



NAJWYŻSZA IZBA KONTROLI

Delegatura w Białymstoku

LBI.410.005.04.2020



Mirosław Korolczuk
Burmistrz Augustowa
ul. 3-go Maja 60, 16-300 Augustów

WYSTĄPIENIE POKONTROLNE

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

NAJWYŻSZA IZBA KONTROLI
Delegatura w Białymstoku
ul. Akademicka 4, 15-267 Białystok
T +48 85 874 81 00, F +48 85 874 81 33
lbi@nik.gov.pl

I. Dane identyfikacyjne

Jednostka kontrolowana	Urząd Miejski w Augustowie, ul. 3-go Maja 60, 16-300 Augustów ¹
Kierownik jednostki kontrolowanej	Mirosław Korolczuk, Burmistrz Augustowa od 5 listopada 2018 r. ²
Zakres przedmiotowy kontroli	Świadczenie przez Urząd 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 24 lipca 2019 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 w Białymstoku
Kontroler	Beata Palinowska, starszy inspektor kontroli państwowej, upoważnienie do kontroli nr LBI/80/2020 z 29 czerwca 2020 r. (akta kontroli str. 1-3)

¹ Dalej: *Urząd*.

² Dalej: *Burmistrz*.

³ Dz. U. z 2020 r. poz. 1200, ze zm. Ustawa zwana dalej: *ustawą o NIK*.

II. Ocena ogólna⁴ kontrolowanej działalności

OCENA OGÓLNA

Wdrożone w Urzędzie zasady świadczenia e-usług umożliwiły ich terminową i sprawną realizację. Zapewniały również bezpieczne gromadzenie i przetwarzanie baz danych wykorzystywanych w Urzędzie. Brak odpowiednich procedur wewnętrznych w zakresie bezpieczeństwa może mieć jednak negatywny wpływ na zachowanie bezpieczeństwa informacji.

Urząd udostępniał na portalu ePUAP 31 e-usług w siedmiu kategoriach oraz prowadził działania informacyjne dotyczące możliwości załatwienia spraw drogą elektroniczną. Udostępnione informacje nie były rzetelne. Na stronie internetowej Urzędu nie zamieszczono bowiem danych o wszystkich rodzajach oferowanych e-usług oraz linków przekierowujących do strony ePUAP. Brak takich informacji tworzył barierę w dostępie do usług elektronicznych i mógł być jedną z przyczyn niewielkiego zainteresowania tą formą załatwiania spraw (w I półroczu 2020 r. zgłoszono 363 sprawy, w ramach pięciu z siedmiu grup e-usług świadczonych w Urzędzie).

Sprawy napływające do Urzędu za pośrednictwem ePUAP były załatwiane bez zbędnej zwłoki, z wykorzystaniem posiadanych informacji i danych zgromadzonych w rejestrach publicznych. Wnioskodawcy nie byli również zobowiązani do dostarczania dodatkowych dokumentów, będących w posiadaniu innych jednostek administracji publicznej. Wprowadzony system elektronicznego zarządzania dokumentami⁵ stosowano równolegle do ewidencjonowania i rejestrowania przesyłek elektronicznych.

Urząd prawidłowo zabezpieczył sprzęt informatyczny przed nieuprawnionym dostępem i w 14 (z 15) przypadkach przed samodzielnym instalowaniem oprogramowania przez użytkowników. Jednak naruszono przepisy 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 teleinformatycznych⁶, które mogą mieć wpływ na zachowanie bezpieczeństwa informacji:

- nie opracowano systemu zarządzania bezpieczeństwem informacji, w tym polityki bezpieczeństwa informacji;
- w latach 2016–2017 i 2019–2020 (do 24 lipca) nie przeprowadzono corocznego audytu z zakresu bezpieczeństwa informacji.

III. Opis ustalonego stanu faktycznego

OBSZAR

Świadczenie przez Urząd e-usług.

Opis stanu faktycznego

1. Zagadnienia dotyczące elektronicznego świadczenia usług publicznych zostały ujęte w *Strategii Rozwoju Gminy Miasta Augustów na lata 2014–2020*⁷. W ramach celu szczegółowego *Nowoczesna administracja* wyznaczono kierunek działania *Zwiększenie dostępności i zapewnienie wysokiej jakości e-usług*. W opisie kierunku zaplanowano utworzenie nowej strony internetowej Miasta Augustów z treścią odpowiednio dostosowaną do potrzeb różnych grup odbiorców oraz zwiększenie katalogu e-usług świadczonych przez Urząd i podmioty gminne (nie wskazano terminu wdrożenia tych działań). Wskaźnikiem służącym do monitorowania realizacji działania była liczba wniosków składanych za pomocą strony internetowej i poczty elektronicznej. W latach 2016–2019 w Urzędzie nie monitorowano realizacji tego działania. Burmistrz wyjaśnił, że: *Tryb prac nad przygotowaniem Raportu z realizacji Strategii został wszczęty w 2017 roku, jednakże w związku z trudną sytuacją kadrową Referatu Funduszy Zewnętrznych oraz dużą liczbą realizowanych projektów prace nad Raportem zostały przesunięte na 2018 rok. W 2018 roku w wyniku analizy danych wynikała potrzeba zmiany wskaźników monitorowania celów operacyjnych.* (akta kontroli str. 4-19, 330-333)

⁴ Najwyższa Izba Kontroli formułuje ocenę ogólną jako ocenę pozytywną, ocenę negatywną albo ocenę w formie opisowej.

⁵ Dalej: EZD.

⁶ Dz. U. z 2017 r. poz. 2247. Rozporządzenie zwane dalej „rozporządzeniem KRP”.

⁷ Przyjęto ją uchwałą nr IX/70/15 Rady Miejskiej w Augustowie z 23 czerwca 2015 r. w sprawie przyjęcia Strategii Rozwoju Gminy Miasta Augustów na lata 2014–2020.

2. Urząd udostępniał za pośrednictwem platformy ePUAP 31 e-usług, w kategoriach:

- podatki i opłaty – siedem usług⁸,
- dowody osobiste, meldunki, wybory – szesnaście usług⁹,
- budownictwo, architektura, urbanistyka – jedna usługa¹⁰,
- pismo ogólne, skargi, wnioski, zapytania do urzędu – trzy usługi,
- urodzenia, małżeństwa, zgony – dwie usługi¹¹,
- geodezja, kartografia – jedna usługa¹²,
- ochrona środowiska – jedna usługa.

Wszystkie z tych usług były również dostępne na platformie Cyfrowy Urząd Wrót Podlasia, obejmującej swoim zasięgiem województwo podlaskie.

W Urzędzie nie udostępniano usług elektronicznych w dziewięciu dziedzinach: [1] bezpieczeństwo i zarządzanie kryzysowe (imprezy masowe, zgromadzenia publiczne, sprawy obronne), [2] komunikacja, drogownictwo i transport, [3] kultura, sport, turystyka, oświata, [4] nieruchomości, lokale mieszkalne i użytkowe, [5] ochrona praw konsumentów, [6] rolnictwo, leśnictwo, łowiectwo, rybołówstwo, [7] zdrowie i sprawy społeczne (pomoc społeczna, świadczenia rodzinne, zasiłki), [8] rozwój regionalny. (akta kontroli str. 325)

3. Od 1 stycznia do 30 czerwca 2020 r. mieszkańcy złożyli do Urzędu 363 wnioski, w tym:

- 17 od 1 stycznia do 29 lutego 2020 r.;
- 32 od 1 marca do 30 kwietnia 2020 r.;
- 314 od 1 maja do 30 czerwca 2020 r.

Znaczny wzrost zainteresowania mieszkańców e-usługami odnotowano w okresie epidemii COVID-19 (od 1 marca do 30 czerwca 2020 r.). W okresie tym płynęło 95% wszystkich spraw zarejestrowanych w Urzędzie w I półroczu 2020 r. Największy wzrost liczby e-usług odnotowano w zakresie dowodów osobistych (w okresie epidemii wpłynęło 45 wniosków o wydanie dowodu osobistego, tj. 87% wszystkich spraw tego rodzaju złożonych w I półroczu 2020 r.). Dotyczyło to również spraw z obszaru pisma ogólne, skargi wnioski i zapytania do urzędu oraz budownictwo, architektura i urbanistyka. W okresie epidemii wpłynęło odpowiednio dziewięć i cztery wnioski, przy braku takich spraw przed epidemią (od 1 stycznia do 29 lutego 2020 r.).

Znaczny wzrost liczby spraw od 1 maja do 30 czerwca 2020 r. wynikał z zaplanowanych na 28 czerwca 2020 r. wyborów Prezydenta RP. Wpłynęło wówczas 268 wniosków o dopisanie do Rejestru Wyborców (przy braku takich spraw we wcześniejszym okresie).

Poziom zainteresowania mieszkańców pozostałymi e-usługami był znikomy lub nie było nimi zainteresowania (kategorie: gospodarka komunalna, ochrona środowiska, podatki i opłaty, urodzenia, małżeństwa, zgony).

Burmistrz wyjaśnił, że: *Jedną z barier korzystania z e-usług w Urzędzie może być brak potrzeb i motywacji do korzystania z takich rozwiązań. Powodem mogą być też wieloletnie przyzwyczajenia klientów do „dokumentu papierowego”, a także chęć osobistego kontaktu z Urzędnikiem w celu wyjaśnienia wątpliwości. Istotną barierą stanowi również brak możliwości sprzętowych, dostęp do Internetu, a także brak podpisu kwalifikowanego lub*

⁸ W tym: [1] DL-1 Deklaracja na podatek leśny, [2] IL-1 Informacja o lasach; [3] DN-1 Deklaracja na podatek od nieruchomości, [4] DR-1 Deklaracja na podatek rolny, [5] DT-1 Deklaracja na podatek od środków transportowych, [6] IR-1 Informacja o gruntach, [7] IN-1 Informacja o nieruchomościach i obiektach budowlanych.

⁹ W tym: [1] wniosek o wydanie dowodu osobistego, [2] dopisanie się do spisu wyborców, [3] skreślenie z rejestru wyborców, [4] sporządzenie aktu pełnomocnictwa do głosowania w wyborach, [5] udostępnienie rejestru wyborców, [6] wpisanie się do rejestru wyborców, [7] zgłoszenie zamiaru głosowania korespondencyjnego dla osób głosujących w Polsce, [8] zgłoszenie wymeldowania z pobytu stałego, [9] zgłoszenie wymeldowania z pobytu czasowego, [10] zgłoszenie wyjazdu poza granice RP, [11] zgłoszenie powrotu z wyjazdu poza granice RP, sprawdzenie danych zawartych w rejestrze PESEL i rejestrze mieszkańców i usunięcie niezgodności w przypadku ich wystąpienia, [12] zameldowanie na pobyt stały lub czasowy, [13] wpisanie się do rejestru wyborców, [14] Zgłoszenie lub cofnięcie zawieszenia dowodu osobistego dziecka lub innej osoby, [15] Zgłoszenie utraty lub uszkodzenia dowodu osobistego – formularz do samodzielnego uzupełnienia, [16] Udostępnianie z Rejestru Dowodów Osobistych dokumentacji związanej z dowodami osobistymi.

¹⁰ Wydanie wypisu i wyrysu ze studium uwarunkowań i kierunków zagospodarowania przestrzennego.

¹¹ W tym: wydanie odpisu aktu stanu cywilnego, zgłoszenie urodzenia dziecka.

¹² Ustalenie nr porządkowego budynku.

profilu zaufanego. Brak umiejętności po stronie klientów w tym zakresie również może stanowić istotną przeszkodę. Urząd pozyskuje środki na organizację szkoleń, które obejmują szkolenia informatyczne dla mieszkańców. Obecnie Urząd realizuje bezpłatne szkolenia organizowane w ramach grantu „Akademia kompetencji cyfrowych dla mieszkańców Augustowa”. (akta kontroli str. 325-327, 313)

4. W Urzędzie w latach 2016–2019 nie gromadzono i nie analizowano w sposób usystematyzowany danych dotyczących korzystania przez obywateli i przedsiębiorców z e-usług, mimo że jednym ze wskaźników rezultatu określonym w Strategii była liczba wniosków składanych za pomocą strony internetowej i poczty elektronicznej (co opisano w punkcie 1). W 2020 roku dokonano analizy poziomu korzystania z e-usług w latach 2017–2019. Stwierdzono, że liczba wszystkich spraw zrealizowanych za pośrednictwem platform elektronicznych ePUAP i Cyfrowy Urząd Wrót Podlasia złożonych przez mieszkańców oraz przez inne urzędy systematycznie rosła – z 828 w 2017 r. poprzez 1.279 w 2018 r., do 2.173 w 2019 r. (akta kontroli str. 288-299)

5. W okresie objętym kontrolą (do 24 lipca 2020 r.) do Urzędu nie wpłynęły skargi w zakresie świadczenia usług publicznych w formie elektronicznej lub wnioski w sprawie usprawnienia tej formy komunikacji z Urzędem. (akta kontroli str. 300)

6. Obowiązującym w Urzędzie podstawowym sposobem dokumentowania przebiegu załatwiania i rozstrzygania spraw, wykonywania czynności kancelaryjnych oraz gromadzenia i tworzenia dokumentów był system tradycyjny (papierowy). Zarządzeniem Burmistrza, od 7 grudnia 2015 r. wprowadzono równolegle system EZD¹³, wykorzystując w tym celu system teleinformatyczny SmartDoc, wdrożony w związku z realizacją projektu pn. *Wdrożenie elektronicznych usług dla ludności województwa podlaskiego – część II administracja samorządowa*, zakładający wdrożenie do użytkowania programu do elektronicznego zarządzania dokumentacją.

Przyjęte uregulowania obejmowały dokumenty wpływające i wychodzące drogą elektroniczną oraz tradycyjną (z pewnymi wyjątkami). Ewidencji w EZD nie podlegały m.in. dokumenty znajdujące się w aktach osobowych pracowników Urzędu, wnioski o wpis do centralnej ewidencji działalności gospodarczej, rachunki, faktury i inne dokumenty księgowe, dokumentacja z zakresu rejestracji stanu cywilnego, deklaracje o wysokości opłaty za gospodarowanie odpadami komunalnymi, wnioski o udzielenie uczniom pomocy materialnej o charakterze socjalnym, wnioski pracodawców o dofinansowanie kosztów kształcenia młodocianych pracowników, dokumentacja podatkowa i wymiarowa, dokumentacja związana z opłatami, z egzekucją i windykacją oraz rozliczaniem wynagrodzeń.

Poszczególne etapy procesu obiegu pism w EZD obejmowały:

- wpływ dokumentu do Urzędu w formie papierowej lub elektronicznej;
- rejestrację sprawy w ewidencji, poprzez wprowadzenie przez pracownika do systemu EZD obrazu dokumentu złożonego w formie papierowej oraz przesłanie do EZD dokumentu otrzymanego drogą elektroniczną;
- dekretację otrzymanej korespondencji, elektronicznie i papierowo przez Burmistrza lub jego zastępcę oraz kierowników odpowiednich wydziałów, następnie przekazanie dokumentów do odpowiednich pracowników;
- rozpatrywanie sprawy;
- przygotowanie projektu rozstrzygnięcia;
- akceptację projektu przez przełożonego;
- podpisanie decyzji i wysyłkę dokumentu w sposób wskazany we wniosku.

W odniesieniu do przesyłek wpływających drogą elektroniczną określono również, że wnioski podlega weryfikacji w zakresie podpisania bezpiecznym podpisem elektronicznym lub profilem zaufanym. Pisma przeznaczone do wysyłki w postaci

¹³ Zarządzenie Burmistrza nr 227/15 z 7 grudnia 2015 r. w sprawie wprowadzenia Systemu do Elektronicznego Zarządzania Dokumentacją w Urzędzie Miejskim w Augustowie.

elektronicznej mogły być wysłane automatycznie, po ich podpisaniu podpisem elektronicznym, przez punkt kancelaryjny oraz przez pracowników upoważnionych do obsługi elektronicznych doręczeń. (akta kontroli str. 228-232)

Elektroniczna Skrzynka Podawcza na platformie ePUAP nie była zintegrowana z systemem EZD. Tym samym pisma wpływające do Urzędu i wychodzące z Urzędu drogą elektroniczną nie były automatycznie przesyłane pomiędzy tymi systemami. Pisma wpływające do Urzędu były drukowane, a następnie ich obraz był wprowadzany do EZD. Główny Specjalista w Wydziale Organizacyjno-Prawnym Urzędu Miejskiego w Augustowie wyjaśnił, że: *Przyczyną odłączenia ePUAP od systemu EZD były błędy podczas pobierania dużych plików. Błąd został zgłoszony do Centralnego Ośrodka Informatyki¹⁴. Po konsultacji z firmą MAXTO (producent aplikacji SmartDoc) ePUAP został odpięty od EZD. Do dnia dzisiejszego COI nie odniosło się czy błąd został naprawiony.* (akta kontroli str. 334-335)

Według stanu na 30 czerwca 2020 r. kwalifikowany podpis elektroniczny w Urzędzie posiadało 30 osób, w tym Burmistrz i jego zastępca, Skarbnik Miasta, Kierownik Urzędu Stanu Cywilnego i jego zastępca. Profil zaufany w Urzędzie posiadało natomiast dziesięciu pracowników. Od 1 stycznia do 30 czerwca 2020 r. podpisem elektronicznym opatrzone 499 pism¹⁵, z których 213 podpisał Burmistrz, a 42 jego zastępca. (akta kontroli str. 300-302)

7. W toku kontroli analizą objęto 20 spraw, które od 1 stycznia do 30 czerwca 2020 r. wpłynęły do Urzędu w formie elektronicznej poprzez ePUAP, w tym:

- pięć z kategorii pismo ogólne, skargi, wnioski, zapytania do urzędu – trzy pisma ogólne oraz dwa wnioski o udostępnienie informacji publicznej;
- 14 z kategorii sprawy osobowe – po pięć wniosków o wydanie dowodu osobistego i dopisanie do rejestru wyborców oraz cztery wnioski dotyczące zgłoszenia pobytu stałego i jeden dotyczący wymeldowania;
- jedną z kategorii ochrona środowiska – wniosek o dofinansowanie do usunięcia azbestu.

Analiza wykazała, że: [1] wszystkie wnioski podpisano elektronicznie, a ich podpis został pozytywnie zweryfikowany przez pracownika Urzędu; [2] pisma wydrukowano z systemu, a następnie procedowano w formie papierowej i elektronicznej; [3] wszystkie wnioski niezwłocznie zadekretowano na pracownika prowadzącego sprawę; [4] żaden nie wymagał korekty bądź uzupełnienia. System do EZD nie komunikował się automatycznie z innymi systemami informatycznymi Urzędu, a przy załatwianiu spraw nie zaszła potrzeba zasięgnięcia informacji w innym organie administracji publicznej.

Podczas załatwiania pięciu spraw Urząd, korzystając z oprogramowania *Źródło*, pozyskiwał dane gromadzone w zewnętrznych systemach/rejestrach państwowych, tj. Rejestrze Dowodów Osobistych (pięć wniosków o wydanie dowodu osobistego z warstwą elektroniczną) oraz z systemu Selwin (cztery wnioski dotyczące zameldowania). Wszystkie sprawy zostały załatwione bez zbędnej zwłoki, tj. w terminie od jednego do 24 dni od wpływu sprawy do Urzędu.

Wnioskodawcom umożliwiono uzyskanie informacji na temat aktualnego stanu sprawy drogą telefoniczną, e-mailową, a także za pośrednictwem platformy ePUAP. Wydane rozstrzygnięcia były przekazywane zgodnie ze wskazaniem zawartym we wniosku, w formie elektronicznej za pośrednictwem platformy ePUAP. (akta kontroli str. 342-345)

8. W Urzędzie nie prowadzono rejestru awarii występujących na platformie ePUAP. Główny specjalista w Wydziale Organizacyjno-Prawnym wyjaśnił, że: *W okresie od 1 stycznia do 30 czerwca 2020 r. nie występowały problemy techniczne w funkcjonowaniu platformy ePUAP. W razie problemów z funkcjonowaniem ePUAP następuje kontakt z centrum pomocy użytkowników ePUAP w COI poprzez wybranie jednej formy do kontaktu z Service Desk: formularz kontaktowy, telefon, adres e-mail.* (akta kontroli str. 328-329)

9. Obsługa serwisowa systemu EZD, dostarczonego w ramach projektu pn. *Wdrożenie elektronicznych usług dla ludności województwa podlaskiego – część II administracja*

¹⁴ Dalej: COI.

¹⁵ Kwalifikowanym podpisem elektronicznym podpisano również 52 dokumentów do Zakładu Ubezpieczeń Społecznych (w programie Płatnik) oraz 891 deklaracji podatkowych za 2019 r.

samorządowa (szerzej opisano w pkt 6 wystąpienia), była realizowana na podstawie umowy zawartej przez Urząd Marszałkowski Województwa Podlaskiego z firmą zewnętrzną na świadczenie usług gwarancji, wsparcia i asysty technicznej. W okresie trwania umowy Urzędowi umożliwiono zgłaszanie awarii i problemów związanych z EZD poprzez dedykowaną platformę serwisową (<http://sos.wrotapodlasia.pl>). (akta kontroli str. 233-249)

Umowa z firmą zewnętrzną wygasła 21 maja 2020 r.¹⁶ Urząd Marszałkowski poinformował, że obowiązek zabezpieczenia posiadanego systemu EZD od 22 maja 2020 r. do 19 maja 2021 r. (koniec okresu trwałości projektu) ciąży na Urzędzie. Od 22 maja 2020 r. wsparcie i asysta techniczna była realizowana na podstawie umowy zawartej przez Urząd z firmą zewnętrzną. Zgłaszanie awarii i problemów technicznych umożliwiono poprzez System Obsługi Zgłoszeń Wykonawcy, telefonicznie oraz drogą e-mail. W umowie zagwarantowano czas reakcji na problemy w działaniu systemu: cztery godziny dla błędów krytycznych¹⁷, osiem godzin dla błędów poważnych¹⁸ i 48 godzin dla błędów pozostałych¹⁹.

Od 1 stycznia do 30 czerwca 2020 r. wystąpiły dwa problemy w funkcjonowaniu systemu EZD. Zostały one niezwłocznie usunięte i nie wpłynęły znacząco na pracę Urzędu, w tym na terminowość realizowanych spraw. (akta kontroli str. 250-275)

10. Urząd upubliczniał informacje o możliwości załatwiania spraw drogą elektroniczną poprzez stronę internetową²⁰ oraz Biuletyn Informacji Publicznej²¹. Na stronie internetowej zamieszczono informacje o trzech (z siedmiu) kategoriach spraw realizowanych w formie e-usług (podatki i opłaty, dowody osobiste, meldunki, wybory, pismo ogólne, skargi, wnioski, zapytania do urzędu), konieczności posiadania profilu zaufanego oraz odnośniki do portalu Cyfrowy Urząd Wrót Podlasia i na stronę www.obywatel.gov.pl. W BIP zamieszczono link przekierowujący bezpośrednio do platformy Cyfrowy Urząd Wrót Podlasia oraz ePUAP. Na stronie internetowej Urzędu brak było wykazu spraw możliwych do załatwienia w formie e-usług oraz sposobów uzyskania profilu zaufanego lub nowego dowodu osobistego z warstwą elektroniczną.

Burmistrz wyjaśnił, że: *Pracownicy Wydziału Spraw Społecznych i Administracyjnych Urzędu w trakcie realizacji procedury wydawania dowodu osobistego z warstwą elektroniczną informowali ustnie petentów o możliwościach związanych z e-dowodem. Ponadto petenci otrzymywali ulotki informacyjne oraz mogli zapoznać się z informacjami wywieszonymi w budynku, w którym mieści się Wydział Spraw Społecznych i Administracyjnych.*

(akta kontroli str. 319-324)

11. Pracownicy Urzędu uczestniczyli w 20 szkoleniach z zakresu obsługi systemów informatycznych, ochrony danych osobowych (m.in. w związku z wejściem w życie przepisów RODO) oraz elektronizacji procesu zamówień publicznych i cyberbezpieczeństwa.

Od 1 lipca 2018 r. do 30 czerwca 2020 r. jeden pracownik Urzędu (Administrator Systemów Informatycznych²²) uczestniczył w dwóch szkoleniach z zakresu bezpieczeństwa informacji, wymaganych § 20 ust. 2 pkt 6 *rozporządzenia KRI*. Szkolenia obejmowały m.in. zagadnienia dotyczące zagrożeń bezpieczeństwa informacji, skutki naruszenia bezpieczeństwa informacji, stosowanie środków zapewniających bezpieczeństwo informacji. Pozostali pracownicy nie uczestniczyli w odrębnych szkoleniach z tego zakresu. Natomiast 47 pracowników zaangażowanych w proces przetwarzania informacji 22 stycznia 2019 r. uczestniczyło w szkoleniu z zakresu ochrony danych osobowych, które obejmowało zagadnienia związane z bezpieczeństwem informacji (występujące zagrożenia bezpieczeństwa informacji, organizacyjne i techniczne środki zapobiegania naruszeniom

¹⁶ Urząd Marszałkowski Województwa Podlaskiego poinformował wszystkich swoich partnerów, w tym Urząd o wygaśnięciu 21 maja 2020 r. umowy z firmą zewnętrzną.

¹⁷ Błędy, w wyniku których co najmniej jedna komórka organizacyjna nie może realizować swojej funkcji statutowej przy pomocy systemu lub żadna z funkcji statutowych Urzędu nie może być w pełni zrealizowana przy pomocy systemu na skutek ujawnienia się jego wady.

¹⁸ Błędy, w wyniku których co najmniej jedna komórka organizacyjna Urzędu napotyka w systemie na ograniczenia ilościowe lub funkcjonalne uniemożliwiające realizację pełnego zakresu jej funkcji statutowej przewidzianego do realizacji przy pomocy systemu na skutek ujawnienia się wady tego systemu.

¹⁹ Błędy, w wyniku których przeprowadzenie określonych operacji w systemie jest niemożliwe lub daje niepoprawny rezultat na skutek ujawnienia się wady tego systemu.

²⁰ <https://urzad.augustow.pl/>.

²¹ Dalej: BIP.

²² Dalej: ASI.

bezpieczeństwa informacji, sposoby postępowania pracowników zapobiegające naruszeniom oraz skutki naruszenia bezpieczeństwa informacji łącznie z zagadnieniami odpowiedzialności prawnej). (akta kontroli str. 303-310)

12. W Urzędzie w okresie objętym kontrolą obowiązywała polityki bezpieczeństwa, odnosząca się do bezpieczeństwa danych osobowych, wprowadzona zarządzeniami Burmistrza: *Polityka bezpieczeństwa Urzędu Miejskiego w Augustowie* z 20 stycznia 2014 r. (obowiązująca do 31 marca 2016 r.), następnie *Polityka bezpieczeństwa przetwarzania danych osobowych oraz Instrukcja zarządzania systemami informatycznymi służącymi do przetwarzania danych osobowych*²³, zaktualizowana 30 maja 2019 r.²⁴ Natomiast nie opracowano i nie wdrożono systemu zarządzania bezpieczeństwem informacji (w tym polityki bezpieczeństwa informacji), o którym mowa w § 20 ust. 1 i w § 2 pkt 15 *rozporządzenia KRI* (szerzej kwestię tą opisano w sekcji *Stwierdzone nieprawidłowości*).

Opracowanie, wdrożenie, monitorowanie, przeglądanie, utrzymywanie i doskonalenie tych dokumentów Burmistrz powierzył Inspektorowi Ochrony Danych (dalej *IOD*). Treść dokumentów została przekazana pracownikom Urzędu, których zobligowano jednocześnie do ich przestrzegania i stosowania. Problematykę zawartą w tych dokumentach omówiono na szkoleniach z zakresu RODO, przeprowadzonych m.in. 22 stycznia, 20 sierpnia i 20 grudnia 2019 r. oraz 13 stycznia 2020 r. Przeszkolono wówczas odpowiednio 47, 54, 3 i 13 pracowników Urzędu. (akta kontroli str. 276-287)

13. Urząd nie dysponował formalną dokumentacją potwierdzającą poddawanie cyklicznym przeglądom *Polityki bezpieczeństwa danych osobowych*. W okresie objętym kontrolą *Polityka* była dwukrotnie aktualizowana – 31 marca 2016 r. i 30 maja 2019 r. Zmiany wynikały ze zmian organizacyjnych w Urzędzie oraz zmian prawnych, wynikających z wejścia w życie przepisów RODO. Nie przyjęto i nie wdrożono natomiast innych dokumentów dotyczących bezpieczeństwa informacji (co opisano w pkt 12 wystąpienia pokontrolnego). (akta kontroli str. 20-170)

14. Politykę ochrony danych osobowych przyjęto i wdrożono łącznie z dokumentami wykonawczymi. Na dokumentację dotyczącą ochrony danych osobowych składały się m.in.: [1] rejestr czynności przetwarzania danych osobowych, [2] procedury bezpieczeństwa fizycznego i bezpieczeństwa informacji, [3] ewidencja osób upoważnionych do przetwarzania danych osobowych, [4] metodyka szacowania ryzykiem, [5] analiza ryzyka, [6] instrukcja postępowania przy naruszeniu danych. (akta kontroli str. 20-92)

15. W Urzędzie prowadzony był elektroniczny rejestr zasobów informatycznych. Służyło do tego dedykowane oprogramowanie do zarządzania systemami i procesami, wykorzystywane do gromadzenia bieżących danych oraz prowadzenia inwentaryzacji posiadanego sprzętu i oprogramowania, wymaganych postanowieniami § 20 ust. 2 pkt 2 *rozporządzenia KRI*. Gromadzone informacje umożliwiały identyfikację poszczególnych jednostek wchodzących w skład systemu komputerowego Urzędu (m.in. komputerów, drukarek i skanerów) oraz przypisania tym jednostkom odpowiedniego oprogramowania i konfiguracji. Przeprowadzone w trakcie kontroli oględziny obejmujące porównanie stanu faktycznego²⁵ z zapisami w elektronicznym rejestrze potwierdziły, że Urząd posiada aktualne dane o posiadanym sprzęcie i oprogramowaniu oraz jego konfiguracji. Posiadane zasoby informatyczne przypisano do osób, które opowiadały za dany sprzęt.

(akta kontroli str. 346-348)

16. W Urzędzie podjęto działania w celu uniemożliwienia użytkownikom systemów informatycznych niebędących pracownikami służb informatycznych samodzielnej instalacji oprogramowania na komputerach służbowych. Oględziny dziesięciu komputerów (w tym dziewięciu stacjonarnych i jednego przenośnego) wykazały, że na dziewięciu pracownicy nie posiadali uprawnień administracyjnych (nie było możliwości zainstalowania oprogramowania

²³ Zarządzenie nr 315/16 Burmistrza Miasta Augustowa z dnia 31 marca 2016 r. w sprawie ustalenia *Polityki bezpieczeństwa przetwarzania danych osobowych w Urzędzie Miejskim w Augustowie* i wprowadzenia do użytku służbowego *Instrukcji zarządzania systemem informatycznym służącym do przetwarzania danych osobowych w Urzędzie Miejskim w Augustowie*.

²⁴ Zaktualizowano zarządzeniem nr 175/2019 Burmistrza Miasta Augustowa z 30 maja 2019 r. w sprawie aktualizacji *Polityki ochrony danych osobowych w Urzędzie Miejskim w Augustowie*.

²⁵ Do próby wytypowano 10 komputerów, jeden serwer, jeden laptop i jedną drukarkę.

na komputerze). W jednym przypadku użytkownik komputera posiadał takie uprawnienia, co opisano w sekcji *Stwierdzone nieprawidłowości*. (akta kontroli str. 315-316)

17. W okresie objętym kontrolą zatrudnienie w Urzędzie zakończyło 55 pracowników. Oględziny kont w systemie informatycznym 15 pracowników wykazały, że osobom tym zablokowano dostęp do systemów informatycznych. Zasady cofania uprawnień w systemie informatycznym pracownikom określono w załączniku nr 8 do Polityki ochrony danych osobowych pn. *Procedura bezpieczeństwa fizycznego i bezpieczeństwa informacji*. Zgodnie z przyjętymi zasadami cofnięcie uprawnień następowało na wniosek przełożonego skierowany do Burmistrza. Nie określono terminu składania wniosków o cofnięcie/zmianę uprawnień. W dwóch (z 15) przypadkach niezwłocznie sporządzono formalne wnioski o zamknięcie kont przez przełożonego. W pozostałych 13 przypadkach takie wnioski nie były złożone (szerzej tą kwestię opisano w sekcji *Stwierdzone nieprawidłowości*).

(akta kontroli str. 305-307, 317-318)

18. W Urzędzie od 12 lipca do 6 września 2018 r.²⁶ przeprowadzono audyt wewnętrzny, którego zakres obejmował bezpieczeństwo informacji (zgodnie z § 20 ust. 2 pkt 14 rozporządzenia KRI). Dotyczył on obszaru LAN oraz na styku z siecią Internet, w szczególności: oceny aktualnej infrastruktury wraz z koncepcją jej rozbudowy, łącza fizyczne (w tym sposób połączenia elementów infrastruktury teleinformatycznej, okablowanie strukturalne), komunikację sieciową, urządzenia (przełączniki sieciowe), routing, wykorzystywanie adresów zewnętrznych/publicznych i dostęp do usług z wewnątrz Urzędu. W wyniku audytu sformułowano rekomendacje dotyczące uporządkowania pomieszczeń serwerowni, odpowiednie rozmieszczenie serwerów, skonfigurowanie urządzeń sieciowych. Zalecenia zostały zrealizowane.

Od 1 stycznia 2016 r. do 11 lipca 2018 r. i od 5 września 2019 r. do 24 lipca 2020 r. nie przeprowadzono audytu wewnętrznego z zakresu bezpieczeństwa informacji, co szerzej opisano w dalszej części wystąpienia pokontrolnego w sekcji *Stwierdzone nieprawidłowości*.

(akta kontroli str. 171-227)

Stwierdzone
nieprawidłowości

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

1. Urząd nierzetelnie informował na swojej stronie internetowej o sposobach załatwienia spraw drogą elektroniczną, ponieważ nie zamieścił na niej:
 - informacji o usługach świadczonych w formie elektronicznej poprzez ePUAP w czterech (z siedmiu) obszarach: urodzenia, małżeństwa, zgony; budownictwo, architektura, urbanistyka; geodezja i kartografia),
 - odnośników kierujących osoby zainteresowane bezpośrednio na platformę ePUAP, na której przygotowano dla nich 31 e-usług;
 - informacji o sposobach uzyskania profilu zaufanego.

Burmistrz wyjaśnił, że: *Informacja dotycząca możliwości złożenia wniosku drogą elektroniczną w zakresie uzyskania odpisu aktu stanu cywilnego znajduje się w wykazie spraw, gdzie klient zostaje przekierowany na Cyfrowy Urząd Wrót Podlasia. W Biuletynie Informacji Publicznej został umieszczony wykaz spraw możliwych do załatwienia drogą elektroniczną poprzez Cyfrowy Urząd Wrót Podlasia. Klient składając wniosek, po jego wypełnieniu jest przekierowany do platformy ePUAP, loguje się profilem zaufanym, za pośrednictwem banku lub e-dowodu. Sporządzenie dodatkowego wykazu spraw załatwianych poprzez ePUAP byłoby dublowaniem usługi i mając na uwadze klientów, Urząd maksymalizuje ułatwienia przy załatwianiu spraw drogą elektroniczną. Zarówno na stronie, jaki i w BiP znajduje się link do strony ePUAP. Klient po zalogowaniu zostaje automatycznie przekierowany na tę stronę, gdzie w strefie Klienta ma możliwość wyboru Katalogu usług a następnie Urzędu i złożenia wniosku w danej dziedzinie, którą Urząd udostępnia.*

Zdaniem NIK niezamieszczenie takich informacji bezpośrednio na stronie internetowej Urzędu stanowi barierę w dostępie do usług elektronicznych udostępnionych przez

²⁶ Wówczas nastąpił odbiór dokumentacji.

ePUAP i mogło być jedną z przyczyn niewielkiego zainteresowania tą formą załatwiania spraw (w I półroczu 2020 r. zgłoszono 363 sprawy, w ramach pięciu z siedmiu grup e-usług świadczonych w Urzędzie). (akta kontroli str. 319-324, 337-341)

2. W Urzędzie nie opracowano systemu zarządzania bezpieczeństwem Informacji, w szczególności polityki bezpieczeństwa informacji w rozumieniu § 2 pkt 15 rozporządzenia KRI, co było niezgodne z § 20 ust. 1 powołanego rozporządzenia. Przepis ten stanowi, 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. Ponadto § 20 ust. 3 rozporządzenia KRI wskazuje, że wymagania powyższe uznaje się za spełnione, jeżeli system zarządzania bezpieczeństwem informacji 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 Urzędzie brakowało między innymi: procedur i regulacji wewnętrznych dotyczących zarządzania ryzykiem.

Burmistrz wyjaśnił, że: *Działania zmierzające do ustanowienia Polityki bezpieczeństwa informacji zostały rozpoczęte w 2019 r. Podjęto szereg czynności zmierzających do aktualizacji dokumentacji w zakresie ochrony danych osobowych, zapewnienie kompetentnej kadry oraz infrastruktury informatycznej. Pracownicy Urzędu zostali przeszkoleni w zakresie bezpieczeństwa informacji. W związku z art. 21 i art. 22 ustawy z dnia 5 lipca 2018 r. o krajowym systemie cyberbezpieczeństwa powołano w Urzędzie Koordynatora ds. cyberbezpieczeństwa. Dane koordynatora zostały przekazane do NASK / CERT Polska. Koordynator jest odpowiedzialny za utrzymywanie kontaktów z podmiotami krajowego systemu cyberbezpieczeństwa. W 2020 r. w Planie szkoleń pracowników zostały ujęte szkolenia wewnętrzne pracowników w tym zakresie. Planowany audyt KRI miał wskazać niezgodności i zalecenia względem stosowanych rozwiązań w zakresie bezpieczeństwa informacji. Na ich podstawie planowano wdrożyć odpowiednie regulacje i procedury w nowej lokalizacji. Okres pandemii przesunął w czasie wykonanie audytu i wdrożenie powyższych. Należy wskazać, że pomimo braku formalnych procedur stanowiących politykę bezpieczeństwa informacji, w urzędzie nie doszło do wystąpienia incydentów lub naruszeń w tym zakresie. System ochrony danych osobowych związany jest pośrednio, a niekiedy bezpośrednio z zagadnieniami bezpieczeństwa informacji i w ramach wdrożonych polityk wyczerpuje część wymagań określonych przez rozporządzenie KRI, w tym dla zapewnienia poufności, dostępności i integralności informacji przetwarzanych w systemie teleinformatycznym z uwzględnieniem takich atrybutów, jak autentyczność, rozliczalność, niezaprzeczalność i niezawodność, m.in. wdrożono regulacje związane z nadawaniem i kontrolą uprawnień w systemach informatycznych, wykonuje się cykliczne szkolenia dla pracowników w zakresie przetwarzania danych, zagrożeń i pracy przy użyciu systemu informatycznego, wdrożono regulacje związane z pracą zdalną z wykorzystaniem systemu informatycznych, wdrożono zabezpieczenia techniczno-organizacyjne w celu zapewnienia bezpieczeństwa danych i informacji oraz zachowania poufności, integralności i dostępności i informacji.* (akta kontroli str. 337-341)

3. Użytkownik jednego komputera (z 10 poddanych oględzinom) do 21 lipca 2020 r. posiadał uprawnienia administratora, tj. możliwość zainstalowania nieautoryzowanego oprogramowania, wbrew wymogom określonym w § 20 ust. 2 pkt 4 rozporządzenia KRI. Zgodnie z tym przepisem zarządzanie bezpieczeństwem informacji realizowane jest m.in. przez podejmowanie działań zapewniających, że osoby zaangażowane w proces przetwarzania informacji posiadają stosowne uprawnienia i uczestniczą w tym procesie w stopniu adekwatnym do realizowanych przez nie zadań oraz obowiązków.

Główny specjalista w Wydziale Organizacyjno-Prawnym wyjaśnił, że: *W wyniku błędu systemu komputer nie pobrał bieżących aktualizacji. Spowodowało to, że użytkownik uzyskał możliwość instalacji programów. Po aktualizacji użytkownik utracił uprawnienia administratora do systemu informatycznego.*

Nieprawidłowość została usunięta w trakcie kontroli (21 lipca 2020 r.).

(akta kontroli str. 315-316, 334-335, 346)

4. W 13 (z 15) przypadkach przełożeni pracowników, którzy zakończyli zatrudnienie w Urzędzie nie złożyli formalnych wniosków do ASI o cofnięcie uprawnień w systemie informatycznym, wbrew wymogom określonym w załączniku nr 8 do Polityki ochrony danych osobowych pn. *Procedury bezpieczeństwa fizycznego i bezpieczeństwa informacji*.

Burmistrz wyjaśnił, że: *W celu zminimalizowania ryzyka niedopatrzenia złożenia wniosku o cofnięcie uprawnień i zwiększenia kontroli nad tym obowiązkiem, w dniu 9 kwietnia 2020 r. zarządzeniem Nr 113/2020 Burmistrza Miasta została wprowadzona karta obiegowa dla pracowników w sytuacji rozwiązania stosunku pracy, w której jednym z elementów jest informacja o posiadanych uprawnieniach do systemu elektronicznego. Jako weryfikator spełnienia obowiązku wskazany został Wydział Organizacyjno-Prawny (informatycy).*

(akta kontroli str. 315-316, 337-341)

5. Od 1 stycznia 2016 r. do 11 lipca 2018 r. i od 5 września 2019 r. do 24 lipca 2020 r. w Urzędzie nie przeprowadzano corocznego audytu wewnętrznego z zakresu bezpieczeństwa informacji, o którym mowa w § 20 ust. 2 pkt 14 rozporządzenia KRI (audyt był przeprowadzony od 12 lipca do 6 września 2018 r.²⁷ przez podmiot zewnętrzny).

Burmistrz wyjaśnił, że: *Audyt był prowadzony w ramach bieżącego nadzoru a uformalnienie prowadzonych działań kontrolnych miało nastąpić w 2020 r. Dodatkową kwestią była perspektywa planowanej zmiany lokalizacji Urzędu i zmiany infrastruktury informatycznej. Dnia 6.02.2020 r. podjęto działania zmierzające do realizacji wymogu określonego w § 20 ust. 2 pkt. 14 rozporządzenia KRI. Inspektor Ochrony Danych²⁸ posiada uprawnienia audytora wewnętrznego, w tym audytora zarządzania bezpieczeństwem informacji zgodnie z ISO 27001.*

NIK zwraca uwagę, że bieżący nadzór stanowi jeden z elementów kontroli zarządczej, o której mowa w art. 68 i 69 ustawy z dnia 27 sierpnia 2009 r. o finansach publicznych²⁹, natomiast audyt wewnętrzny jest odrębną od kontroli zarządczej instytucją, unormowaną w art. 272–296 powołanej ustawy.

(akta kontroli str. 337-341)

IV. Wnioski

Wnioski

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

1. Umieszczenie rzetelnej i pełnej informacji o realizowanych e-usługach na stronie internetowej Urzędu.
2. Opracowanie i wdrożenie systemu zarządzania bezpieczeństwem informacji, w tym polityki bezpieczeństwa informacji wymaganych § 2 pkt 15 i § 20 ust. 1 rozporządzenia KRI.
3. Niezwłoczne odbieranie pracownikom uprawnień do systemów informatycznych wraz z ustaniem zatrudnienia.
4. Zapewnienie okresowego audytu wewnętrznego z zakresu bezpieczeństwa informacji, o którym mowa w § 20 ust. 2 pkt 14 rozporządzenia KRI.

²⁷ Wówczas nastąpił odbiór dokumentacji poaudytowej.

²⁸ Zatrudniony na podstawie umowy z 1 lipca 2019 r.

²⁹ Dz. U. z 2019 r. poz. 869, ze zm.

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 Białymstoku. 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
wykonania wniosków

Zgodnie z art. 62 ustawy o NIK, należy poinformować Najwyższą Izbę Kontroli, w terminie 21 dni 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.

Białystok, 31 lipca 2020 r.

Kontroler:

Beata Palinowska
starszy inspektor kontroli państwowej

Palinowska Beata

podpis

p.o. DYREKTORA DELEGATURY
Najwyższej Izby Kontroli w Białymstoku
z up. p.o. WICEDYREKTORA
Robert Skwarko

[Signature]

podpis