowej.

[3] Ogólnopolska platforma teleinformatyczna, zapewniająca ustandaryzowaną komunikację m.in. pomiędzy obywatelami a administracją samorządową oraz pomiędzy urzędami administracji publicznej.

[4] Dz. U. z 2017 r. poz. 2247.

[5] Tj. od 1 lipca 2018 r. do 30 czerwca 2020 r.

III. Opis ustalonego stanu faktycznego

Opis stanu faktycznego

1. W przyjętych na lata 2014-2020 dokumentach o charakterze strategicznym[6], wskazujących kierunki rozwoju Gminy Zelów, nie zawarto celów związanych z dostosowaniem Urzędu do elektronicznego świadczenia usług publicznych, bądź podniesieniem jakości takich usług. Burmistrz Miasta Zelowa (dalej: Burmistrz) wyjaśnił, że z przeprowadzonych konsultacji społecznych, stanowiących podstawę opracowania Planu i Programu Rozwoju Gminy, nie wynikała potrzeba poprawy e-usług świadczonych przez Urząd. Praca Urzędu i dostępność internetu zostały wysoko ocenione przez mieszkańców[7]. Natomiast rozwój szeroko rozumianych usług publicznych, w tym infrastruktury i technologii informacyjno-komunikacyjnych, ujęto w ramach celu strategicznego nr III[8] i powiązano z dostępem do internetu szerokopasmowego, którego realizację mieszkańcy Gminy wskazali, w przeprowadzonych konsultacjach, jako zadanie na lata przyszłe, tj. po okresie 2014-2020.

(akta kontroli str. 69-98, 829, 833-834, 839-841)

2. Według stanu na dzień 31 maja 2020 r. Urząd udostępniał obywatelom za pośrednictwem platformy ePUAP w sumie 61 usług, w kategoriach:

- sprawy obywatelskie oraz wybory– łącznie 32 usługi[9],
- podatki i opłaty – 14 usług,
- praca i zatrudnienie – cztery usługi,
- ochrona środowiska – trzy usługi,
- sprawy ogólne – trzy usługi,
- budownictwo i mieszkania – dwie usługi,
- dziecko – jedna usługa,
- egzekucja – jedna usługa,
- geodezja i kartografia – jedna usługa.

Jednocześnie platforma ePUAP wskazywała, że Urząd świadczy dla obywateli 136 e-usług, pomimo iż w rzeczywistości, jak wskazano wyżej, było ich 61. Jak stwierdzono, nie wszystkie wyświetlane przez ePUAP usługi elektroniczne należały do właściwości tej jednostki. Burmistrz wyjaśnił, że nie podejmowano działań celem zaktualizowania tej liczby w ePUAP.

Urząd nie udostępniał usług elektronicznych z wykorzystaniem innych środków, jak np. platformy regionalne, bądź miejscowe.

(akta kontroli str. 99-107, 842-843, 855, 865, 867-876)

3. W pierwszym półroczu 2020 r. za pośrednictwem ogólnopolskiej platformy e-PUAP w Urzędzie zrealizowano 315 usług elektronicznych na rzecz obywateli, z czego:

- 99 usług w okresie od 1 stycznia 2020 r. do 28 lutego 2020 r.;
- 162 usługi w okresie od 1 marca 2020 r. do 30 kwietnia 2020 r.;
- 54 usługi w okresie od 1 maja 2020 r. do 30 czerwca 2020 r.

---

[6] „Program Rozwoju Gminy Zelów na lata 2014-2020" i „Lokalny Plan Rozwoju Gminy Zelów na lata 2014-2020", przyjęte uchwałami Rady Miejskiej w Zelowie nr XIII/112/2015 oraz nr XIII/113/2015 z 29 grudnia 2015 r., dalej: Plan i Program Rozwoju.

[7] Zadowolenie z pracy Urzędu podczas przeprowadzonych wśród mieszkańców konsultacji wyraziło 73% pytanych (odpowiedzi „dobrze" „bardzo dobrze"), pozostali uczestniczący w ankiecie byli niezadowoleni z pracy Urzędu (28%). Dostęp do internetu oceniono „bardzo dobrze" lub „dobrze" (52% odpowiedzi), zaś łącznie 20% stanowiły odpowiedzi: „źle" i „bardzo źle".

[8] „Program Rozwoju Gminy Zelów na lata 2014-2020, cel strategiczny nr III: Rozwój usług publicznych, odnawialne źródła energii.

[9] W tym: dowody osobiste (siedem usług), wybory (dziesięć usług), wnioski o udostępnianie lub sprawdzenie danych z Rejestru Dowodów Osobistych lub Rejestru PESEL (siedem usług), zgłoszenia: pobytu, wyjazdu, wymeldowania (sześć usług), wydanie odpisu aktu stanu cywilnego (dwie usługi).

Najwięcej spraw wpłynęło do Urzędu w postaci pisma ogólnego, głównie o charakterze informacyjnym lub stanowiącym zapytanie (łącznie 283, tj. 89,8% wszystkich e-usług w tym okresie). Pozostałe wnioski lub zawiadomienia dotyczyły spraw obywatelskich, jak m.in.: wydania dowodu osobistego (13 wniosków), zgłoszenia pobytu czasowego lub stałego (trzy), dopisania do spisu wyborców (łącznie siedem wniosków lub zawiadomień), udostępnienia spisu wyborców (jeden wniosek) lub akt osobowych (jeden wniosek), danych archiwalnych z ksiąg stanu cywilnego (pięć wniosków), odpisów aktów małżeństwa (dwa wnioski).
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. 63,6% w porównaniu z pierwszymi dwoma miesiącami roku). W tym czasie ponaddwukrotnie częściej wnioskowano w ramach usług związanych ze zdrowiem i sprawami społecznymi i niespełna dwukrotnie częściej w zakresie gospodarki komunalnej, nieruchomości oraz spraw obywatelskich. Z kolei w trakcie kolejnych dwóch miesięcy (maj-czerwiec 2020 r.) liczba spraw kierowanych do Urzędu przez ePUAP była o prawie połowę mniejsza niż z początku roku (styczeń-luty 2020 r.) i trzykrotnie mniejsza niż w miesiącach marzec-kwiecień 2020 r., co - zdaniem Burmistrza - mogło wynikać z poluzowania restrykcji epidemiologicznych dotyczących pracy urzędów i umożliwieniem osobistego kontaktu, preferowanego i wybieranego przez mieszkańców Gminy.

(akta kontroli str. 108-135, 843, 856)

4. Prowadzony w Urzędzie monitoring korzystania w okresie objętym kontrolą przez obywateli oraz przedsiębiorców z usług świadczonych w formie elektronicznej nie przybrał formy szczegółowych analiz - jak wyjaśnił Burmistrz - ze względu na stosunkowo niewielkie zainteresowanie petentów cyfrową formą kontaktu. W przeważającej większości preferowaną przez obywateli formą realizacji spraw była postać tradycyjna, polegająca na kontakcie osobistym. Mieszkańcy wybierali tę formę, pomimo możliwości procedowania elektronicznego, dla m.in. spraw podatkowych, dotyczących nieruchomości, zameldowania, dowodów osobistych czy wydania odpisu aktu stanu cywilnego. Brak zainteresowania poszczególnymi e-usługami wynikał, według Burmistrza, z charakteru Gminy, struktury wiekowej mieszkańców, poziomu ogólnej wiedzy informatycznej i dostępności sprzętu komputerowego oraz internetu. Jako utrudnienia wskazał także procedurę założenia konta na ePUAP, obawy o wiarygodność elektronicznego kontaktu z Urzędem, niezrozumiały język używany w aplikacjach oraz niski poziom promowania e-usług. Burmistrz wyjaśnił, że wizyty w Urzędzie pozwalały mieszkańcom na szybkie uzyskanie informacji co do przedmiotu załatwianej sprawy lub uzupełnienie ewentualnych braków we wnioskach, dzięki czemu możliwym było wyeliminowanie, już w początkowej fazie, ewentualnych braków lub błędów.

(akta kontroli str. 798, 829, 834-835, 843, 855-856, 860)

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

(akta kontroli str. 136, 799)

6. Zgodnie z zarządzeniem Burmistrza[10] podstawowym sposobem dokumentowania przebiegu załatwiania i rozstrzygania spraw był system tradycyjny, o którym mowa

[10] Zarządzenie Burmistrza Zelowa nr 120.6.2011 z dnia 17 marca 2011 r. w sprawie wskazania sposobu wykonywania czynności kancelaryjnych w Urzędzie Miejskim w Zelowie i wyznaczenia koordynatora czynności kancelaryjnych, ze zmianami wprowadzonymi zarządzeniem nr 120.18.2018 z dnia 20 listopada 2018 r.

w § 1 załącznika nr 1 do rozporządzenia w sprawie instrukcji kancelaryjnej[11]. W Urzędzie nie opracowano innych wewnętrznych procedur regulujących obieg i zarządzanie dokumentami. Burmistrz wyjaśnił, że wiedzę o sposobie postępowania z pismami wpływającymi do Urzędu poprzez ePUAP i wychodzącymi drogą elektroniczną z jednostki, w tym weryfikacji podpisów elektronicznych, pracownicy czerpali z informacji przekazywanych przez przełożonych.

Funkcję koordynatora czynności kancelaryjnych pełnił pracownik Referatu Organizacyjnego, zaś nadzór nad realizacją przywołanego zarządzenia powierzony został Kierownikowi tego referatu i Sekretarzowi Miasta.

(akta kontroli str. 207-223, 796, 829, 835)

W praktyce obieg dokumentów, zarówno papierowych, jak i elektronicznych, realizowany był przy użyciu *Systemu Elektronicznego Monitorowania Pracy* (dalej: SEMP), który obejmował rejestr korespondencji przychodzącej oraz umożliwiał śledzenie postępu spraw. Dokumenty elektroniczne wpływały na adres kontaktowy Urzędu[12], obsługiwany przez pracowników sekretariatu, bądź elektroniczną skrzynkę podawczą, poprzez ePUAP, skąd były odbierane przez Informatyka lub Inspektora Ochrony Danych, a następnie przesyłane do sekretariatu, rejestrowane w SEMP i drukowane. Weryfikacji podpisu elektronicznego, którym opatrzone były dokumenty elektroniczne, dokonywał Informatyk lub Inspektor Ochrony Danych, podczas pobierania korespondencji z ePUAP. Sprawy procedowane były w sposób tradycyjny (papierowy). Pracownik Urzędu otrzymywał ich wydrukowaną wersję, z naniesioną dekretacją przełożonych. Osoby zaangażowane w przebieg danej sprawy miały wgląd - poprzez system SEMP - do stanu jej realizacji. Pracownicy merytoryczni komórek organizacyjnych Urzędu byli zobowiązani do zamknięcia sprawy w SEMP, jednak takie zobowiązanie wynikało z ogólnie przyjętych praktyk postępowania ze sprawami, a nie z regulacji wewnętrznych, nieopracowanych dla funkcjonującego w Urzędzie systemu.

(akta kontroli str. 150-151, 155-159, 178-181, 224-242, 796-797,829-830, 835)

Odpowiedzi przekazywane w imieniu Urzędu przez ePUAP, podpisywane były przez Inspektora Ochrony Danych lub Informatyka, profilem zaufanym, z uwagi na fakt, iż jedynie tym dwóm pracownikom umożliwiono dostęp do skrzynki Urzędu założonej na ePUAP. Załączniki przesyłane były w postaci skanów dokumentów odręcznie podpisanych przez upoważnione osoby[13], bądź plików, przygotowanych przez pracowników merytorycznych i podpisanych elektronicznie, podpisem kwalifikowanym, przez osoby wliczane do kierownictwa Urzędu. Przy procedowaniu spraw drogą elektroniczną poza ePUAP, w zależności od wymagań instytucji, do których przesyłane były dokumenty/sprawozdania, podpisy elektroniczne składane były przy użyciu profilu zaufanego pracownika Urzędu (11 pracowników Urzędu wykorzystujących profil zaufany do celów służbowych[14]), bądź podpisem kwalifikowanym (13 osób wyposażonych w czytniki i karty do dokonywania takiego podpisu[15]).

(akta kontroli str. 225-242, 247-249, 732-739, 743, 796-797, 815-824, 832-838, 867)

---

[11] 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.).

[12] umzelow@zelow.pl.

[13] Dokumenty te stanowiły załącznik do wysyłanej wiadomości podpisywanej elektronicznie profilem zaufanym. Nie występowało zjawisko podwójnego podpisywania dokumentów, tzn. sytuacja, gdy dokument byłby drukowany, podpisywany odręcznie a następnie skanowany i podpisywany elektronicznie.

[14] Osoby te w 2020 r. (I połowa) podpisały elektronicznie łącznie 448 dokumentów.

[15] Osoby te w 2020 r. (I połowa) podpisały elektronicznie łącznie 836 dokumentów.

7. Szczegółowa analiza[16] 20 spraw wpływających do Urzędu przez ePUAP w I półroczu 2020 r. wykazała, że:

- przekazanie do pracownika merytorycznego prowadzącego daną sprawę następowało w dniu złożenia dokumentu lub najpóźniej w kolejnym dniu roboczym;
- w dwóch przypadkach, w których badane wnioski nie były kompletne, po dokonanym przez Urząd wezwaniu, możliwe było ich uzupełnienie w drodze komunikacji elektronicznej. Niemniej jednak pierwszy z wnioskodawców zadecydował o osobistym przedłożeniu dokumentów (potwierdzenie dokonania opłaty), a drugi nie podjął żadnych czynności[17], co zadecydowało o pozostawieniu sprawy bez rozpatrzenia;
- od momentu rozpoczęcia prowadzenia sprawy ciężar kontaktu z obywatelami oraz ewentualnie z innymi instytucjami spoczywał na Urzędzie. W 16 z 19 analizowanych przypadków, informacje przekazywano wnioskodawcom wyłącznie w formie elektronicznej (poprzez wiadomość mailową lub ePUAP), a w trzech pozostałych: telefonicznie, drogą pocztową lub jednocześnie pocztą i pocztą elektroniczną (e-mailem). W jednym przypadku nie wystąpiła konieczność kontaktowania się z wnioskodawcą. Przy realizacji sześciu spraw wymagających komunikacji z inną jednostką administracji publicznej, w pięciu przypadkach[18] informacje przesyłano za pośrednictwem platformy ePUAP, a w jednym[19] wystąpiono o opinie do: Państwowego Powiatowego Inspektoratu Sanitarnego w Bełchatowie, Regionalnego Dyrektora Ochrony Środowiska w Łodzi i Zarządu Zlewni w Sieradzu, pismem przesłanym pocztą oraz mailowo (uzupełnienie wniosku). Instytucje te przekazały opinie poprzez ePUAP;
- system elektronicznego obiegu dokumentów (SEMP) nie komunikował się automatycznie z innymi systemami, programami lub platformami informatycznymi w zakresie przesyłania danych. Dla załatwienia spraw Urząd korzystał z danych gromadzonych w zewnętrznych systemach takich jak m.in.: *Geoportal, Źródło, Rejestr PESEL, Rejestr Dowodów Osobistych, czy Rejestr Wyborców* i nie żądał od wnioskodawców dodatkowych informacji w tym zakresie;
- 10 z analizowanych spraw zostało przez Urząd zrealizowanych tego samego lub kolejnego dnia (licząc od daty dekretowania na pracownika merytorycznego). Równie sprawnie przekazywano obywatelom potwierdzenia złożenia wniosku w sześciu przypadkach dotyczących wydania dowodu osobistego. Wskazywano wówczas przewidywany termin odbioru dowodu oraz możliwość weryfikacji tego terminu na stronie: obywatel.gov.pl. Uzyskanie informacji na temat aktualnego stanu procedowania sprawy w pozostałych czterech przypadkach możliwe było poprzez kontakt osobisty, mailowy lub

---

[16] 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.: wniosek o dokonanie zmiany w miejscowym planie zagospodarowania przestrzennego, wniosek o wydanie decyzji o środowiskowych uwarunkowaniach, sześć wniosków o wydanie dowodu osobistego, pięć wniosków o dopisanie do spisu wyborców, dwa zgłoszenia pobytu czasowego, dwa wnioski o udostępnienie materiałów archiwalnych USC, dwa wnioski o wydanie zupełnego odpisu aktu małżeństwa, pismo z zapytaniem o możliwość uzyskania wsparcia finansowego.

[17] Nie uzupełnił wymaganego na podstawie art. 28 ust. 2a ustawy z 24 września 2010 r. o ewidencji ludności (Dz. U. z 2019 r. poz. 1397, ze zm.) dokumentu potwierdzającego tytuł prawny do lokalu.

[18] Zawiadomienia urzędów gmin o dopisaniu do spisu wyborców.

[19] Wymagającym pozyskania opinii co do obowiązku przeprowadzenia oceny oddziaływania na środowisko dla planowanego przedsięwzięcia inwestycyjnego.

telefoniczny, bowiem nie były one udostępniane poprzez SEMP, stronę bądź platformę internetową, pozwalającą na samodzielne śledzenie postępu sprawy przez obywatela;

– za wyjątkiem jednej, poprowadzonej telefonicznie sprawy (zapytania o możliwość wsparcia finansowego), wszystkie przypadki zostały zarejestrowane w SEMP, wydrukowane i przekazane do komórek merytorycznych w formie papierowej. Odpowiedzi na cztery wnioski skierowane do USC oraz jedno zameldowanie na pobyt czasowy (niewymagające informowania petenta) zostały całkowicie procedowane w formie elektronicznej. W pozostałych czternastu przypadkach przy prowadzeniu sprawy wspomagano się formą papierową dokumentów (dokumenty podpisywane odręcznie, przesyłane pocztowo lub w formie skanu).

(akta kontroli str. 155-156, 194-195, 243-256, 797-798, 844, 856)

8. W latach 2016-2020 (I półrocze) wykorzystywana platforma ePUAP nie zawsze działała sprawnie i bezawaryjnie. Urząd dwukrotnie (w 2018 r. i 2020 r.) dokonywał zgłoszeń, drogą mailową, do Centralnego Ośrodka Informatyki (*COI*), w związku z napotkanymi problemami w funkcjonowaniu ePUAP. Konsultacja telefoniczna z 2018 r. dotyczyła możliwości utworzenia odpowiedzi do wcześniej przesłanej sprawy oraz wysyłania pism, w sytuacji gdy znany był tylko adres skrytki, bez pełnej nazwy adresata. Z kolei problem zgłoszony w kwietniu 2020 r. związany był ze składaniem podpisu kwalifikowanego Burmistrza i wyświetlanej informacji o brakujących komponentach systemowych umożliwiających podpisanie korespondencji w formie elektronicznej, pomimo iż komponenty te - według dokonującego zgłoszenia Inspektora Ochrony Danych - były zainstalowane poprawnie. Do dnia zakończenia kontroli NIK problem nie został rozwiązany[20].
Ponadto wystąpiły utrudnienia, które nie były zgłaszane, a które wiązały się m.in. z załączaniem dokumentów i „zawieszaniem się" platformy podczas przygotowywania korespondencji wychodzącej. Wskazane problemy nie wpłynęły na terminowość realizacji zadań.

(akta kontroli str. 245-246, 257-276, 830, 835-836)

9. System monitorowania obiegu dokumentów, w tym elektronicznych (SEMP), dostarczany był Urzędowi przez podmiot komercyjny. Umowy dotyczące korzystania z oprogramowania zawierane były corocznie, w sposób zapewniający ciągłość dostępu do systemu. Treść umów nie odnosiła się do czasu, bądź sposobu reakcji producenta na usunięcie ewentualnych usterek w jego działaniu. W latach 2016-2020 nie wystąpiły błędy w funkcjonowaniu przyjętego systemu.

(akta kontroli str. 156, 181, 277-304, 798, 808, 810-811, 830, 835)

10. Aktualna na dzień prowadzenia kontroli NIK strona internetowa Gminy[21] posiadała zakładkę „ePUAP", której wybór umożliwiał zapoznanie się z podstawowymi informacjami o możliwości załatwienia spraw drogą elektroniczną, w tym m.in. o:

– ustawowym[22] zobowiązaniu podmiotów świadczących usługi publiczne do umożliwienia interesantom wnoszenia ich wniosków w formie dokumentów elektronicznych poprzez Elektroniczną Skrzynkę Podawczą podmiotu,

---

[20] Ostatni kontakt w tej sprawie z Zespołem Service Desk COI (epuap-pomoc@coi.gov.pl) miał miejsce 28 kwietnia 2020 r.

[21] http://www.zelow.pl (dalej: strona internetowa Gminy), dostęp 24 czerwca 2020 r.

[22] Zgodnie z ustawą z dnia 12 lutego 2010 roku o zmianie ustawy o informatyzacji działalności podmiotów realizujących zadania publiczne oraz niektórych innych ustaw (Dz. U. z 2010 r. nr 40 poz. 230).

– koniecznych do spełnienia warunkach umożliwiających korzystanie z e-usług świadczonych przez platformę e-PUAP, w tym wymogu założenia konta użytkownika na platformie ePUAP (wraz z informacją, że konto takie jest bezpłatne) oraz możliwościach, jakie daje posiadanie profilu zaufanego i podpisu elektronicznego.

Na stronie nie zawarto informacji o sposobie uzyskania profilu zaufanego lub dowodu osobistego z warstwą elektroniczną (e-dowód), ani nie wskazano możliwości posługiwania się e-dowodem przy prowadzeniu spraw drogą elektroniczną, o czym szerzej w sekcji „stwierdzone nieprawidłowości". Zamieszczono natomiast linki odsyłające do strony ePUAP[23] oraz www.login.gov.pl, stanowiących źródło wiedzy w tym zakresie. Ponadto Urząd, poprzez bezpłatny informator o zasięgu gminnym (wydanie z kwietnia 2019 r.), a także – według oświadczenia Kierownika Referatu Spraw Obywatelskich - każdorazowo przy wydawaniu e-dowodów, informował mieszkańców o funkcjach takiego dokumentu tożsamości i sposobie posługiwania się nim.

(akta kontroli str. 309-342)

Na stronie internetowej Gminy nie zawarto listy spraw możliwych do zrealizowania w Urzędzie drogą elektroniczną. W celu ustalenia, czy dana usługa była możliwa do przeprowadzenia przez ePUAP, należało zapoznać się z opisem zagadnień realizowanych przez komórki organizacyjne Urzędu, zawartym na stronie Biuletynu Informacji Publicznej[24], przy czym na 61 e-usług świadczonych przez Urząd, informacja o takiej możliwości została wskazana dla pięciu, prowadzonych wyłącznie przez Referat Spraw Obywatelskich. W dniu 14 maja 2020 r., na stronie Gminy poświęconej aktualnościom, zamieszczono informację[25] o uruchomionej od 21 kwietnia 2020 r., przez Ministerstwo Cyfryzacji możliwości elektronicznego wnioskowania o odpis aktu stanu cywilnego, wraz z niezbędnym linkiem do strony[26], umożliwiającym dalsze procedowanie on-line.

(akta kontroli str. 99-107, 309-316, 830, 836)

11. W okresie od 1 lipca 2018 r. do 30 czerwca 2020 r. pracownicy Urzędu uczestniczyli w 125 szkoleniach zewnętrznych, z czego w sumie 13 dotyczyło: ochrony danych osobowych lub bezpieczeństwa danych (pięć szkoleń), obsługi programów merytorycznie związanych z wykonywanymi obowiązkami, głównie aplikacją do ewidencji ludności „*Źródło*" (sześć szkoleń) lub przeciwdziałaniu zagrożeniom związanym z obsługą systemów informatycznych (dwa szkolenia). We wskazanych 13 formach podnoszenia kompetencji udział wzięło ośmiu pracowników Urzędu, w tym czterech w ramach trzech szkoleń dotyczących bezpieczeństwa informacji, które odbyły się wyłącznie w 2019 r.

(akta kontroli str. 181, 193, 361-381, 402-440, 456-465)

W Urzędzie nie prowadzono odrębnych szkoleń w zakresie zapewnienia bezpieczeństwa informacji. Mające miejsce 19 czerwca 2018 r. szkolenie wewnętrzne, przeprowadzone przez Sekretarza Miasta oraz Inspektora Ochrony Danych, dotyczyło ochrony danych osobowych z uwzględnieniem zmian, jakie niosło za sobą wejście w życie przepisów RODO. Przeszkolonych zostało 49 z 69 pracowników Urzędu (wraz z prowadzącymi i kierownictwem Urzędu). Jak

---

[23] https://epuap.gov.pl/wps/portal, dostęp 24 czerwca 2020 r.

[24] https://bip.zelow.pl/ (dalej: strona BIP), dostęp 24 czerwca 2020 r. Po wyborze z menu przedmiotowego opcji „Załatwianie spraw w urzędzie", a następnie „Sposoby załatwiania spraw", która powodowała przeniesienie do podstron dziewięciu komórek organizacyjnych Urzędu, z m.in. zakresem prowadzonych przez tę komórkę spraw, wymaganymi dokumentami, miejscem składania dokumentów, formy zakończenia sprawy, trybu odwoławczego, podstawy prawnej prowadzenia danego typu sprawy, a także możliwymi do pobrania w formie elektronicznej załącznikami.

[25] http://zelow.pl/2020/05/14/wnioskowanie-on-line-o-odpis-aktu-stanu-cywilnego/, dostęp 24 czerwca 2020 r.

[26] https://www.gov.pl/web/gov/uzyskaj-odpis-aktu-stanu-cywilnego-urodzenia-malzenstwa-zgonu, dostęp 24 czerwca 2020 r.

oświadczył prowadzący szkolenie Inspektor Ochrony Danych, w trakcie szkolenia przypomniano zasady zapewnienia bezpieczeństwa informacji na stanowiskach pracy, zachowania ostrożności podczas rozmów telefonicznych i odbioru korespondencji elektronicznej.

(akta kontroli str. 137, 343-347, 356-360, 382-401, 441-455, 466, 844, 856-857)

12. Opracowana i obowiązująca w Urzędzie w latach 2016-2018[27] dokumentacja SZBI, na którą składały się: „Polityka Bezpieczeństwa Informacji"[28] i „Instrukcja zarządzania systemami informatycznymi służącymi do przetwarzania danych osobowych"[29] oraz zastępująca je z dniem 21 czerwca 2018 r. „Polityka Bezpieczeństwa Informacji i Ochrony Danych Osobowych"[30] (dalej określane odpowiednio jako: *Polityki* i *Instrukcja*) ograniczała się - z założenia - do bezpieczeństwa danych osobowych. Innym dokumentem regulującym kwestię bezpieczeństwa i dostępu do przechowywanych w Urzędzie danych była *Instrukcja dotycząca zasad gospodarki kluczami oraz zabezpieczania pomieszczeń i budynku Urzędu Miejskiego w Zelowie*[31], obowiązująca od 23 maja 2013 r.

(akta kontroli str. 163, 467-686, 798-799, 826, 830, 836)

Jak wynika z wyjaśnień Kierownika Referatu Organizacyjnego, dokumenty te zostały udostępnione pracownikom do zapoznania na wewnętrznym, współdzielonym katalogu Urzędu, a wymagane[32] pisemne oświadczenia o zapoznaniu się z treścią i zobowiązaniu do stosowania regulacji były pobierane tylko od nowo zatrudnianych pracowników. Pozostałe osoby nie złożyły takich potwierdzeń.

(akta kontroli str. 488, 583, 615, 670, 808, 810, 812, 814)

Zarządzeniem Burmistrza Zelowa nr 120.15.2015 z dnia 23 czerwca 2015 r. powołano Administratora Bezpieczeństwa Informacji (od 25 maja 2018 r.- Inspektora Ochrony Danych, odpowiedzialnego za m.in. opracowanie, wdrożenie, przegląd i modyfikację wskazanych procedur), a także Administratora Systemu Informatycznego - realizującego zadania w zakresie bezpieczeństwa informatycznego.

(akta kontroli str. 37-40, 137, 687-689)

13. Obowiązek zapewnienia aktualności regulacji wewnętrznych, wynikający z § 20 ust. 2 pkt 1 Rozporządzenia KRI, zawarty został w rozdziale 12 *Polityk* i zakładał, że przeglądy takie powinny być przeprowadzane minimum raz na rok.

W okresie 2016-2020 nie prowadzono formalnych przeglądów dokumentów stanowiących SZBI. Aktualizację „Polityki Bezpieczeństwa Informacji i Ochrony Danych Osobowych" przeprowadzono tylko raz, z dniem 21 czerwca 2018 r., w związku z wejściem w życie RODO oraz związaną z tym zmianą struktury organizacyjnej Urzędu.

(akta kontroli str. 488, 614-615, 756-757, 801, 803)

14. *Polityki* obejmowały zakresem m.in. organizację przetwarzania danych osobowych, identyfikację zagrożeń (analiza ryzyk), infrastrukturę przetwarzania danych osobowych, zasady udostępniania tych danych i postępowania przy naruszeniu ich bezpieczeństwa, odpowiedzialność osób upoważnionych do przetwarzania danych osobowych, zasady funkcjonowania monitoringu wizyjnego.

---

[27] Do dnia 20 czerwca 2018 r.

[28] Wprowadzona zarządzeniem Burmistrza Zelowa nr 120/14/2015 z dnia 19 czerwca 2015 r.

[29] Wprowadzona zarządzeniem Burmistrza Zelowa nr 120/14/2015 z dnia 19 czerwca 2015 r.

[30] Wprowadzona zarządzeniem Burmistrza Zelowa nr 120.8.2018 z dnia 21 czerwca 2018 r.

[31] Stanowiąca załącznik nr 1 do zarządzenia Burmistrza Zelowa nr 120/7/2013 z 23 maja 2013 r.

[32] Rozdział 13 ust. 3 „Polityki Bezpieczeństwa Informacji i Ochrony Danych Osobowych" i „Polityki Bezpieczeństwa Informacji", rozdział 14 ust. 3 „Instrukcji określającej sposób zarządzania systemem informatycznym służącym do przetwarzania danych osobowych".

Integralnym dokumentem *Polityk* była *Instrukcja*, stanowiąca wytyczne w zakresie m.in.: nadawania i rejestrowania uprawnień, metod i środków uwierzytelniania, procedur podczas pracy użytkowników systemu, korzystania z internetu i poczty elektronicznej, tworzenia kopii zapasowych, zabezpieczania i dostępu do systemu informatycznego podmiotów zewnętrznych.

(akta kontroli str. 163, 467-686)

15. Urząd nie został wyposażony w oprogramowanie dedykowane elektronicznej inwentaryzacji zasobów informatycznych, obejmujące ich rodzaj i konfigurację, a także zawierające informacje, w jaki sposób elementy te są ze sobą powiązane (tzw. bazę konfiguracji CMDB[33]). Z wyjaśnień Burmistrza wynikało, że planowany od pięciu lat zakup, był corocznie odraczany z powodów finansowych. Prowadzony wykaz sprzętu i oprogramowania informatycznego, nie spełniał wymagań określonych w § 20 ust. 2 pkt 2 Rozporządzenia KRI, pod kątem utrzymywania aktualności inwentaryzacji sprzętu i oprogramowania służącego do przetwarzania informacji, obejmującej ich rodzaj i konfigurację. Spośród 15 pozycji zasobów informatycznych[34] poddanych szczegółowej analizie, pięć było zgodnych z prowadzonym w postaci pliku tekstowego rejestrem, w zakresie: numerów inwentarzowych, przypisanych użytkowników sprzętu oraz zainstalowanego oprogramowania. W pozostałych 10 przypadkach rozbieżności pomiędzy wykazem a stanem faktycznym dotyczyły: rodzaju zainstalowanego oprogramowania (dziewięć przypadków), wersji zainstalowanego oprogramowania (dwa przypadki), bądź marki użytkowanego sprzętu (trzy przypadki).

Zgodnie z prowadzonym rejestrem posiadane zasoby informatyczne zostały odpowiednio przypisane do osób, które użytkowały dany sprzęt, choć takie powierzenie nie następowało w sposób sformalizowany (brak dokumentów poświadczających moment przekazania i przyjęcia odpowiedzialności przez pracowników za konkretne elementy wyposażenia w dziewięciu spośród 15 przypadków).

(akta kontroli str. 690-730, 799, 831-832, 837-838, 844, 857)

16. Weryfikacja[35] możliwości zainstalowania nieautoryzowanego oprogramowania na komputerach użytkowanych przez pracowników, niebędących pracownikami służb informatycznych Urzędu wykazała, że taka instalacja była możliwa w przypadku dwóch z dziesięciu komputerów poddanych próbie. Stwierdzona sytuacja stanowiła o niewystarczającej realizacji wymagań określonych w § 20 ust. 2 pkt 4 Rozporządzenia KRI, pod kątem adekwatnego przydzielania uprawnień osobom zaangażowanym w proces przetwarzania informacji.

(akta kontroli str. 731-742, 744-745)

17. Tylko w jednym na 15 wyłonionych losowo[36] przypadków rozwiązania stosunku pracy z pracownikiem, jego konto w systemie informatycznym zostało niezwłocznie zablokowane. W 14 pozostałych przypadkach zasoby pozostawały dostępne, przy podaniu loginu i hasła, przez okres od 20 dni do nawet 17 miesięcy od dnia

---

[33] Ang. *Configuration Management Database*, która umożliwia m.in. odtworzenie infrastruktury teleinformatycznej po katastrofie lub innym zdarzeniu losowym.

[34] W tym: 10 komputerów, dwa laptopy, jeden serwer, jeden router i jedna drukarka, dobrane w sposób celowy spośród łącznie: 61 szt. komputerów stacjonarnych oraz serwerów, 10 szt. laptopów, 38 szt. drukarek, sześciu kserokopiarek i trzech routerów.

[35] Do próby wytypowano 10 komputerów, w tym: pięć komputerów stacjonarnych, wyłonionych w sposób losowy spośród 54 komputerów użytkowanych w Urzędzie oraz pięć laptopów/notebooków, wybranych w sposób celowy, spośród 10 laptopów będących na stanie Urzędu.

[36] Weryfikacją objęto próbę 15 byłych pracowników Urzędu, dobranych w sposób losowy spośród 25 osób, które w latach 2016-2020 zakończyły pracę w Urzędzie Miejskim w Zelowie.

zakończenia pracy tych osób. W zakresie blokownia kont lub odbierania uprawnień dostępu nie sporządzano formalnych wniosków; dyspozycja była przekazywana ustnie przez Kierownika Referatu Organizacyjnego odpowiedzialnym za te czynności Informatykowi oraz Inspektorowi Ochrony Danych.

(akta kontroli str. 343-346, 746-752)

18. Do prowadzenia audytu wewnętrznego z zakresu bezpieczeństwa informacji, oprócz Audytora Wewnętrznego, upoważnionym był także Inspektor Ochrony Danych[37], w którego kompetencjach leżał audyt zgodności przetwarzania danych z przepisami o ochronie danych osobowych.

Audytor Wewnętrzny przeprowadził w 2016 r. dwa zadania zapewniające: „Audyt bezpieczeństwa i systemów teleinformatycznych w wybranym obszarze działalności Urzędu Miejskiego w Zelowie" oraz „Audyt bezpieczeństwa systemów teleinformatycznych w placówkach organizacyjnych Gminy Zelów". Po pierwszym z zadań, w związku z niestwierdzeniem uchybień, nie zostały wystosowane do kierownictwa Urzędu wnioski lub inne rekomendacje. Weryfikację realizacji zaleceń, sformułowanych w wyniku drugiego z audytów, przeprowadzono w 2017 r., w formie czynności sprawdzających. Zalecenia te związane były z dokonaniem aktualizacji dokumentów wewnętrznych, dotyczących ochrony danych osobowych, zakupem zewnętrznych pamięci masowych celem dokonywania kopii zapasowych i zrzutów pamięci systemu oraz usunięciem z komputerów, na których przetwarzane były dane osobowe, oprogramowania z przeznaczeniem edukacyjnym. Wszystkie jednostki udzieliły informacji o sposobie wykorzystania rekomendacji, które - po analizie Audytora - zostały uznane za zrealizowane i prawidłowo wdrożone. Audytor nie sformułował uwag po przeprowadzonych czynnościach sprawdzających.

W kolejnych latach nie zaplanowano i nie prowadzono zadań audytowych z zakresu bezpieczeństwa informacji.

(akta kontroli str. 163, 488, 615, 753-795, 800, 815-816, 831, 836-837)

Stwierdzone nieprawidłowości

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

1. Pracownicy Referatu Organizacyjnego nie dochowali należytej staranności przy zawieraniu umów z producentem systemu SEMP, obowiązujących w latach 2016-2020, bowiem w ich treści nie określono rodzajów występujących kategorii zgłoszeń (np. błąd krytyczny, poważny, drobny) oraz czasu na usunięcie ewentualnych usterek tego oprogramowania, przez co nie zagwarantowano maksymalnego czasu, po jakim ma być przywrócone prawidłowe funkcjonowanie systemu. Ponieważ w latach 2016-2020 (I półrocze) nie wystąpiły usterki systemu SEMP, powyższe nie skutkowało konsekwencjami. Kierownik Referatu Organizacyjnego, odpowiedzialnego za realizację przedmiotowych umów i funkcjonowanie systemu Elektronicznego Zarządzania Dokumentacją (EZD) wyjaśnił, że brak zapisów umownych gwarantujących prawidłowe działanie SEMP wynikał z niskiej awaryjności systemu. Według wyjaśnień Burmistrza, wsparcie techniczne ze strony producenta realizowane było natychmiast, bez konieczności ponoszenia dodatkowych opłat.

   (akta kontroli str. 16, 277-306, 798, 808, 810-811, 830, 835)

2. Zamieszczone na stronie internetowej Urzędu informacje o możliwości załatwienia spraw drogą elektroniczną były niekompletne i trudne do odnalezienia. Pomimo iż na stronie internetowej Urzędu przewidziano sposób komunikowania zainteresowanym o sposobie i warunkach realizacji e-usług poprzez ePUAP, informacje tam zawarte nie wskazywały spraw możliwych do

[37] Odpowiednio przed 2018 r. - Administrator Bezpieczeństwa Informacji.

procedowania drogą elektroniczną. Wyszukanie tych danych wymagało przeanalizowania zakresu świadczonych usług na stronie BIP Urzędu, które nie były kompletne i aktualne w tym zakresie, bowiem wskazywały możliwość załatwienia jedynie pięciu rodzajów spraw prowadzonych przez Referat Obywatelski. Ponadto na stronie internetowej Urzędu nie zawarto informacji o użyciu e-dowodów przy kontaktach z Urzędem drogą elektroniczną. Burmistrz wyjaśnił, że Referat ds. Promocji, Informacji i Strategii na bieżąco starał się zamieszczać na stronie internetowej Gminy aktualności przekazywane przez urzędników, a brak informacji o e-dowodzie tłumaczył niedopatrzeniem.

(akta kontroli str. 99-107, 309-316, 830, 836)

3. W okresie od 1 lipca 2018 r. do 30 czerwca 2020 r. nie wszystkim pracownikom Urzędu, zaangażowanym w proces przetwarzania informacji, zapewniono szkolenia z zakresu bezpieczeństwa informacji, wymagane § 20 ust. 2 pkt 6 Rozporządzenia KRI. W zorganizowanej formie podnoszenia wiedzy z zakresu bezpieczeństwa informacji w systemach informatycznych, w 2019 r., wzięło udział czterech spośród 66 przetwarzających informacje pracowników. W pozostałych objętych analizą latach, w przedmiotowym zakresie szkolenia nie były organizowane. Burmistrz wyjaśnił, że plany szkoleń były opracowywane na podstawie potrzeb corocznie zgłaszanych przez kierowników referatów oraz osoby zajmujące samodzielne stanowiska, w wyniku czego na 2018 r. i 2019 r. zaplanowano szkolenia wewnętrzne z zakresu ochrony danych osobowych (przy czym to w 2019 r. nie zostało zrealizowane), natomiast na 2020 r. nie zgłoszono szkoleń obejmujących bezpieczeństwo informacji. Inspektor Ochrony Danych wyjaśnił, że sytuacja wynikała z niedopatrzenia spowodowanego nadmiarem obowiązków na stanowisku pracy.

(akta kontroli str. 137, 181, 343-466, 844, 856-857)

4. W Urzędzie nie opracowano i nie wdrożono SZBI, a w szczególności Polityki Bezpieczeństwa Informacji, zgodnej z wymogami § 20 ust. 1 Rozporządzenia KRI. Przywołany przepis stanowił, że *podmiot realizujący zadania publiczne opracowuje i ustanawia, wdraża i eksploatuje, monitoruje i przegląda oraz utrzymuje i doskonali system zarządzania bezpieczeństwem informacji zapewniający poufność, dostępność i integralność informacji z uwzględnieniem takich atrybutów, jak autentyczność, rozliczalność, niezaprzeczalność i niezawodność.*

   Burmistrz wyjaśnił, że nie wdrożono kolejnych regulacji wewnętrznych, ponieważ obowiązujące w Urzędzie *Polityki* i *Instrukcja* były wystarczające do zapewnienia bezpieczeństwa informacji, a procedury w zakresie ochrony danych osobowych automatycznie chroniły też bezpieczeństwo informacji.

   NIK podkreśla jednak, że obszar ochrony danych osobowych jest obszarem węższym niż SZBI, bowiem nie wszystkie przetwarzane informacje zawierają dane osobowe. Ponadto § 20 ust. 3 Rozporządzenia KRI wskazuje, że wymagania określone w ust. 1 przywołanego rozporządzenia uznaje się za spełnione, jeżeli system zarządzania bezpieczeństwem informacji został opracowany na podstawie Polskiej Normy PN-ISO/IEC 27001 „Technika informatyczna. Techniki bezpieczeństwa. Systemy zarządzania bezpieczeństwem informacji. Wymagania", a ustanawianie zabezpieczeń, zarządzanie ryzykiem oraz audytowanie odbywa się na podstawie odpowiednich Polskich Norm[38]. Wskazane przez Urząd regulacje nie spełniały tych wymogów.

   (akta kontroli str. 163, 467-686, 756-757, 798-799, 826, 830, 836)

[38] W tym: PN-ISO/IEC 27002 - w odniesieniu do ustanawiania zabezpieczeń, PN-ISO/IEC 27005 – w odniesieniu do zarządzania ryzykiem, PN-ISO/IEC 24762 - w odniesieniu do odtwarzania techniki informatycznej po katastrofie w ramach zarządzania ciągłością działania.

5. Rejestr sprzętu i oprogramowania informatycznego prowadzony był w Urzędzie w sposób nierzetelny i nie spełniał wymagań określonych w § 20 ust. 2 pkt 2 Rozporządzenia KRI. Zgodnie ze wskazanym przepisem, zarządzanie infrastrukturą informatyczną wymagało utrzymywania aktualności inwentaryzacji sprzętu i oprogramowania służącego do przetwarzania informacji obejmującej ich rodzaj i konfigurację. Tymczasem, na 15 zweryfikowanych zasobów informatycznych (dziesięciu komputerów, dwóch laptopów, serwera, routera i drukarki) pełną zgodność z prowadzonym spisem potwierdzono dla pięciu zasobów (tj. 33%), natomiast w pozostałych dziesięciu przypadkach wykaz nie zawierał aktualnych, a możliwych do zweryfikowania danych o zainstalowanym oprogramowaniu (dziewięć przypadków), wersji zainstalowanego oprogramowania (dwa przypadki) bądź modelu użytkowanego sprzętu (trzy przypadki). Burmistrz wyjaśnił, że zaistniałe różnice wynikały z ciągłych zmian specyfikacji technicznych aplikacji dziedzinowych i wymagań dla poszczególnych stanowisk pracy oraz, że aktualizacje rejestru nie zawsze były prowadzone na bieżąco z uwagi na nadmiar obowiązków odpowiedzialnych pracowników.

(akta kontroli str. 690-728, 799, 831-832, 837-838)

6. Wbrew § 20 ust. 2 pkt 4 Rozporządzenia KRI, w przypadku dwóch z dziesięciu poddanych weryfikacji komputerów, Informatyk nie ustanowił odpowiednich zabezpieczeń gwarantujących użytkownikom uprawnienia adekwatne do realizowanych zadań. W konsekwencji możliwym stało się samodzielne zainstalowanie przez pracowników nieautoryzowanego oprogramowania na komputerach[39]. Wymóg nieprzyznawania praw administracyjnych do systemu operacyjnego, a co się z tym wiąże - zapobiegania możliwości dokonywania instalacji, wynikał ponadto z praktyki określonej w załączniku A normy PN-ISO/IEC 27001:2014-12 (punkt A.9.2.3) i stanowił, że przydzielanie i wykorzystywanie praw uprzywilejowanego dostępu należało ograniczyć i nadzorować. Informatyk wyjaśnił, że dane stanowiska miały podwyższony poziom uprawnień z uwagi na prowadzone prace serwisowe. W trakcie trwania kontroli NIK komputery obu użytkowników zostały wymienione, a nadane na nowych zasobach informatycznych uprawnienia nie pozwalały na instalację nieautoryzowanego oprogramowania.

(akta kontroli str. 731-739, 744-745, 805-807)

7. W przypadku 14 z 15 zweryfikowanych kont pracowników, którzy w latach 2016-2020 rozwiązali stosunek pracy z Urzędem, zmiana uprawnień dostępu do zasobów komputera nie była dokonywana (konta pięciu osób) lub była przeprowadzana z opóźnieniem (dziewięć kont), co stanowiło naruszenie § 20 ust. 2 pkt 5 Rozporządzenia KRI. Z wyjaśnień Inspektora Ochrony Danych wynikało, że w ramach zmiany serwerów[40], w latach 2016-2018, stopniowo przełączano konta pracowników i nie zablokowano pięciu kont tych pracowników, którzy zakończyli pracę zanim nastąpiła migracja kont, zaś kolejne osiem osób, których konta zostały przeniesione na nowy serwer, z dniem utworzenia konta na nowym serwerze straciło dostęp do swoich zasobów i danych na serwerze starym. Zablokowanie kont istniejących w ramach nowego serwera dziewięciu osobom, po rozwiązaniu z nimi stosunku pracy, następowało w terminach od 20 dni do nawet 17 miesięcy. Odpowiedzialni za powstałą nieprawidłowość Inspektor Ochrony Danych oraz Informatyk wyjaśnili, że logowanie się użytkowników w przypadku kont niezablokowanych, znajdujących się na tzw. „starym serwerze", wymagałoby

[39] Komputery o numerach inwentarzowych: UM.OT/491/02577 i UM.OT/491/03414.
[40] Z Windows Serwer 2003 na Windows Serwer 2012 R2.

posiadania specjalistycznej wiedzy z zakresu informatyki i - poza nazwą użytkownika oraz hasłem - niezbędna byłaby również umiejętność zmiany domeny. Z wyjaśnień wynikało także, że zwłoka w blokowaniu kont osób, które kończyły zatrudnienie uzasadniona była przenoszeniem danych na konto osoby, która przejmowała obowiązki po pracowniku.

(akta kontroli str. 26, 33, 49, 746-752, 799-800, 802, 804-807)

8. W latach 2018-2020 nie zaplanowano i nie przeprowadzono audytu z zakresu bezpieczeństwa informacji, wymaganego § 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.
   Audytor Wewnętrzny wyjaśnił, że bezskutecznie sugerował Kierownictwu potrzebę zlecenia wykonania ekspertyzy przez podmiot zewnętrzny, z uwagi na brak uprawnień i fachowej wiedzy do przeprowadzenia takiego rodzaju audytu. Inspektor Ochrony Danych w wyjaśnieniach wskazał na podjęcie w 2018 r. próby przeprowadzenia audytu, która spotkała się z brakiem zatwierdzenia do realizacji przez ówczesnego Burmistrza. Z wyjaśnień Burmistrza wynikało, że audyt nie został powierzony Inspektorowi Ochrony Danych, ze względu na ryzyko niedochowania obiektywizmu i niezależności od audytowanego obszaru, zaś zlecenie zewnętrznej firmie było odraczane, w związku z pilniejszymi potrzebami wydatkowania środków z budżetu Miasta.

   (akta kontroli str. 163, 488, 615, 753-795, 800, 815-816, 831, 836-837)

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. W umowach zawieranych z producentem systemu elektronicznego obiegu dokumentów określić czas reakcji na usunięcie ewentualnych usterek i błędów tego oprogramowania.
2. Zaktualizować zakres informacji udostępnianych na stronach internetowych Urzędu, wskazujących na rodzaj świadczonych przez Urząd e-usług oraz wymagań, jakie należy spełnić, by realizować sprawy drogą elektroniczną.
3. Zapewnić okresowe szkolenia pracowników Urzędu z zakresu bezpieczeństwa informacji.
4. Opracować i wdrożyć system zarządzania bezpieczeństwem informacji, zgodnie z § 20 ust. 1, w zw. z ust. 3 rozporządzenia KRI.
5. Zapewnić rzetelność informacji o wykorzystywanych zasobach informatycznych, obejmujących ich rodzaj i konfigurację, stosownie do wymogów § 20 ust. 2 pkt 2 rozporządzenia KRI.
6. Bezzwłocznie aktualizować uprawnienia dostępu do zasobów komputerowych pracownikom zaangażowanym w proces przetwarzania informacji, zmieniającym zakres uprawnień lub rozwiązującym stosunek pracy z Urzędem.
7. 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 NIK w Łodzi. Prawo zgłaszania zastrzeżeń, zgodnie z art. 61b 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, 18 września 2020 r.

Najwyższa Izba Kontroli
Delegatura w Łodzi
Dyrektor
Przemysław Szewczyk

Kontroler
Ewa Tworkowska
inspektor k.p.

E. Tworkowska
.....
podpis

P. Szewczyk
.....
podpis