NAJWYŻSZA IZBA KONTROLI
Delegatura we Wrocławiu

LWR.410.014.03.2020

Pan
Tomasz Frischmann
Burmistrz Miasta Oława
Urząd Miejski w Oławie
Plac Zamkowy 15
55-200 Oława

WYSTĄPIENIE POKONTROLNE

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

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

I. Dane identyfikacyjne

Jednostka kontrolowana	Urząd Miejski w Oławie[1], Plac Zamkowy 15, 55-200 Oława
Kierownik jednostki kontrolowanej	Tomasz Frischmann, Burmistrz Miasta Oława[2], od dnia 9 grudnia 2014 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	Od 1 stycznia 2016 r. do dnia zakończenia czynności kontrolnych, tj. do 30 września 2020 r.
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 we Wrocławiu
Kontroler	Renata Połatajko, główny specjalista kontroli państwowej, upoważnienie do kontroli nr LWR/105/2020 z 20 lipca 2020 r.

(akta kontroli str. 1-5)

[1] Dalej: Urząd lub UM Oława.
[2] Dalej: Burmistrz lub Burmistrz Miasta.
[3] Dz. U. z 2020 r. poz. 1200, dalej: ustawa *o NIK*.

II. Ocena ogólna[4] kontrolowanej działalności

OCENA OGÓLNA

Przyjęte w Urzędzie rozwiązania i zasady świadczenia usług elektronicznych umożliwiły ich sprawną oraz terminową realizację. Niemniej jednak, z wyjątkiem ochrony danych osobowych, w Urzędzie nie wprowadzono odpowiednich rozwiązań organizacyjnych w zakresie bezpieczeństwa przetwarzania informacji.

W badanym okresie udostępniono drogą elektroniczną 38 usług dla obywateli, wszystkie za pośrednictwem ogólnopolskiej platformy ePUAP. Liczba realizowanych na rzecz obywateli e-usług w I półroczu 2020 r. wyniosła 890, z czego 90,1% wykonano w dwóch ostatnich jego miesiącach. Badanie 20 e-usług wykazało, że były one kierowane do załatwienia bez zbędnej zwłoki, a obywatele otrzymywali odpowiedź lub decyzję drogą elektroniczną, a na życzenie w formie papierowej. W okresie objętym kontrolą pomocniczo wykorzystywano elektroniczny obieg dokumentów[5], zapewniając jednocześnie sprawne i nieprzerwane działanie dedykowanej mu platformy informatycznej.

Urząd posiadał aktualne informacje o zasobach informatycznych jednostki obejmujące ich rodzaj i konfigurację, a uprawnienia użytkowników komputerów objętych oględzinami nie pozwalały na zainstalowanie nieautoryzowanego oprogramowania, co spełniało wymogi 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*[6].

W wyniku kontroli NIK stwierdziła nieprawidłowości dotyczące m.in.: **[1]** nieopracowania procedur obiegu dokumentów regulujących komunikację elektroniczną w Urzędzie oraz załatwiania spraw w formie elektronicznej, w tym weryfikacji podpisów elektronicznych, co było działaniem nierzetelnym; **[2]** niezapewnienia pełnych i cyklicznych szkoleń wszystkim pracownikom w zakresie bezpieczeństwa informacji, co naruszało § 20 ust. 2 pkt 6 rozporządzenia *KRI*; **[3]** braku na stronach internetowych Urzędu[7] opisu zasad, metod dostarczania oraz wymagań dla dokumentów elektronicznych, określonych w § 3 ust. 1 pkt 2, 4 i 5 rozporządzenia Prezesa Rady Ministrów z dnia 14 września 2011 r. *w sprawie sporządzania i doręczania dokumentów elektronicznych oraz udostępniania formularzy, wzorów i kopii dokumentów elektronicznych*[8] oraz informacji o konieczności posiadania profilu zaufanego lub dowodu osobistego z warstwą elektroniczną w celu skorzystania z e-usług, o rodzajach spraw, które Urząd obsługuje drogą elektroniczną, jak również o sposobie uzyskania profilu zaufanego oraz dowodu osobistego z warstwą elektroniczną, co było działaniem nierzetelnym; **[4]** nieopracowania Systemu Zarządzania Bezpieczeństwem Informacji[9], odpowiadającego w pełni wymogom § 20 ust. 1 i 3 rozporządzenia *KRI*, a w szczególności w zakresie Polityki Bezpieczeństwa Informacji[10]; **[5]** niezapewnienia dokumentowania, czy a jeśli tak, to kiedy pracownicy uczestniczący w procesie przetwarzania informacji zostali poinformowani o wdrożeniu PBI, co było zalecane pkt A.5.1.1 załącznika A do Polskiej Normy PN-ISO/IEC 27001; **[6]** odebrania dostępu do systemu informatycznego byłemu pracownikowi dopiero po 2,5 miesiąca od daty jego zwolnienia, co naruszało § 20

[4] Najwyższa Izba Kontroli formułuje ocenę ogólną jako ocenę pozytywną, ocenę negatywną albo ocenę w formie opisowej.
[5] Dalej: EOD.
[6] Dz. U. z 2017 r. poz. 2247, dalej: rozporządzenie *KRI*.
[7] www.bip.um.olawa.pl oraz www.um.olawa.pl.
[8] Dz. U. z 2018 r. poz. 180. Dalej: rozporządzenie *w sprawie dokumentów elektronicznych*.
[9] Dalej: SZBI.
[10] Dalej: PBI.

ust. 2 pkt 4 i 5 rozporządzenia *KRI;* **[7]** niezgodnego z wymogami § 21 pkt 4 rozporządzenia *KRI* okresu przechowywania logów systemowych w usłudze Active Directory[11]; **[8]** nieprzeprowadzenia okresowego audytu wewnętrznego z zakresu bezpieczeństwa informacji w 2016 r. oraz w 2017 r., co naruszało § 20 ust. 2 pkt 14 rozporządzenia *KRI*.

III. Opis ustalonego stanu faktycznego kontrolowanej działalności

OBSZAR

Świadczenie przez Urząd Miejski w Oławie e-usług

Opis stanu faktycznego

1.1. W obowiązującej od 30 października 2014 r. „Strategii rozwoju miasta Oława – Perspektywa 2020"[12], uwzględniono zagadnienia dotyczące elektronicznego świadczenia e-usług. W ramach celu strategicznego IV.Poprawa dostępności komunikacji[13], celu operacyjnego IV.3. Rozwój społeczeństwa informacyjnego – za kierunek działania przyjęto m.in. rozwój e-usług[14] oraz podnoszenie umiejętności w zakresie wykorzystywania nowoczesnych technologii[15]. W ramach celu strategicznego VI. Rozwój aktywności społeczności miejskiej[16], celu operacyjnego VI.3. Wzmacnianie potencjału i skuteczności administracji publicznej – za kierunek działania przyjęto m.in. usprawnianie procesów w administracji publicznej (w tym rozwój e-usług publicznych oraz upowszechniania elektronicznej obsługi ludności). Strategia nie wyznacza terminu wdrożenia e-usług. Mierniki realizacji celów strategicznych zostały określone w kartach celu strategicznego, stanowiących podstawowe narzędzie w procesie monitorowania i ewaluacji Strategii. W zakresie celu strategicznego IV była to m.in. ilość usług publicznych oferowanych drogą elektroniczną, natomiast w zakresie celu strategicznego VI m.in. liczba kanałów komunikacji Urzędu Miasta z mieszkańcami[17].

Dążąc do rozwoju e-usług pozyskano w dniu 30 stycznia 2019 r.[18] dofinansowanie w ramach Regionalnego Programu Operacyjnego Województwa Dolnośląskiego na lata 2014-2020, na realizację zadania pn. „E-Oława – rozwój i poprawa dostępności elektronicznych usług administracji publicznej dla mieszkańców miasta". Głównym celem projektu jest wsparcie rozwoju elektronicznych usług publicznych w zakresie e-administracji. Projekt zakłada zwiększenie dostępności e-usług realizowanych w szczególności w obszarach: administracji publicznej, wspierania przedsiębiorczości i prowadzenia działalności gospodarczej oraz w zakresie dostępu do informacji przestrzennej GIS. Według umowy z wykonawcą z dnia 24 maja 2019 r. termin zakończenia prac wdrożeniowych określono na dzień 10 listopada 2020 r. Wynikiem realizacji projektu ma być m.in. udostępnienie elektronicznych usług publicznych w zakresie: podatków lokalnych, opłat lokalnych, informacji dotyczącej powadzonych ewidencji oraz informacji dotyczącej wykonania budżetu,

---

[11] Dalej: Usługa AD.

[12] Uchwała Nr LIII/340/14 Rady Miejskiej w Oławie z dnia 30 października 2014 r. *w sprawie uchwalenia strategicznego planu rozwoju Gminy Miasto Oława pn. „Strategia rozwoju miasta Oława – Perspektywa 2020"*, dalej: Strategia.

[13] Koordynatorem tego celu w Urzędzie jest Wydział Rozwoju Gospodarczego, Inwestycji i Zamówień Publicznych.

[14] Cyfryzacja usług publicznych ma na celu wzmocnienie komunikacji jednostek samorządu miejskiego z otoczeniem. Wykorzystanie nowoczesnych technologii i internetu ma na celu usprawnienie procesów administracyjnych w tym obsługi klientów.

[15] Miasto Oława będzie wspierało rozwój kompetencji cyfrowych wśród mieszkańców. Rozwój e-usług jest powiązany bezpośrednio z podnoszeniem umiejętności w zakresie wykorzystywania nowoczesnych technologii.

[16] Koordynatorem tego celu w Urzędzie jest Wydział Promocji, Kultury i Sportu.

[17] Miernik ten nie został zwymiarowany.

[18] Umowa nr RPDS.02.01.01-02-0010/17-00 z dnia 30 stycznia 2019 r. zawarta z Województwem Dolnośląskim, aneksowana 13 sierpnia 2019 r.

wieloletniej prognozy finansowej, wymiany informacji budżetowo-finansowych między jednostkami organizacyjnymi a gminą.

(akta kontroli str. 6-47; 354-374; 429-489; 523-524)

1.2. Według stanu na dzień 30 czerwca 2020 r. dla mieszkańców Oławy dostępnych było 38 rodzajów usług elektronicznych świadczonych w dziewięciu grupach:

- sprawy ogólne – jedna usługa;
- budownictwo, architektura, urbanistyka – jedna usługa;
- sprawy obywatelskie (dowody osobiste, meldunki, wybory) – 20 usług;
- geodezja, kartografia – jedna usługa;
- kultura, sport, turystyka, oświata – dwie usługi;
- ochrona środowiska – jedna usługa;
- podatki i opłaty – osiem usług;
- urodzenia, małżeństwa, zgony – trzy usługi;
- inne – jedna usługa.

Wszystkie wskazane wyżej e-usługi były udostępniane wyłącznie za pośrednictwem ogólnopolskiej platformy ePUAP.

Dodatkowo, w raportach z monitoringu realizacji Strategii, w kartach celu strategicznego, do usług oferowanych drogą elektroniczną zaliczano: elektroniczną skrzynkę pocztową, wirtualny cmentarz, portal mapowy oraz rozpatrywanie wniosków o wyrażenie zgody na używanie herbu Miasta Oława.

(akta kontroli str. 321; 429-455)

1.3. W I półroczu 2020 r. za pośrednictwem ogólnopolskiej platformy ePUAP zrealizowanych zostało 890 usług elektronicznych na rzecz obywateli, z czego:

- 88 usług w okresie od dnia 1 stycznia 2020 r. do dnia 29 lutego 2020 r.;
- 269 usług w okresie od dnia 1 marca 2020 r. do dnia 30 kwietnia 2020 r.;
- 533 usług w okresie od dnia 1 maja 2020 r. do dnia 30 czerwca 2020 r.

880 z tych usług (98,9% wszystkich e-usług w tym okresie) było świadczonych w obszarach: sprawy obywatelskie (539 usług); sprawy (pisma) ogólne wpływające do Urzędu (121 usług) oraz urodzenia, małżeństwa, zgony (220 usług).

Natomiast w I półroczu 2020 r. obywatele nie korzystali z usług elektronicznych dostępnych w obszarze: budownictwo, architektura, urbanistyka (usługa wydania wypisu i wyrysu ze studium uwarunkowań i kierunków zagospodarowania przestrzennego); geodezja, kartografia (usługa ustalenia numeru porządkowego budynku); kultura, sport, turystyka, oświata (oferta na realizację zadania publicznego, sprawozdanie z wykonania zadania publicznego); ochrona środowiska (udostępnienie informacji o środowisku i jego ochronie). Mniej niż pięć przypadków realizacji e-usług odnotowano także w obszarze podatki i opłaty. W Urzędzie nie prowadzono monitoringu realizacji usług elektronicznych, w związku z czym nie były znane przyczyny niskiej realizacji e-usług w tych obszarach w I półroczu 2020 r.

Wyraźny wzrost liczby świadczonych e-usług w ostatnim z badanych okresów (od dnia 1 maja do dnia 30 czerwca 2020 r.) nastąpił w związku z odbywającymi się w tym okresie wyborami prezydenckimi. We wskazanych terminach zrealizowanych zostało 298 usług elektronicznych[19].

Ponadto istotny wzrost (powyżej 15%) w analizowanych okresach w stosunku do okresu od dnia 1 stycznia do dnia 1 lutego 2020 r. dotyczył: pism ogólnych

[19] W tym: 221 wniosków o dopisanie do spisu wyborców, 12 wniosków o wpisanie do rejestru wyborców oraz 65 zgłoszeń zamiaru głosowania korespondencyjnego dla osób głosujących w Polsce.

wpływających do Urzędu (wzrost o 329%[20]); wniosków o wydanie dowodu osobistego (wzrost o 182%[21]); zgłoszenia pobytu stałego (wzrost o 466%[22]); wydania odpisów aktów stanu cywilnego (wzrost o 300%[23]) oraz zgłoszenia urodzenia dziecka (wzrost o 462%[24]).

(akta kontroli str. 322-323)

1.4. W Urzędzie nie prowadzono monitoringu poziomu wykorzystania e-usług. Burmistrz wyjaśnił, że do czasu wdrożenia własnych usług elektronicznych Urzędu, nie dostrzega konieczności bieżącego monitorowania poziomu ich wykorzystania. Od dnia 1 stycznia 2016 r. do dnia 29 lutego 2020 r. liczba pism, które wpłynęły na elektroniczną skrzynkę podawczą[25] była znikoma. Wskazał również, że wzrost zainteresowania elektronicznymi usługami zauważono od momentu pandemii (czyli od marca 2020 r.). Liczbę pism, które wpłynęły na ESP Urzędu można wygenerować w dowolnym momencie z elektronicznego systemu obiegu dokumentów. Poinformował, że obserwuje się wzrost korzystania przez obywateli z usług świadczonych elektronicznie, jednak nie prowadzi się żadnych analiz ani dokumentów dotyczących tego zagadnienia.

(akta kontroli str. 54; 256-262)

1.5. W okresie objętym kontrolą do Urzędu wpłynęła jedna skarga w zakresie świadczenia usług publicznych w formie elektronicznej, dotycząca braku otrzymania pakietu wyborczego do głosowania korespondencyjnego. Skarga została uznana za bezpodstawną, ze względu na brak możliwości weryfikacji zgłoszonej sytuacji. Zgłoszenie takie nie wpłynęło na ESP Urzędu, a składający skargę nie przesłał Urzędowego Poświadczenia Przedłożenia takiego zgłoszenia.

Wpłynął również jeden wniosek w sprawie usprawnienia elektronicznej formy komunikacji z Urzędem poprzez wprowadzenie pakietu sześciu działań „E-Urząd+", tj. w zakresie: jednego miejsca na wnioski oraz wzory wypełniania podań, wprowadzenia Oławskiej platformy konsultacji społecznych oraz terminali w Urzędzie, elektronicznego rejestru umów, systemu monitorowania jakości usług publicznych, a także programu niskiej emisji energii cieplnej. Ze zgłoszonych propozycji unowocześnienia Urzędu nie skorzystano m.in. ze względu na konieczność poniesienia wysokich nakładów finansowych związanych z ich wdrożeniem.

(akta kontroli str. 182-196)

1.6. Stosownie do postanowień § 1 pkt 3 Instrukcji kancelaryjnej stanowiącej załącznik do 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*[26], Burmistrz Miasta wskazał, który z systemów wykonywania czynności kancelaryjnych jest podstawowym sposobem dokumentowania przebiegu załatwiania i rozstrzygania spraw dla Urzędu. Zarządzeniem[27] Burmistrza Miasta Oława z dnia

[20] Z 17 usług w okresie od dnia 1 stycznia do dnia 29 lutego 2020 r. do 56 usług w okresie od dnia 1 marca do 30 kwietnia 2020 r.
[21] Z 33 usług w okresie od dnia 1 stycznia do dnia 29 lutego 2020 r. do 60 usług w okresie od dnia 1 maja do dnia 30 czerwca 2020 r.
[22] Z ośmiu usług w okresie od dnia 1 stycznia do dnia 29 lutego 2020 r. do 28 usług w okresie od dnia 1 marca do dnia 30 kwietnia 2020 r.
[23] Z 15 usług w okresie od dnia 1 stycznia do dnia 29 lutego 2020 r. do 45 usług w okresie od dnia 1 maja do dnia 30 czerwca 2020 r.
[24] Z 13 usług w okresie od dnia 1 stycznia do dnia 29 lutego 2020 r. do 60 usług w okresie od 1 marca do 30 kwietnia 2020 r.
[25] Dalej: ESP.
[26] Dz. U. Nr 14 poz. 67 ze zm., dalej: Instrukcja kancelaryja.
[27] Nr 3/120/2011.

7 lutego 2011 r. przyjęto, że podstawowym systemem wykonywania czynności kancelaryjnych w Urzędzie jest system tradycyjny. Burmistrz nie skorzystał z możliwości wskazania wyjątków od podstawowego sposobu dokumentowania przebiegu załatwiania i rozstrzygania spraw.

Poza systemem tradycyjnym, czynności kancelaryjne były wykonywane również w systemie elektronicznego zarządzania dokumentacją[28]. Zgodnie z § 36 Regulaminu organizacyjnego[29], dokumentacja nadsyłana i składana w Urzędzie rejestrowana była przez pracowników Referatu ds. kancelaryjnych i obsługi sekretariatu w elektronicznym systemie obiegu dokumentów. Dla EOD w Urzędzie, w tym dokumentów wpływających do Urzędu poprzez ePUAP, nie opracowano i nie wdrożono wewnętrznej procedury. Nie określono wewnętrznych zasad postępowania z przesyłkami wpływającymi na ESP oraz procedur zobowiązujących pracowników do weryfikacji opatrzenia aktualnym podpisem elektronicznym dokumentów elektronicznych wpływających do Urzędu, co opisano w sekcji dotyczącej stwierdzonych nieprawidłowości. Burmistrz wyjaśnił, że w zakresie EOD również stosowana była Instrukcja kancelaryjna, a weryfikację podpisów elektronicznych przeprowadzano zgodnie z § 47 ust. 4 Instrukcji kancelaryjnej. Informacje te weryfikowali i potwierdzali podpisem pracownicy, którzy wykonywali czynności kancelaryjne.

Stosowany w Urzędzie EOD wykorzystywał system informatyczny SIDAS EZD, który automatycznie pobierał pismo, które wpłynęło na ESP. Następnie:

- pracownik punktu kancelaryjnego rejestrował pismo w elektronicznej książce podawczej systemu SIDAS EZD;
- przekazywał pismo do dekretacji, a w przypadku spraw „typowych" bezpośrednio do komórki merytorycznej;
- osoby dekretujące przekazywały pismo do załatwienia do komórki merytorycznej;
- kierownik komórki merytorycznej, kierował sprawę do załatwienia bezpośrednio do pracownika;
- pracownik zakładał sprawę, nadawał jej numer zgodny z jednolitym rzeczowym wykazem akt lub dołączał pismo do już istniejącej sprawy;
- jeśli sprawa tego wymagała, pracownik merytoryczny przygotowywał odpowiedź i wysyłał ją do zatwierdzenia przełożonemu;
- przełożony (w zależności od potrzeb) zatwierdzał lub/i podpisywał przygotowany dokument;
- pracownik po wskazaniu adresata przekazywał zatwierdzony dokument do wysyłki, którą przed wysłaniem podpisywała osoba do tego uprawniona;
- po podpisaniu wysyłki system SIDAS EZD automatycznie wysyłał dokument na elektroniczną skrzynkę podawczą Urzędu;
- ePUAP zapewniał przekazanie wysyłki z ESP Urzędu na ESP adresata.

System SIDAS EZD zapewniał weryfikację podpisów elektronicznych. Po otrzymaniu podpisanego dokumentu można było zweryfikować jego skład. Ważność podpisu można było sprawdzić na podstawie autentyczności certyfikatu elektronicznego identyfikatora podpisu oraz integralności dokumentu. Weryfikacja pozwalała stwierdzić, czy certyfikat osoby podpisującej jest uwzględniony na liście zaufanych sprawdzającego. Weryfikacja integralności dokumentu pozwalała natomiast stwierdzić, czy podpisana zawartość uległa zmianie po podpisaniu.

(akta kontroli str. 54-55; 330-350; 526-549)

[28] Proces tożamy z elektroniczny obiegiem dokumentów, stąd też dalej: EOD.

[29] Zarządzenie nr 20/120/2016 Burmistrza Miasta Oława z dnia 7 września 2016 r. *w sprawie regulaminu organizacyjnego Urzędu Miejskiego w Oławie*, ze zm.

Według stanu na dzień 30 czerwca 2020 r. bezpieczny podpis elektroniczny w Urzędzie posiadało 14 osób. Badanie 20 spraw, z których w 11 przypadkach odpowiedzi zostały udzielone elektronicznie poprzez ePUAP wykazało, że dokumenty elektroniczne podpisywane były przez kierownika lub zastępcę kierownika komórki organizacyjnej. W I półroczu 2020 r. elektronicznie zostały podpisane 404 dokumenty, przy czym najwięcej przez Sekretarza (138) oraz Burmistrza Miasta (106).
Kontrola nie wykazała przypadków, w których podpis elektroniczny danej osoby był w posiadaniu i użytkowaniu przez innego pracownika Urzędu.

(akta kontroli str. 516-522)

Realizacja e-usługi zgłoszenia urodzenia się dziecka wiązała się z przesyłaniem za pośrednictwem ePUAP skanu opatrzonego pieczęcią i podpisanego odręcznie zaświadczenia o zameldowaniu dziecka oraz skanu podpisanego odręcznie powiadomienia o nadaniu numeru PESEL, które były następnie podpisywane elektronicznie. Tym samym, dokumenty te posiadały dwa podpisy – odręczny i elektroniczny.

Burmistrz wyjasnił, że Ministerstwo Cyfryzacji nie zapewniło możliwości pobierania zaświadczeń o zameldowaniu oraz powiadomień o nadaniu numeru PESEL w formie dokumentu elektronicznego. Nie ma możliwości pobrania takich elektronicznych dokumentów z aplikacji ŹRÓDŁO. Przedmiotowe dokumenty są zgodnie z wytycznymi Dolnośląskiego Urzędu Wojewódzkiego we Wrocławiu z dnia 6 sierpnia 2018 r. drukowane, a po opatrzeniu ich pieczęcią wysyłane w formie skanu, podpisanego następnie elektronicznie.

(akta kontroli str. 256-262; 326-329; 519)

1.7. Realizacja usług elektronicznych świadczonych przez Urząd w I półroczu 2020 r. na rzecz obywateli została zbadana na próbie 20 e-usług, z których dziewięć dotyczyło urodzeń, małżeństw lub zgonów, sześć – dowodów osobistych, meldunków lub wyborów, dwie – podatków, trzy – pism ogólnych skierowanych do Urzędu. W zbadanych przypadkach sprawy otrzymane za pośrednictwem e-PUAP:

✓ były kierowane do załatwienia bez zbędnej zwłoki, w dniu przyjęcia lub kolejnym dniu roboczym;
✓ w trzech przypadkach, w których dokumenty przesłane elektronicznie nie były wypełnione poprawnie i wymagały korekt, Urząd wzywał stronę do uzupełnienia lub naniesienia poprawek, przy czym odbyło się to w dwóch przypadkach przez platformę ePUAP i w jednym przypadku telefonicznie;
✓ we wszystkich zbadanych przypadkach nie było potrzeby komunikowania się z inną jednostką administracji publicznej w celu załatwienia sprawy;
✓ Urząd korzystał z danych gromadzonych w zewnętrznych systemach/rejestrach państwowych takich jak PESEL, Rejestr Dowodów Osobistych, Baza Usług Aktu Stanu Cywilnego;
✓ uzyskanie informacji na temat aktualnego stanu załatwianej sprawy możliwe było elektronicznie w aplikacji www.obywatel.gov.pl w zakresie dowodu osobistego, w pozostałych przypadkach informację można było uzyskać na zapytanie ustne, telefoniczne lub pisemne, w tym za pomocą platformy ePUAP;
✓ w dalszym biegu czynności kancelaryjne wykonywane były elektronicznie z wykorzystaniem platformy ePUAP lub w formie papierowej.

System EOD w Urzędzie nie komunikował się automatycznie z innymi systemami informatycznymi Urzędu w zakresie przesyłania danych niezbędnych dla załatwienia sprawy. Burmistrz wskazał, że zmiany w tym zakresie planowane są do końca 2020 roku po zakończeniu wdrożenia projektu „E-Oława – rozwój i poprawa dostępności elektronicznych usług administracji publicznej dla mieszkańców miasta”.

(akta kontroli str. 518-522)

1.8. W sytuacji wystąpienia problemów technicznych w funkcjonowaniu ePUAP, korzystano w Urzędzie z oficjalnego wsparcia użytkowników znajdującego się na stronie internetowej tej platformy. W pierwszej kolejności zgłoszenie konsultowano telefonicznie, a po stwierdzeniu jego zasadności przesyłano przez formularz kontaktowy. W I półroczu 2020 r. przez formularz kontaktowy dokonano dwóch zgłoszeń awarii platformy ePUAP.

(akta kontroli str. 181; 197-203)

1.9. W latach 2016-2020 Burmistrz zawierał coroczne umowy[30] zapewniające ciągłość świadczenia usług serwisowych oraz nadzoru autorskiego nad oprogramowaniem SIDAS EZD. Wykonawca umów (producent oprogramowania) udostępniał system teleinformatyczny umożliwiający rejestrowanie i obsługę zgłoszeń serwisowych. Dodatkowo przekazywanie zgłoszeń serwisowych było możliwe e-mailowo oraz telefonicznie. Kategorie zgłoszeń klasyfikowano jako: błąd krytyczny, błąd poważny, błąd drobny oraz propozycja. Przyjęty umownie czas reakcji producenta oraz czas realizacji zgłoszenia wynosił odpowiednio od jednej godziny do jednego dnia roboczego oraz od dwóch do 14 dni roboczych i był uzależniony od kategorii zgłoszenia. W latach 2016-2020 (I półrocze) dokonano 83 zgłoszeń serwisowych.

Zapisy przedmiotowych umów gwarantowały zabezpieczenie poufności informacji uzyskanych przez wykonawcę w związku z ich realizacją pod rygorem ponoszenia odpowiedzialności odszkodowawczej oraz informowały o posiadaniu przez wykonawcę umowy wdrożonego SZBI. W odrębnych umowach określano zasady dostępu do danych i powierzenia ich przetwarzania oraz zdalnego dostępu serwisowego. Zleceniobiorca był m.in. odpowiedzialny za stosowanie wymaganego poziomu bezpieczeństwa C oraz wymagań SZBI w zakresie przetwarzania powierzonych mu danych na sprzęcie i infrastrukturze, udostępnionej mu do indywidualnego stosowania i użytkowania[31].

(akta kontroli str. 119-180; 408-426)

1.10. Według stanu na dzień 15 września 2020 r. na stronie internetowej www.um.olawa.pl była umieszczona informacja o adresie ESP, natomiast na stronie www.bip.um.olawa.pl zarówno o adresie ESP, jak i o adresie umożliwiającym przesłanie pisma na platformie ePUAP.

Ze stron internetowych Urzędu nie można było natomiast uzyskać informacji o konieczności posiadania profilu zaufanego lub dowodu osobistego z warstwą elektroniczną w celu skorzystania z e-usług, o rodzajach spraw, które Urząd obsługuje drogą elektroniczną, jak też o sposobie uzyskania profilu zaufanego oraz dowodu osobistego z warstwą elektroniczną. Na stronach Urzędu brakowało również opisu zasad, metod dostarczania oraz wymagań dla dokumentów elektronicznych wymaganych § 3 ust. 1 pkt 2 rozporządzenia *w sprawie dokumentów elektronicznych*, co opisano w sekcji dotyczącej stwierdzonych nieprawidłowości.

Osoby, którym wydawano dowód osobisty z warstwą elektroniczną informowane były, jak wskazał Burmistrz, o sprawach możliwych do załatwiania przy użyciu tego dowodu. Przekazywano im ogólną informację o e-dowodzie oraz udzielano odpowiedzi na ewentualne szczegółowe pytania. Dodatkowo osobom zainteresowanym przekazywano informację papierową, zawierającą najważniejsze informacje o e-dowodzie wskazane przez Ministerstwo Cyfryzacji. Dodatkowo taka informacja wywieszona była w gablocie przed biurem, w którym prowadzone są

[30] MK/EZD/50/2016 z 29 lutego 2016 r.; MK/EZD/75/2017 z 1 lutego 2017 r.; 82/2018 z 12 lutego 2018 r.; 89/2019 z 21 stycznia 2019 r.; 124/2020 z 4 lutego 2020 r.

[31] Np. laptop, urządzenia mobilne, przenośne urządzenia gromadzenia danych, poczta itp.

sprawy związane z wydawaniem dowodów osobistych, aby osoby oczekujące na wejście mogły się ewentualnie z nimi zapoznać.

(akta kontroli str. 244-245; 256-262; 268-269)

1.11. W latach 2016-2020 (I półrocze) pracownicy Urzędu zaangażowani w proces przetwarzania informacji wzięli udział łącznie w 16 szkoleniach zewnętrznych[32].

W 2016 r. w trzech szkoleniach udział wzięły trzy osoby[33] na ponad 90 osób biorących udział w procesie przetwarzania informacji. W 2017 r. w badanym zakresie szkoliły się dwie osoby. Szkolenia przeprowadzone w latach 2018-2019 dotyczyły zakresu ochrony danych osobowych i nie obejmowały stosowania środków zapewniających bezpieczeństwo informacji, w tym urządzeń oraz oprogramowania minimalizujących ryzyko błędów ludzkich. W 2018 r. przeprowadzono szkolenie 93 osób, natomiast w 2019 r. sześciu osób na odpowiednio 98 i 104 osoby biorące udział w procesie przetwarzania informacji. W I półroczu 2020 r. 84 osoby wzięły udział w szkoleniu teoretycznym z e-administracji. W ocenie NIK w okresie objętym kontrolą w Urzędzie nie zapewniono pełnych i cyklicznych szkoleń pracowników w zakresie bezpieczeństwa informacji co szerzej opisano w sekcji dotyczącej stwierdzonych nieprawidłowości.

(akta kontroli str. 324-325; 553-563)

1.12. Z dniem 8 stycznia 2016 r. w Urzędzie została wprowadzona[34] PBI (stanowiąca część SZBI), składająca się z: Polityki Danych Osobowych[35], Instrukcji Zarządzania Systemem Informatycznym[36] oraz Instrukcji korzystania z systemu informatycznego służącego do przetwarzania danych osobowych[37]. Wprowadzona PBI odnosiła się zatem do bezpieczeństwa danych osobowych i nie obejmowała zasobów informacji nie zawierających danych osobowych, co opisano szerzej w części dotyczącej stwierdzonych nieprawidłowości. Instrukcja Zarządzania Systemem Informatycznym[38] przeznaczona była dla pracowników zarządzających bezpieczeństwem danych osobowych, tj. dla kierownictwa Urzędu, naczelników i kierowników komórek organizacyjnych, administratora Bezpieczeństwa Informacji, pracownika ds. kadr i szkoleń oraz informatyka. Wskazana wyżej Instrukcja korzystania z systemu informatycznego służącego do przetwarzania danych osobowych (stanowiąca część PBI) określała procedury przetwarzania, ochrony i przepływu danych osobowych.

Ustalono ponadto, że:

✓ oprócz PBI do dokumentów SZBI, w Urzędzie zaliczano również Regulamin Pracy Zdalnej z dnia 6 kwietnia 2020 r.[39], Zasady funkcjonowania kontroli zarządczej z 2014 r.[40] oraz Instrukcje bezpieczeństwa pożarowego z 2016 r.[41];

---

[32] W 2016 r. – w trzech, w 2017 r. – w dwóch, w 2018 r. – w pięciu, w 2019 r. – w pięciu, w I półroczu 2020 r. – w jednym.

[33] Jedna osoba w dwóch szkoleniach i jedna w jednym szkoleniu.

[34] Zarządzenie nr 2/120/2016 Burmistrza Miasta Oława z dnia 8 stycznia 2016 r.

[35] Załącznik nr 1 do Polityki Bezpieczeństwa Informacji wprowadzonej zarządzeniem nr 2/120.2016 z dnia 8 stycznia 2016 r. Burmistrza Miasta Oława.

[36] Załącznik nr 2 do Polityki Bezpieczeństwa Informacji wprowadzonej zarządzeniem nr 2/120.2016 z dnia 8 stycznia 2016 r. Burmistrza Miasta Oława.

[37] Załącznik nr 3 do Polityki Bezpieczeństwa Informacji wprowadzonej zarządzeniem nr 2/120.2016 z dnia 8 stycznia 2016 r. Burmistrza Miasta Oława.

[38] Za podstawę prawną tego dokumentu wskazano rozporządzenie Ministra Spraw Wewnętrznych i Administracji z dnia 29 kwietnia 2004 r. *w sprawie dokumentacji przetwarzania danych osobowych oraz warunków technicznych i organizacyjnych, jakim powinny odpowiadać urządzenia i systemy informatyczne służące do przetwarzania danych osobowych* (Dz. U. Nr 100 poz. 1024).

[39] Zarządzenie nr 9/120/2020 Burmistrza Miasta Oława z dnia 6 kwietnia 2020 r. *w sprawie wprowadzenia Regulaminu Pracy Zdalnej jako elementu Systemu Bezpieczeństwa Informacji*.

[40] Zarządzenie nr 5/120/2014 Burmistrza Miasta Oława z dnia 20 marca 2014 r. *w sprawie zasad funkcjonowania kontroli zarządczej*.

[41] Zarządzenie nr 18/120/2016 Burmistrza Miasta Oława z dnia 23 sierpnia 2016 r. *w sprawie wprowadzenia instrukcji bezpieczeństwa pożarowego w budynku przy ul. Rynek 1-Ratusz w Oławie*, ze zm. oraz zarządzenie

✓ zgodnie z oświadczeniem stanowiącym załącznik nr 2.5 do Instrukcji Zarządzania Systemem Informatycznym, pracownicy Urzędu składali oświadczenie o zapoznaniu się z przepisami prawa dotyczącymi ochrony danych osobowych, ustawą o ochronie danych osobowych, rozporządzeniem w sprawie określenia podstawowych warunków technicznych i organizacyjnych, jakim powinny odpowiadać urządzenia i systemy informatyczne, służące przetwarzaniu danych osobowych oraz o zapoznaniu się z wewnętrzną instrukcją określającą sposób korzystania z systemów informatycznych, służących przetwarzaniu danych osobowych. Pracownicy składający wniosek o wyrażenie zgody na pracę zdalną, składali natomiast oświadczenie o zapoznaniu się z zasadami określonymi w Regulaminie pracy zdalnej i zobowiązaniu się do ich stosowania;
✓ w PBI przypisano nadzór nad prawidłowym przestrzeganiem przepisów o ochronie danych osobowych (Administrator Bezpieczeństwa Informacji) oraz nadzór nad systemami informatycznymi i ich prawidłowym funkcjonowaniem (Administrator Systemów Informatycznych);
✓ Urząd nie posiadał dokumentów potwierdzających, że pracownicy uczestniczący w procesie przetwarzania informacji zostali poinformowani o wdrożeniu PBI i zapoznali się z tym dokumentem, co zostało opisane w sekcji dotyczącej stwierdzonych nieprawidłowości.

(akta kontroli str. 53-54; 56-112; 550-552)

1.13. W latach 2016-2020 (I półrocze) nie dokonywano aktualizacji regulacji wewnętrznych stanowiących SZBI, o której mowa w § 20 ust. 2 pkt 1 rozporządzenia *KRI*, co opisano szerzej w sekcji dotyczącej stwierdzonych nieprawidłowości.

Przeglądy dokumentacji bezpieczeństwa informacji sprowadzały się do dokumentacji z audytów przeprowadzonych w latach 2018-2019.

(akta kontroli str. 56-118)

1.14. Dokumenty stanowiące PBI, tj. Polityka Ochrony Danych Osobowych, Instrukcja Zarządzania Systemem Informatycznym oraz Instrukcja korzystania z systemu informatycznego służącego do przetwarzania danych osobowych, nie określały innych dokumentów wykonawczych stanowiących jej uzupełnienie. Wskazane wyżej instrukcje zawierały jednak regulacje wewnętrze dotyczące bezpieczeństwa danych osobowych, m.in. w zakresie:

- środków technicznych i organizacyjnych niezbędnych dla zapewnienia poufności, integralności i rozliczalności przetwarzanych danych;
- nadawania, zmiany i odbierania upoważnień i uprawnień;
- prowadzenia szkoleń stanowiskowych;
- bezpieczeństwa fizycznego;
- monitorowania bezpieczeństwa;
- zgłaszania incydentów;
- zarządzania sprzętem i kopiami zapasowymi;
- zarządzaniem bezpieczeństwem sieciowym i oprogramowaniem;
- rozpoczęcia, zawieszenia oraz zakończenia pracy.

(akta kontroli str. 56-101)

1.15. W Urzędzie zapewniono utrzymywanie aktualności inwentaryzacji sprzętu i oprogramowania służącego do przetwarzania informacji obejmującej ich rodzaj i konfigurację, o czym mowa w § 20 ust. 2 pkt 2 rozporządzenia *KRI*.

Do monitorowania aktualności sieci i urządzeń informatycznych w Urzędzie wykorzystywano specjalistyczne oprogramowanie. Zakupiona aplikacja składała się

---

nr 26/120/2016 Burmistrza Miasta Oława z dnia 20 grudnia 2016 r. *w sprawie wprowadzenia instrukcji bezpieczeństwa pożarowego w budynku Urzędu Miejskiego w Oławie, pl. Zamkowy 15*.

z czterech modułów: proaktywnego monitorowania i wizualizacji sieci, inwentaryzacji sprzętu i oprogramowania, zdalnego wsparcia technicznego oraz ochrony danych przed wyciekiem. Obejmowała ona sprzęt, który jest lub był wpięty do sieci (w tym: komputery stacjonarne i laptopy, drukarki, switches, serwery, rutery, zasilacze UPS itp.) oraz oprogramowanie zainstalowane na komputerach. Agent programu zainstalowany na komputerach/laptopach monitorował oraz odczytywał aktualną konfigurację sprzętową, jak i zainstalowane na nich oprogramowanie. Dodatkowo program skanował sieć komputerową i wykazywał wszystkie znajdujące się w niej urządzenia. Natomiast w arkuszu Excel prowadzona była dodatkowo ewidencja sprzętu informatycznego, obejmująca informację m.in. o numerze inwentarzowym sprzętu, użytkowniku sprzętu, komórce organizacyjnej oraz opis sprzętu.

Na próbie dziesięciu komputerów służbowych (pięciu stacjonarnych[42] i pięciu laptopach[43]) sprawdzono, że dane zasobu sprzętu informatycznego były aktualne w zakresie oprogramowania przedmiotowych komputerów. Logowanie do rutera wykazanego w zasobach informatycznych Urzędu potwierdziło zgodność nazwy, adresu IP i MAC adresu. Logowanie na serwer wykazanego w zasobach informatycznych Urzędu potwierdziło zgodność nazwy, adresu IP i MAC adresu.

(akta kontroli str. 242-243)

1.16. Uprawnienia użytkowników 10 komputerów objętych oględzinami[44] nie pozwalały na zainstalowanie nieautoryzowanego oprogramowania i były adekwatne w tym zakresie do realizowanych przez nich zadań oraz obowiązków mających na celu zapewnienie bezpieczeństwa informacji, o czym mowa w § 20 ust. 2 pkt 4 rozporządzenia *KRI*.

(akta kontroli str. 242-243)

1.17. W przypadku zmiany zadań (zakresu obowiązków) osób zaangażowanych w proces przetwarzania informacji lub osób zajmujących się tym zakresem, dokonywano zmiany uprawnień, o której mowa w § 20 ust. 2 pkt 5 rozporządzenia *KRI*. Likwidacja/dezaktywacja kont dokonywana była przez informatyka na podstawie ustnej lub pisemnej informacji od kadrowej. W przypadku osoby przeniesionej do wykonywania innych czynności uprawnienia były weryfikowane, odbierane (na wniosek przełożonego) niewykorzystywane na nowym stanowisku i nadawane nowe jeśli stanowisko tego wymagało. Daty dodania oraz odebrania uprawnień były odnotowywane w Karcie uprawnień użytkownika do systemu informatycznego, stanowiącej załącznik do Instrukcji Zarządzania Systemem Informatycznym w Urzędzie Miejskim w Oławie.

Badanie przeprowadzone na próbie 15 byłych pracowników, którzy w latach 2016-2020 zakończyli zatrudnienie w Urzędzie wykazało, że wszystkie te osoby miały nieaktywne lub usunięte konta w domenie oraz użytkowanych przez siebie systemach. Karty uprawnień użytkownika do systemu informatycznego odzwierciedlały aktualny zakres uprawnień. W badanych przypadkach dla wszystkich uprawnień wskazano daty ich odebrania. Przeprowadzone badanie wykazało jednak jeden przypadek zablokowania dostępu do systemu SELWIN dopiero po 2,5 miesiąca od daty zwolnienia pracownika, co opisano w sekcji dotyczącej stwierdzonych nieprawidłowości.

W pozostałych programach z poziomu panelu administracyjnego nie było możliwości odczytania daty zablokowania/usunięcia konta. W usłudze AD także nie było

[42] K-219; K-234; K-304; K-239; K-280.
[43] K-233; K-235; K-299; K-303; K-301.
[44] W tym: K-219; K-234; K-304; K-239; K-280; K-233; K-235; K-299; K-303; K-301.

możliwości sprawdzenia tych dat z powodu przechowywania logów do 15 dni, co opisano w sekcji dotyczącej stwierdzonych nieprawidłowości.

Wyniki analizy danych dostarczonych przez producenta systemu informatycznego SIDAS EZD w zakresie dat zablokowania konta w tym systemie, wykazały, że usunięcia konta dokonywano w okresie od kilku dni do kilku miesięcy od daty odebrania uprawnień. Informatyk wyjaśnił, że opóźnienie takie może wynikać z modelu działania systemu SIDAS EZD. W systemie tym nie można zablokować konta, jedyna możliwość to jego usunięcie. Konto nie jest kasowane dopóki sprawy pracownika, któremu odebrano uprawnienia nie zostaną przypisane innym osobom lub nowemu pracownikowi.

(akta kontroli str. 246-252; 319-320)

1.18. W latach 2016-2017 w Urzędzie nie przeprowadzono audytu wewnętrznego z zakresu bezpieczeństwa informacji, co opisano w sekcji dotyczącej stwierdzonych nieprawidłowości.

W okresie od dnia 1 listopada do dnia 31 grudnia 2018 r. przeprowadzony został „Audyt bieżącego stanu bezpieczeństwa informatycznego w zakresie stosowanych systemów informatycznych", natomiast w okresie od dnia 1 listopada 2019 r. do dnia 31 marca 2020 r. „Ocena polityki bezpieczeństwa informacji w Urzędzie w zakresie ochrony danych osobowych". W 2018 r. audyt został przeprowadzony w celu analizy bieżącego stanu bezpieczeństwa informatycznego na potrzeby projektu „E-Oława – rozwój i poprawa dostępności elektronicznych usług administracji publicznej dla mieszkańców miasta", natomiast celem audytu przeprowadzonego w 2019 r. było przedstawienie Burmistrzowi zapewnienia, że system kontroli zarządczej w zakresie danych osobowych jest adekwatny, efektywny i skuteczny. Audyty zakończyły się wydaniem zaleceń/rekomendacji. Ze względu na zakres oraz charakter audyt z 2019 r. nie spełniał w pełni wymogów rozporządzenia *KRI*.

Burmistrz wyjaśnił, że zalecenia dotyczące uzupełnienia procedur w zakresie prowadzenia ewidencji kontroli legalności oprogramowania, wykazu usług sieciowych i zestawienia konfiguracji urządzeń sieciowych wynikające z audytu przeprowadzonego w 2018 r. zostaną zrealizowane przy najbliższej aktualizacji Instrukcji Zarządzania Systemem Informatycznym. Zalecenie dotyczące systemu gaśniczego w serwerowni jest analizowane pod kątem możliwości realizacji technicznej i kosztów. Jeśli wynik tej analizy będzie pozytywny środki na system gaszący zostaną zaplanowane na przyszły rok budżetowy. Zalecenia wynikające z audytu przeprowadzonego w 2019 r. są w trakcie realizacji, w tym opracowanie nowej polityki bezpieczeństwa, na co termin wykonania określono do dnia 31 grudnia 2020 r.

(akta kontroli str. 204-241; 377-380)

Stwierdzone nieprawidłowości

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

1. W Urzędzie nie opracowano procedur obiegu dokumentów regulujących komunikację elektroniczną oraz załatwiania spraw w formie elektronicznej, w tym weryfikacji podpisów elektronicznych. W ocenie NIK było to działanie nierzetelne, ponieważ pomimo przyjęcia w Urzędzie tradycyjnego sposobu dokumentowania, część spraw dokumentowana była elektronicznie.

Burmistrz wyjaśnił, że w Urzędzie nie opracowano wewnętrznych procedur obiegu dokumentów regulujących komunikację elektroniczną, ponieważ sposób obiegu dokumentów uregulowany jest w Instrukcji kancelaryjnej. W ocenie Burmistrza, dokument ten w sposób szczegółowy i kompletny reguluje obieg dokumentów w Urzędzie. Informatyczny system elektronicznego obiegu dokumentów SIDAS zapewnia obieg dokumentów zgodny z ww. Instrukcją kancelaryjną.

NIK nie podziela ww. stanowiska, ponieważ do spraw załatwianych elektronicznie winna zostać opracowna procedura obiegu dokumentów, która nie wynika z Instrukcji kancelaryjnej, gdyż w Urzędze przyjęto tradycyjny sposób dokumentowania obiegu spraw.

(akta kontroli str. 54-55; 256-262; 330-350)

2. W okresie objętym kontrolą w Urzędzie nie zapewniono pełnych i cyklicznych szkoleń wszystkim pracownikom zaangażowanym w zakresie bezpieczeństwa informacji, tj. uwzględniających m.in.: zagrożenia bezpieczeństwa informacji, skutki naruszenia bezpieczeństwa informacji, w tym odpowiedzialność prawną, co naruszało § 20 ust. 2 pkt 6 rozporządzenia *KRI.*

Burmistrz wyjaśnił, że w kontrolowanym okresie szkolenia z zakresu, o których mowa w § 20 ust. 2 pkt 6 rozporządzenia *KRI* odbyli pracownicy, którzy byli bezpośrednio odpowiedzialni za zapewnienie bezpieczeństwa informacji. W październiku 2015 r. wszyscy pracownicy Urzędu zaangażowani w proces przetwarzania informacji zostali przeszkoleni z omawianego zakresu podczas szkolenia pt.: „Zagrożenia przy przetwarzaniu danych osobowych". Szkolenie to, uwzględniało tematy dotyczące zagrożenia bezpieczeństwa informacji oraz skutki naruszenia bezpieczeństwa informacji (w tym odpowiedzialność prawną). Ponadto, każdy nowozatrudniony pracownik przed przystąpieniem do przetwarzania informacji był zobowiązany do zapoznania się z wewnętrznymi regulacjami dotyczącymi bezpieczeństwa informacji, podpisywał oświadczenie o zapoznaniu się z nimi oraz wykaz przepisów prawnych, w tym informujących o odpowiedzialności karnej. Dodatkowo wskazał, że niezależnie od powyższego jeszcze w tym roku zostanie przeprowadzone szkolenie z zakresu bezpieczeństwa informacji dla wszystkich pracowników Urzędu zaangażowanych w proces przetwarzania informacji.

(akta kontroli str. 256-262; 324-325)

3. Na stronach internetowych[45] Urzędu nie zamieszczono opisu zasad, metod dostarczania oraz wymagań dla dokumentów elektronicznych, w tym o:

- maksymalnym rozmiarze dokumentu elektronicznego wraz z załącznikami (wyrażonym w megabajtach), możliwym do doręczenia za pomocą elektronicznej skrzynki podawczej, nie mniejszym niż pięciu megabajtów (§ 3 ust. 1 pkt 2 rozporządzenia *w sprawie dokumentów elektronicznych*);
- rodzajach informatycznych nośników danych, na których może zostać doręczony dokument elektroniczny (§ 3 ust. 1 pkt 4 rozporządzenia *w sprawie dokumentów elektronicznych*);
- rodzajach informatycznych nośników danych, na których może zostać zapisane urzędowe poświadczenie odbioru (§ 3 ust. 1 pkt 5 rozporządzenia *w sprawie dokumentów elektronicznych*).

Nie udostępniono również informacji o konieczności posiadania profilu zaufanego lub dowodu osobistego z warstwą elektroniczną w celu skorzystania z e-usług, o rodzajach spraw, które Urząd obsługuje drogą elektroniczną, jak też o sposobie uzyskania profilu zaufanego oraz dowodu osobistego z warstwą elektroniczną, co było działaniem nierzetelnym.

Burmistrz wyjaśnił, że informacja taka jest w trakcie opracowywania i w najbliższych dniach zostanie umieszczona na stronach Urzędu www.bip.um.olawa.pl oraz www.um.olawa.pl.

(akta kontroli str. 244-245; 256-262)

[45] www.bip.um.olawa.pl oraz www.um.olawa.pl.

4. W Urzędzie nie opracowano i nie wdrożono SZBI odpowiadającego w pełni wymogom § 20 ust. 3 rozporządzenia *KRI*, a w szczególności w zakresie PBI. Wprowadzone zarządzeniem Burmistrza z dnia 8 stycznia 2016 r. dokumenty odnosiły się do systemów przetwarzających dane osobowe i tym samym nie obejmowały wszystkich danych jakie były przetwarzane w Urzędzie.

Zgodnie bowiem z § 20 ust. 3 rozporządzenia *KRI*, wymagania w zakresie systemu zarządzania bezpieczeństwem informacji uznaje się za spełnione jeżeli system ten został opracowany na podstawie Polskiej Normy PN-ISO/IEC 27001, a ustanawianie zabezpieczeń, zarządzanie ryzykiem oraz audytowanie odbywa się na podstawie Polskich Norm związanych z tą normą, w tym: PN-ISO/IEC 27002, PN-ISO/IEC 27005, PN-ISO/IEC 24762. W pkt 5.1.1 normy PN-ISO/IEC 27002[46], wskazano opracowanie i stosowanie dokumentu polityki bezpieczeństwa informacji oraz zalecenia w tym zakresie. Wprowadzona w Urzędzie PBI nie spełnia wszystkich wymogów przytoczonych norm i obejmowała węższy obszar.

Burmistrz wyjaśnił, że dokumenty stanowiące PBI, zawierają m.in. zapisy dotyczące ochrony danych osobowych, jednak większość procedur odnosi się do bezpieczeństwa informacji w ogóle. W praktyce procedury stosowane do ochrony danych osobowych obejmują ochronę wszelkich informacji wytwarzanych w Urzędzie. Jeśli w procedurach zawartych w PBI opisano np. zasady dostępu do systemu informatycznego i użyto niefortunnie sformułowania „służącego do przetwarzania danych osobowych" zamiast „służącego do przetwarzania informacji", to oczywiście nie oznacza, że zapisy tej procedury nie obejmują ochroną wszystkich innych informacji przetwarzanych w Urzędzie. W praktyce procedura ta (jak wiele innych w Polityce) jest stosowana do wszystkich informacji – nie tylko do danych osobowych. Wskazał również, że przy konstruowaniu nowego dokumentu (nowej Polityki Bezpieczeństwa) w procedurach zostaną uwzględnione zapisy nieograniczające się wyłącznie do danych osobowych.

(akta kontroli str. 56-112; 377-380)

5. Obowiązująca w Urzędzie PBI z 2016 r. nie została zaktualizowana w związku ze zmianami zachodzącymi w otoczeniu. Nie uwzględniono w niej np. zapisów dotyczących wprowadzonego od dnia 25 maja 2018 r. rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r.[47], *w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE* (ogólne rozporządzenie o ochronie danych). Tym samym naruszono postanowienia § 20 ust. 2 pkt 1 rozporządzenia *KRI*.

Burmistrz wyjaśnił, że jedyną zmianą, którą wprowadziła nowa ustawa o ochronie danych osobowych, a mającą wpływ na zapisy w PBI był art. 158 ust. 1, zgodnie z którym osoba pełniąca w dniu 24 maja 2018 r. funkcję administratora bezpieczeństwa informacji staje się inspektorem ochrony danych. W ocenie Burmistrza nie jest to zmiana mająca wpływ na ustalone w PBI procedury, zwłaszcza, że osoba, która pełniła funkcję Administratora Bezpieczeństwa Informacji została Inspektorem Ochrona Danych.

NIK wskazuje, że ww. rozporządzenie nakłada na organy administracji publicznej szereg obowiązków związanych z ochroną danych osobowych, polegających nie tylko na wyznaczeniu inspektora ochrony danych. Powyższe zostało potwierdzone wynikami audytu[48] – Ocena polityki bezpieczeństwa informacji w Urzędzie Miejskim w zakresie ochrony danych osobowych, które wykazały m.in. konieczność

[46] Technika informatyczna. Techniki bezpieczeństwa. Praktyczne zasady zabezpieczania informacji.
[47] Dalej: RODO.
[48] Przeprowadzonego od listopada 2019 r. do marca 2020 r.

wprowadzenia w obowiązującej w Urzędzie PBI zmian polegających na uregulowaniu np. procesów w zakresie prowadzenia rejestru czynności przetwarzania (art. 30 ust. 1 i 2 RODO). Zmiana w otoczeniu była zatem na tyle istotna i ważna, że należało w tym zakresie dokonać aktualizacji PBI, aby wypełnić obowiązek zapisany w § 20 ust. 2 pkt 1 rozporządzenia *KRI*.

(akta kontroli str. 53-112; 210-241; 253-262)

6. W Urzędzie nie zapewniono dokumenowania potwierdzającego, czy a jeśli tak, to kiedy pracownicy uczestniczący w procesie przetwarzania informacji zostali poinformowani o wdrożeniu PBI, o czym mowa w pkt A.5.1.1 załącznika A do Polskiej Normy PN-ISO/IEC 27001[49].

Burmistrz wyjaśnił, że wszystkie zarządzenia są umieszczane na serwerze w folderze, do którego mają dostęp wszyscy pracownicy Urzędu zaangażowani w proces przetwarzania informacji i w dowolnym momencie mogą się z nim zapoznać. Procedury dotyczące pracowników wprowadzone w PBI w 2016 r. pokrywały się z procedurami zawartymi we wcześniejszej Polityce. Zmiany wprowadzone w 2016 r. dotyczyły zapisów wynikających z rozporządzenia *KRI* i dotyczyły głównie Informatyka i Administratora Bezpieczeństwa Informacji, którzy uczestniczyli w przygotowaniu tego dokumentu i znali jego zapisy. Każdy nowo zatrudniany pracownik otrzymuje PBI do zapoznania się oraz jest instruowany przez Inspektora Ochrony Danych o najważniejszych elementach związanych z bezpieczeństwem informacji i procedurami zawartymi w tym dokumencie. Od 2016 r. istniał obowiązek złożenia oświadczenia o zobowiązaniu się do przestrzegania zasad przepisów dotyczących ochrony danych osobowych i wewnętrznych procedur dotyczących korzystania z systemów informatycznych (załącznik nr 2.5 do Instrukcji Zarządzania Systemem Informatycznym stanowiącej załącznik Nr 2 do Polityki Bezpieczeństwa). Wskazał również, że w nowej PBI zostanie przygotowany wzór oświadczenia zawierający szerszy zakres zobowiązania pracownika do ochrony informacji. Po opracowaniu nowej PBI wszyscy pracownicy zostaną zapoznani z tym dokumentem.

(akta kontroli str. 56-112; 256-262)

7. Dostęp do systemu SELWIN dla jednego zwolnionego pracownika zablokowano dopiero po 2,5 miesiąca od daty odebrania uprawnień, co naruszało § 20 ust. 2 pkt 4 i 5 rozporządzenia *KRI*.

Burmistrz wyjaśnił, że system SELWIN pracuje w odrębnej sieci Urzędu wydzielonej na potrzeby Systemu Rejestrów Państwowych. Do systemu SELWIN nie ma możliwości zalogowania się poza wydzieloną siecią, czyli dostęp jest możliwy tylko w trzech pomieszczeniach Urzędu. W związku z tym, że ASI nie ma bezpośredniego dostępu do panelu zarządzającego systemem SELWIN ze swojego stanowiska, uprawnienia zostały odebrane przy kolejnych pracach serwisowych w systemie SELWIN. Zwolniony pracownik nie może przebywać w pomieszczeniach, w których dochodzi do przetwarzania danych bez nadzoru. W związku z tym nie ma on fizycznej możliwości zalogowania do systemu.

(akta kontroli str. 246-247; 377-380)

8. Przechowywanie logów systemowych (usługa AD) tylko przez 15 dni uniemożliwiało sprawdzenie informacji o fakcie dostępu do danych po tym okresie. Tym samym okres przechowywania logów nie spełniał wymogów określonych w § 21 pkt 4 rozporządzenia *KRI*. Zgodnie z wskazanymi regulacjami, informacje w dziennikach systemów przechowywane są od dnia ich zapisu, przez okres

[49] „Technika informatyczna. Techniki bezpieczeństwa. Systemy zarządzania bezpieczeństwem informacji. Wymagania".

wskazany w przepisach odrębnych, a w przypadku braku przepisów odrębnych przez dwa lata.

Burmistrz wyjaśnił, że wynika to z faktu, że usługa AD generuje bardzo duże ilości logów (około 50 000 dziennie). Przechowywanie takiej ilości logów jest bardzo trudne. W najbliższej przyszłości zostanie to przeanalizowane i wdrożone rozwiązanie pozwalające przechowywać wymagane zdarzenia przez okres dwóch lat.

(akta kontroli str. 246-247; 377-380)

9. W Urzędzie nie przeprowadzono okresowego audytu wewnętrznego z zakresu bezpieczeństwa informacji w 2016 r., ani w 2017 r., tym samym nie wykonano obowiązku wynikającego z § 20 ust. 2 pkt 14 rozporządzenia *KRI*, tj. zapewnienia okresowego audytu wewnętrznego w zakresie bezpieczeństwa informacji, nie rzadziej niż raz na rok. Zakresem audytów przeprowadzonych w latach 2018-2019 nie objęto sprawdzenia wdrożonych zabezpieczeń oraz identyfikacji obszarów, które należy usprawnić.

Burmistrz wyjaśnił, że bardzo szczegółowy audyt teleinformatyczny i weryfikacji dokumentacji PBI był przeprowadzony w 2015 r. W kolejnych latach nie wprowadzano znaczących zmian w systemie teleinformatycznym, w związku z tym nie przeprowadzano audytów. W ocenie Burmistrza, audyty przeprowadzone w latach 2018-2019 w wystarczającym stopniu weryfikowały wdrożone zabezpieczenia oraz identyfikowały obszary, które należy usprawnić. Niemniej jednak, biorąc pod uwagę spostrzeżenia NIK, zaplanowano zlecenie przeprowadzenia audytu zewnętrznego przez firmę specjalizującą się ww. zakresie.

(akta kontroli str. 204-241; 256-262; 270-314; 377-380)

IV. Uwagi i wnioski

Uwagi

Najwyższa Izba Kontroli nie formułuje uwag.

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

Wnioski

1. Zapewnienie opracowania i wprowadzenia procedur elektronicznego obiegu dokumentów oraz załatwiania spraw w formie elektronicznej w Urzędzie.

2. Przeprowadzanie pełnych cyklicznych szkoleń z zakresu bezpieczeństwa informacji dla wszystkich pracowników biorących udział w procesie przetwarzania informacji, zgodnie z § 20 ust. 2 pkt 6 rozporządzenia *KRI.*

3. Zamieszczenie na stronie internetowej Urzędu informacji o których mowa w § 3 ust. 1 pkt 2, 4 i 5 rozporządzenia *w sprawie dokumentów elektronicznych* oraz o usługach świadczonych elektronicznych przez Urząd.

4. Opracowanie Polityki Bezpieczeństwa Informacji, zgodnej z Polską Normą PN-ISO/IEC 27001 oraz zapewnienie złożenia przez pracowników Urzędu oświadczeń o zapoznaniu się z ww. dokumentem, jak też zobowiązania się do przestrzegania jego zapisów, zgodnie z wymogami § 20 ust. 3 rozporządzenia *KRI*.

5. Zapewnianie aktualizacji regulacji wewnętrznych systemu bezpieczeństwa informacji w zakresie dotyczącym zmieniającego się otoczenia, zgodnie z § 20 ust. 2 pkt 1 rozporządzenia *KRI*.

6. Zapewnienie bezzwłocznego odbierania uprawnień do systemów informatycznych zwolnionym pracownikom, zgodnie z § 20 ust. 2 pkt 4 i 5 rozporządzenia *KRI*.

7. Przechowywania logów systemowych przez co najmniej 2 lata, zgodnie z § 21 ust. 4 rozporządzenia *KRI*.

8. Przeprowadzanie okresowych audytów wewnętrznych w zakresie bezpieczeństwa informacji, z wymaganą częstotliwością, tj. nie rzadziej niż raz w roku, zgodnie z § 20 ust. 2 pkt 14 rozporządzenia *KRI*.

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 we Wrocławiu. 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 dni od otrzymania wystąpienia pokontrolnego, o sposobie wykorzystania uwag i wykonania wniosków pokontrolnych oraz o podjętych działaniach lub przyczynach niepodjęcia tych działań.

W przypadku wniesienia zastrzeżeń do wystąpienia pokontrolnego, termin przedstawienia informacji liczy się od dnia otrzymania uchwały o oddaleniu zastrzeżeń w całości lub zmienionego wystąpienia pokontrolnego.

Wrocław, października 2020 r.

Kontroler
Renata Połatajko
Główny specjalista kontroli państwowej

.....
podpis

Najwyższa Izba Kontroli
Delegatura we Wrocławiu
p.o. Dyrektor
Marcin Kaliński

.....
podpis