



NAJWYŻSZA IZBA KONTROLI

Delegatura w Łodzi

LLO.410.009.01.2020

Pan
Dariusz Wojciech Kosno
Burmistrz
Urząd Miejski w Opocznie
ul. Staromiejska 6
26-300 Opoczno

WYSTĄPIENIE POKONTROLNE

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

I. Dane identyfikacyjne

Jednostka kontrolowana	Urząd Miejski w Opocznie, ul. Staromiejska 6, 26-300 Opoczno
Kierownik jednostki kontrolowanej	Dariusz Wojciech Kosno, Burmistrz Opoczna od 5 listopada 2018 r. W okresie objętym kontrolą funkcję kierownika jednostki poprzednio pełnił: Rafał Janusz Kądziera, Burmistrz Opoczna w okresie od 3 grudnia 2014 r. do 4 listopada 2018 r.
Zakres przedmiotowy kontroli	Świadczenie przez urzędy jednostek samorządu terytorialnego e-usług. Rozwiązania organizacyjne i techniczne w zakresie zapewnienia bezpieczeństwa przetwarzania informacji w urzędzie i ich stosowanie.
Okres objęty kontrolą	Od 1 stycznia 2016 r. do 14 września 2020 r.
Podstawa prawna podjęcia kontroli	Art. 2 ust. 2 ustawy z dnia 23 grudnia 1994 r. o Najwyższej Izbie Kontroli ¹
Jednostka przeprowadzająca kontrolę	Najwyższa Izba Kontroli Delegatura w Łodzi
Kontroler	Adam Markiewicz, specjalista kontroli państwowej, upoważnienie do kontroli nr LLO/105/2020 z dnia 10 lipca 2020 r. oraz nr LLO/142/2020 z dnia 2 września 2020 r.

(akta kontroli str. 1-4)

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

II. Ocena ogólna² kontrolowanej działalności

OCENA OGÓLNA

Najwyższa Izba Kontroli ocenia, że w latach 2016-2020 (I połowa) Urząd Miejski w Opocznie (dalej: Urząd) sprawnie realizował usługi, w sprawie których obywatele składali wnioski za pośrednictwem platformy ePUAP³ oraz przyjął rozwiązania organizacyjno-techniczne, dzięki którym zapewnił w wymaganym stopniu bezpieczeństwo przetwarzania informacji.

W Urzędzie spełniono wymagania wynikające z rozporządzenia Rady Ministrów z dnia 12 kwietnia 2012 r. *w sprawie Krajowych Ram Interoperacyjności, minimalnych wymagań dla rejestrów publicznych i wymiany informacji w postaci elektronicznej oraz minimalnych wymagań dla systemów teleinformatycznych*⁴ (dalej: Rozporządzenie KRI), w tym m.in.:

- ustanowiono i wdrożono kompleksowy System Zarządzania Bezpieczeństwem Informacji (dalej: SZBI), wynikający z § 20 ust. 1, w związku z § 20 ust. 3 rozporządzenia KRI;
- zgodnie z § 20 ust. 2 pkt 5 Rozporządzenia KRI niezwłocznie realizowano zmiany uprawnień dostępu do zasobów komputera;
- zapewniono szkolenia, wymagane § 20 ust. 2 pkt. 6 Rozporządzenia KRI;
- ustanowiono zgodnie z treścią § 20 ust. 2 pkt 4 Rozporządzenia KRI zabezpieczenia systemów informatycznych, gwarantujące adekwatne uprawnienia użytkowników, względem realizowanych przez nich zadań;
- przeprowadzano corocznie audyt bezpieczeństwa informacji, o którym mowa w § 20 ust. 2 pkt 14 Rozporządzenia KRI.
- ewidencjonowano sprzęt i oprogramowanie komputerowe zgodnie z § 20 ust. 2 pkt 2 Rozporządzenia KRI, tj. Urząd posiadał bieżącą informację o zasobach informatycznych.

Ponadto widniejące na stronie internetowej Urzędu informacje o rodzaju spraw możliwych do załatwienia drogą elektroniczną, a także wymogach z tym związanych, były aktualne i kompletne.

III. Opis ustalonego stanu faktycznego

Opis stanu faktycznego

1. W przyjętym na lata 2014-2020 dokumencie o charakterze strategicznym pn. Strategia Rozwoju Gminy Opoczno na lata 2016-2020⁵, wskazującym kierunki rozwoju Gminy Opoczno, nie zawarto celów związanych z dostosowaniem Urzędu do elektronicznego świadczenia usług publicznych, bądź podniesieniem jakości takich usług. Powyższy dokument w ramach celu strategicznego nr IV⁶ odnosił się jedynie do zwiększenia szeroko rozumianej dostępności usług publicznych.

Jednakże Urząd, w ramach systemu monitorowania ww. Strategii sporządzał coroczne Raporty o Stanie Gminy Opoczno⁷. Raporty za 2018 i 2019 rok zawierały obszerną informację dot. infrastruktury teleinformatycznej w gminie, w tym zwiększenia dostępności do elektronicznego świadczenia usług publicznych.

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

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

⁴ Dz. U. z 2017 r. poz. 2247.

⁵ Przyjęła Uchwałą Nr XXII/226/2016 Rady Miejskiej w Opocznie z dnia 30 czerwca 2016 r.

⁶ Opoczno subregionalnym ośrodkiem rozwoju społeczno-gospodarczego o funkcjach egzogenicznych.

⁷ Podstawę prawną tworzenia raportu o stanie gminy stanowił art. 28aa ust. 1 i 2 ustawy z dnia 8 marca 1990 r. o samorządzie gminnym (Dz. U. z 2020 r. poz. 713).

2. Według stanu na dzień 31 maja 2020 r. Urząd udostępniał obywatelom za pośrednictwem platformy ePUAP łącznie 32 usługi, w następujących kategoriach:

- sprawy obywatelskie oraz wybory – łącznie 13 usług⁸;
- gospodarka komunalna – trzy usługi;
- budownictwo, architektura, urbanistyka – dwie usługi;
- rolnictwo, leśnictwo, łowiectwo, rybołówstwo – dwie usługi;
- rozwój regionalny – dwie usługi;
- podatki i opłaty – jedna usługa;
- bezpieczeństwo i zarządzanie kryzysowe – jedna usługa;
- geodezja i kartografia – jedna usługa;
- komunikacja i transport – jedna usługa;
- kultura, sport, turystyka, oświata – jedna usługa;
- nieruchomości i lokale mieszkalne – jedna usługa;
- ochrona praw konsumentów – jedna usługa;
- ochrona środowiska – jedna usługa;
- zdrowie i sprawy społeczne – jedna usługa.

Ponadto Urząd udostępniał usługi elektroniczne z wykorzystaniem regionalnej platformy internetowej zamieszczonej na stronie internetowej Urzędu - e-urząd.um.opoczno.pl. Dostępne usługi dotyczyły: deklaracji na podatek od środków transportowych, na podatek leśny, na podatek od nieruchomości, na podatek rolny, deklaracji o wysokości opłat za gospodarowanie odpadami komunalnymi, informacji o lasach, o nieruchomościach i obiektach budowlanych oraz o gruntach.

(akta kontroli str. 54)

3. W pierwszym półroczu 2020 r. za pośrednictwem ogólnopolskiej platformy e-PUAP w Urzędzie zrealizowano 977 usług elektronicznych na rzecz obywateli, z czego:

- 137 usług w okresie od 1 stycznia 2020 r. do 28 lutego 2020 r.;
- 314 usług w okresie od 1 marca 2020 r. do 30 kwietnia 2020 r.;
- 526 usług w okresie od 1 maja 2020 r. do 30 czerwca 2020 r.

Najwięcej spraw wpłynęło do Urzędu w postaci pisma ogólnego, głównie o charakterze informacyjnym lub stanowiącym zapytanie (łącznie 214, tj. 21,9% wszystkich e-usług w tym okresie). Równie licznie do Urzędu wpływały sprawy z zakresu: dopisania do spisu wyborców lub głosowania korespondencyjnego (187, tj. 19,1%), wniosków o dowód osobisty, zameldowania lub wymeldowania (łącznie 169, tj. 17,3%) lub urodzeń, małżeństw, zgonów (103, tj. 10,5%).

Pozostałe wnioski lub zawiadomienia dotyczyły m.in.: ochrony środowiska (45 spraw), podatków i opłat (41 spraw) czy też zdrowia i spraw społecznych (35 spraw), wniosków do planu zagospodarowania przestrzennego (27 wniosków), rozliczeń i dotacji (21 spraw), wniosków o udzielenie informacji publicznej (20 wniosków).

Istotny wzrost zainteresowania e-usługami świadczonymi przez Urząd, nastąpił w okresie od 1 marca 2020 r. do 30 kwietnia 2020 r., tj. w początkowym okresie epidemii COVID-19 w Polsce (o prawie 130% w porównaniu z pierwszymi dwoma miesiącami roku). W tym czasie znacznie częściej występowało do Urzędu: w sprawach związanych ze zdrowiem i sprawami społecznymi (wzrost o 1100%), z wnioskiem do planu zagospodarowania przestrzennego (wzrost o 350%), w zakresie urodzeń, małżeństw i zgonów (wzrost o 300%), z wnioskiem o dowód osobisty, zameldowania lub wymeldowania (wzrost o 300%), w postaci pisma

⁸ W tym: dowody osobiste (pięć usług), wybory (jedna usługa), urodzenia, małżeństwa, zgony (sześć usług), inne (jedna usługa).

ogólnego, głównie o charakterze informacyjnym lub stanowiącym zapytanie (wzrost o 69%).

Z kolei w trakcie kolejnych dwóch miesięcy (maj-czerwiec 2020 r.) liczba spraw kierowanych do Urzędu przez ePUAP pozostawała w większości na stałym poziomie lub nadal wzrastała. Wyraźny wzrost w porównaniu do poprzednich dwóch miesięcy (marzec-kwiecień 2020r.) wystąpił w zakresie dopisywania do spisu wyborców lub głosowania korespondencyjnego (wzrost o 153 spraw, tj. o 900%). Wzrost ten spowodowany był przeprowadzanymi w miesiącu maju 2020 r. wyborami powszechnymi na Prezydenta Rzeczypospolitej Polskiej.

(akta kontroli str. 45-50)

4. Prowadzony w Urzędzie monitoring korzystania w okresie objętym kontrolą przez obywateli oraz przedsiębiorców z usług świadczonych w formie elektronicznej nie przybrał formy formalnych/papierowych analiz. Jednakże poziom wykorzystywania e-usług był analizowany na bieżąco przez komórkę informatyki w Urzędzie. Analiza polegała na sprawdzaniu ilości spraw, które wpływały przez system ePUAP, a następnie proponowaniu konkretnych działań polegających na poprawie wykorzystywania e-usług publicznych przez mieszkańców.

Ponadto, jak wyjaśnił Zastępca Burmistrza, system ePUAP nie udostępniał statystyk czy innego rodzaju zestawień – jedyną możliwością było ręczne zliczanie dokumentów wpływających przez system. Zauważony wzrost liczby dokumentów wpływających systemem, zdaniem Zastępcy Burmistrza, przyspieszył prace nad wdrożeniem systemu Elektronicznego Zarządzania Dokumentacją połączonego z ePUAP.

(akta kontroli str. 37-44)

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

(akta kontroli str. 37-44)

6. Zgodnie z zarządzeniem Burmistrza⁹ podstawowym sposobem dokumentowania przebiegu załatwiania i rozstrzygania spraw był w Urzędzie system tradycyjny, o którym mowa w § 1 załącznika nr 1 do rozporządzenia w sprawie instrukcji kancelaryjnej¹⁰. W Urzędzie czynności kancelaryjne wykonywane były w systemie Elektronicznego Zarządzania Dokumentacją (zwanym dalej systemem EZD), który był wspomagającym sposobem dokumentowania przebiegu, załatwiania i rozstrzygania spraw dla systemu podstawowego. Korespondencja wpływająca przez system EZD nie podlegała rejestracji w systemie tradycyjnym, tj. w dziennikach korespondencyjnych papierowych. System EZD pozwalał na wydrukowanie dzienników korespondencyjnych po zakończeniu każdego dnia pracy. System EZD, jako narzędzie wspomagające, wykorzystywany był do wykonywania następujących czynności kancelaryjnych związanych z obiegiem korespondencji:

- a) prowadzenia rejestru korespondencji przychodzącej i wychodzącej z Urzędu;
- b) dekretacji dokumentów;
- c) prowadzenia spisu spraw;
- d) gromadzenia dokumentów w zakresie prowadzonych spraw obejmujących przebieg załatwienia i rozstrzygnięcia, poprzez dołączenie istniejących dokumentów elektronicznych i skanowanie dokumentów papierowych;

⁹ Zarządzenie Burmistrza Opoczna nr 249/2019 z dnia 18 grudnia 2019 r. w sprawie zasad obiegu korespondencji przy wykorzystaniu Elektronicznego Zarządzania Dokumentacją (EZD) w Urzędzie Miejskim w Opocznie.

¹⁰ Rozporządzenie Prezesa Rady Ministrów z dnia 18 stycznia 2011 r. w sprawie instrukcji kancelaryjnej, jednolitych rzeczowych wykazów akt oraz instrukcji w sprawie organizacji i zakresu działania archiwów zakładowych (Dz. U. z 2011 r. Nr 14, poz. 67 ze zm.).

- e) sporządzania i udostępniania pism wewnątrz Urzędu;
- f) prowadzenia rejestrów;
- g) obsługi korespondencji wychodzącej z Urzędu;
- h) elektronicznego podpisywania korespondencji w systemie EZD;
- i) wysyłania korespondencji elektronicznej.

Funkcję administratora systemu EZD pełnił Inspektor Ochrony Danych Osobowych w Urzędzie, zaś nadzór nad realizacją przywołanego zarządzenia powierzony został Sekretarzowi Miasta.

(akta kontroli str. 37-44, 81-88)

W praktyce obieg dokumentów, zarówno papierowych, jak i elektronicznych, realizowany był przy użyciu systemu EZD, który umożliwiał także śledzenie postępu spraw. Dokumenty elektroniczne wpływały za pośrednictwem elektronicznej skrzynki podawczej poprzez ePUAP oraz na adres e-mail Urzędu¹¹, obsługiwany przez pracowników Biuro Obsługi Interesanta¹². Powyższe dokumenty następnie były rejestrowane w systemie EZD.

Weryfikacji podpisu elektronicznego, którym opatrzone były dokumenty elektroniczne, dokonywał pracownik Biura Obsługi Interesanta podczas pobierania korespondencji z ePUAP. Sprawy procedowane były w sposób mieszany (papierowy oraz elektroniczny). Pracownik Urzędu otrzymywał ich wydrukowaną wersję, z naniesioną dekretacją przełożonych. Osoby zaangażowane w przebieg danej sprawy miały wgląd - poprzez system EZD - do stanu jej realizacji. Pracownicy merytoryczni komórek organizacyjnych Urzędu byli zobowiązani do prowadzenia i zakończenia sprawy w EZD.

W Urzędzie, kwalifikowany podpis elektroniczny posiadali i wykorzystywali: Burmistrz, Zastępcy Burmistrza, Skarbnik, Sekretarz oraz Dyrektorzy poszczególnych Wydziałów (łącznie dziewięć osób). Pracownicy merytoryczni natomiast posiadali i wykorzystywali profil zaufany.

W okresie od 1 stycznia 2020 r. do 30 czerwca 2020 r. zostało podpisanych elektronicznie i wysłanych za pośrednictwem ePUAP 377 pism. Na dzień 14 września 2020 r. liczba ta wynosiła 529.

(akta kontroli str. 31-44, 81-106)

Odpowiedzi przekazywane w imieniu Urzędu przez ePUAP, podpisywane były przez osoby do tego upoważnione, tj. kierownictwo Urzędu lub Dyrektorów poszczególnych Wydziałów. Załączniki przesyłane były w postaci skanów dokumentów odręcznie podpisanych przez upoważnione osoby, bądź plików, przygotowanych przez pracowników merytorycznych i podpisanych elektronicznie, podpisem kwalifikowanym, przez osoby upoważnione przez Burmistrza. Przy procedowaniu spraw drogą elektroniczną poza ePUAP, w zależności od wymagań instytucji, do których przesyłane były dokumenty/sprawozdania, podpisy elektroniczne składane były przy użyciu profilu zaufanego pracownika Urzędu.

System EZD przy wyborze podpisu dokumentu proponował wybór pomiędzy profilem zaufanym a podpisem kwalifikowanym, jednakże system EZD nie posiadał możliwości wygenerowania raportu o liczbie dokumentów podpisanych poszczególnym podpisem.

(akta kontroli str. 37-44, 81-88)

¹¹ umopoczno@um.opoczno.pl,

¹² Odpowiednik kancelarii.

7. Szczegółowa analiza¹³ 20 spraw wpływających do Urzędu przez ePUAP w I półroczu 2020 r. wykazała, że:

- przekazanie do pracownika merytorycznego prowadzącego daną sprawę następowało w dniu złożenia dokumentu, kolejnym dniu roboczym lub w trzech przypadkach - najpóźniej po upływie trzech dni roboczych;
- w jednym przypadku, w którym badany wniosek nie był kompletny, po dokonanych przez Urząd wezwaniu, możliwe było jego uzupełnienie w drodze komunikacji elektronicznej;
- od momentu rozpoczęcia prowadzenia sprawy ciężar kontaktu z obywatelami oraz ewentualnie z innymi instytucjami spoczywał na Urzędzie. We wszystkich 20 analizowanych przypadkach, informacje przekazywano wnioskodawcom wyłącznie w formie elektronicznej (poprzez wiadomość mailową lub ePUAP). Przy realizacji sześciu spraw wymagających komunikacji z inną jednostką administracji publicznej, w sześciu przypadkach informacje przesyłano za pośrednictwem platformy ePUAP - występowano o opinie do: Zarządu Dróg Wojewódzkich w Łodzi, Państwowego Gospodarstwa Wodnego Wody Polskie w Warszawie, Regionalnej Dyrekcji Lasów Państwowych, Wojewódzkiego Urzędu Ochrony Zabytków w Łodzi, Samorządowego Kolegium Odwoławczego w Piotrkowie Trybunalskim oraz Państwowego Powiatowego Inspektora Sanitarnego w Opocznie. Instytucje te przekazały opinie poprzez ePUAP;
- system elektronicznego obiegu dokumentów (EZD) komunikował się automatycznie z innym systemem informatycznym w zakresie przesyłania danych – systemem dziedzicznym E-podatki. Ponadto dla załatwienia spraw Urząd korzystał z danych gromadzonych w zewnętrznych systemach takich jak m.in.: *Geoportal*, *Źródło*, *Rejestr PESEL*, *Rejestr Dowodów Osobistych*, czy *Rejestr Wyborców* i nie żądał od wnioskodawców dodatkowych informacji w tym zakresie;
- w jednym przypadku umożliwiono uzyskanie informacji o aktualnym stanie sprawy na stronie: *obywatel.gov.pl*. Uzyskanie informacji na temat aktualnego stanu procedowania sprawy w pozostałych 19 przypadkach możliwe było poprzez kontakt osobisty, mailowy lub telefoniczny, bowiem nie były one udostępniane poprzez EZD, stronę bądź platformę internetową, pozwalającą na samodzielne śledzenie postępu sprawy przez obywatela;
- wszystkie badane sprawy zostały całkowicie procedowane w formie elektronicznej.

(akta kontroli str. 57-59)

8. W latach 2016-2020 (I półrocze) wykorzystywana platforma ePUAP nie zawsze działała sprawnie i bezawaryjnie. Urząd ośmiokrotnie dokonywał zgłoszeń, drogą mailową, do Centralnego Ośrodka Informatyki (COI), w związku z napotkanymi problemami w funkcjonowaniu ePUAP. Zgłoszone problemy dotyczyły m.in.

¹³ Do szczegółowego badania wybrano losowo próbę 20 spraw wnoszonych przez obywateli (osoby fizyczne), w formie elektronicznej poprzez ePUAP, w okresie pomiędzy 1 stycznia 2020 r. a 30 czerwca 2020 r.: wniosek o wydanie dowodu osobistego, wniosek o wydanie zaświadczenia o zameldowaniu, wniosek o wydanie aktu urodzenia, wniosek o dopisanie do spisu wyborców, wniosek o ustalenie lokalizacji celu publicznego (2), wniosek o ustalenie warunków zabudowy i zagospodarowania terenu (2), odwołanie ws. naliczenia podatku, zawiadomienie o zmianach geodezyjnych (2), zawiadomienie o wygaśnięciu tytułów wykonawczych, pismo dot. opieki nad bezdomnymi zwierzętami, skarga na funkcjonowanie miejskiego przedsiębiorstwa komunalnego, informacja w zakresie publicznego transportu zbiorowego, prośba o wydanie decyzji na zajęcie pasa drogowego, wniosek o wydanie decyzji środowiskowej (2), wniosek o dostęp do geoportalu, informacja o realizacji zadania.

problemów z dodawaniem załączników do wysyłanych wiadomości, obsługi skrytki pocztowej (problemy z wysyłaniem i odbieraniem wiadomości).

(akta kontroli str. 107-184)

9. System monitorowania obiegu dokumentów, w tym elektronicznych (EZD), dostarczany był Urzędowi przez podmiot komercyjny. Umowa dotycząca korzystania z oprogramowania zawarta została w 2018 r. na pięć lat, w sposób zapewniający ciągłość dostępu do systemu. Treść umowy odnosiła się do czasu oraz sposobu reakcji producenta na usunięcie ewentualnych usterek w jego działaniu. Umowa określała rodzaje występujących kategorii zgłoszeń (tj. awaria, błąd lub wada) oraz czasy na usunięcie ewentualnych usterek tego oprogramowania, przez co zagwarantowała maksymalny czas, po jakim ma być przywrócone prawidłowe funkcjonowanie systemu.

(akta kontroli str. 185-204)

10. Aktualna na dzień prowadzenia kontroli NIK strona podmiotowa Biuletynu Informacji Publicznej Gminy¹⁴ posiadała łatwo dostępną zakładkę „Elektroniczna skrzynka podawcza ePUAP”, której wybór umożliwiał zapoznanie się z podstawowymi informacjami o możliwości załatwienia spraw drogą elektroniczną, w tym m.in. o:

- ustawowym¹⁵ zobowiązaniu podmiotów świadczących usługi publiczne do umożliwienia interesantom wnoszenia ich wniosków w formie dokumentów elektronicznych poprzez Elektroniczną Skrzynkę Podawczą podmiotu,
- konieczności do spełnienia warunkach umożliwiających korzystanie z e-usług świadczonych przez platformę e-PUAP, w tym wymogu założenia konta użytkownika na platformie ePUAP (wraz z informacją, że konto takie jest bezpłatne) oraz możliwościach, jakie daje posiadanie profilu zaufanego i podpisu elektronicznego.

Na stronie internetowej zawarto informacje o sposobie uzyskania profilu zaufanego, ale nie zawarto informacji dot. dowodu osobistego z warstwą elektroniczną (e-dowód), ani nie wskazano możliwości posługiwania się e-dowodem przy prowadzeniu spraw drogą elektroniczną, jednakże zamieszczono linki odsyłające do stron: epuap.gov.pl oraz www.obywatel.gov.pl, stanowiących źródło wiedzy w tym zakresie.

Ponadto znajdowały się odniesienia (hiperłącza) do następujących stron internetowych: www.elodzkie.pl – Wrota Regionu Łódzkiego Portal E-usług, Rejestr Danych Kontaktowych, Centralna Ewidencja i Informacja o Działalności Gospodarczej, Elektroniczne Księgi Wieczyste, Baza Adresowa Wojewódzkiego Łódzkiego.

(akta kontroli str. 45-50, 205)

Na stronie internetowej Gminy w zakładce „e-urząd” znajdował się dostęp do elektronicznego portalu miejskiego z publicznymi e-usługami dostępnymi dla mieszkańców. Liczba usług została opisana w pkt 2 niniejszego wystąpienia pokontrolnego.

(akta kontroli str. 205)

11. W okresie od 30 maja 2018 r. do 30 czerwca 2020 r. pracownicy Urzędu uczestniczyli w czterech wewnętrznych szkoleniach z zakresu ochrony danych osobowych oraz bezpieczeństwa informacji (uwzględniając m.in.: zagrożenia bezpieczeństwa informacji, skutki naruszenia bezpieczeństwa informacji, w tym odpowiedzialność prawną, o czym mowa w § 20 ust. 2 pkt 6 rozporządzenia KRI),

¹⁴ www.bip.opoczno.pl.

¹⁵ Zgodnie z ustawą z dnia 12 lutego 2010 roku o zmianie ustawy o informatyzacji działalności podmiotów realizujących zadania publiczne oraz niektórych innych ustaw (Dz. U. z 2010 r. nr 40 poz. 230).

prowadzonych przez Inspektora Danych Osobowych. We wskazanych formach podnoszenia kompetencji udział wzięło łącznie 106 pracowników Urzędu.

W powyższym okresie Inspektor Danych Osobowych odbył cztery zewnętrzne szkolenia w przedmiotowym zakresie.

Ponadto: w dniu 9 listopada 2017 r. 56 pracowników Urzędu i jednostek podległych wzięło udział w szkoleniu zewnętrznym pn. Ochrona danych osobowych w perspektywie zmian (...); w dniach 22-25 kwietnia 2018 r. czterech pracowników Urzędu wzięło udział w zewnętrznym szkoleniu - warsztaty kompetencyjne w zakresie ochrony danych osobowych.

(akta kontroli str. 37-44, 206-238)

12. Opracowana i obowiązująca w Urzędzie w latach 2016-2018¹⁶ dokumentacja SZBI, na którą składały się: „Polityka Bezpieczeństwa Informacji”¹⁷, „Instrukcja zarządzania systemami informatycznymi służącymi do przetwarzania danych osobowych”, „Instrukcja postępowania w przypadku naruszenia ochrony danych osobowych w systemie informatycznym”¹⁸ oraz zastępująca je z dnia 25 maja 2018 r. „Polityka Bezpieczeństwa Informacji”¹⁹ wraz z Instrukcjami²⁰ (dalej określane odpowiednio jako: *Polityki i Instrukcja*) była zgodna z wymogami § 20 ust. 1 Rozporządzenia KRI. Zgodnie z treścią ww. przepisu prawa, Urząd opracował, ustanowił, eksploatował i monitorował, przeglądał oraz utrzymywał i doskonalił system zarządzania bezpieczeństwem informacji zapewniający poufność, dostępność i integralność informacji z uwzględnieniem takich atrybutów jak autentyczność, rozliczalność, niezaprzeczalność i niezawodność. Ponadto, przedstawione przez Urząd regulacje – zgodnie z § 20 ust. 3 Rozporządzenia KRI - zostały opracowane na podstawie Polskiej Normy PN-ISO/IEC 27001 „Technika informatyczna. Techniki bezpieczeństwa. Systemy zarządzania bezpieczeństwem informacji. Wymagania”, a ustanawianie zabezpieczeń, zarządzanie ryzykiem oraz audytowanie odbywało się na podstawie odpowiednich Polskich Norm²¹.

Innym dokumentem regulującym kwestię bezpieczeństwa i dostępu do przechowywanych w Urzędzie danych była *Instrukcja postępowania z kluczami oraz zabezpieczenia pomieszczeń w budynkach Urzędu Miejskiego w Opocznie*²², obowiązująca od 6 lutego 2020 r.

(akta kontroli str. 239-301)

Zgodnie z treścią Polityk²³ - wszyscy pracownicy Urzędu zostali zapoznani z treścią ww. dokumentów o czym świadczyły pisemne oświadczenia pracowników o zapoznaniu się z treścią i zobowiązaniu do stosowania regulacji.

(akta kontroli str. 239-289)

Zarządzeniem Burmistrza Opoczna nr 4/2001 z dnia 19 listopada 2001 r. powołano Administratora Bezpieczeństwa Informacji (od 23 sierpnia 2018 r. – zgodnie z zarządzeniem nr 147/2018 - Inspektora Ochrony Danych, odpowiedzialnego za m.in. opracowanie, wdrożenie, przegląd i modyfikację wskazanych procedur).

¹⁶ Do dnia 25 maja 2018 r.

¹⁷ Obydwie instrukcje zostały wprowadzona zarządzeniem Burmistrza Opoczna nr 205 z dnia 12 grudnia 2008 r. w sprawie wdrożenia Dokumentacji Systemu Zarządzania Bezpieczeństwem Informacji w Urzędzie Miejskim w Opocznie.

¹⁸ Wprowadzona zarządzeniem Burmistrza Opoczna nr 205 z dnia 12 grudnia 2008 r. w sprawie wdrożenia Dokumentacji Systemu Zarządzania Bezpieczeństwem Informacji w Urzędzie Miejskim w Opocznie.

¹⁹ Wprowadzona zarządzeniem Burmistrza Opoczna nr 96/2018 z dnia 25 maja 2018 r. w sprawie wdrożenia Dokumentacji Systemu Zarządzania Bezpieczeństwem Informacji w Urzędzie Miejskim w Opocznie.

²⁰ Instrukcja zarządzania systemem informatycznym oraz Instrukcja postępowania w sytuacji naruszeń danych osobowych.

²¹ W tym: PN-ISO/IEC 27002 - w odniesieniu do ustanawiania zabezpieczeń, PN-ISO/IEC 27005 – w odniesieniu do zarządzania ryzykiem, PN-ISO/IEC 24762 - w odniesieniu do odtwarzania techniki informatycznej po katastrofie w ramach zarządzania ciągłością działania.

²² Stanowiąca załącznik nr 1 do zarządzenia Burmistrza Opoczna nr 18/2020 z dnia 6 lutego 2020 r.

²³ Rozdział XII.

(akta kontroli str. 302-209)

13. Obowiązek zapewnienia aktualności regulacji wewnętrznych, wynikający z § 20 ust. 2 pkt 1 Rozporządzenia KRI, zawarty został w rozdziale XX *Polityki* z 2018 r. i zakładał, że IOD okresowo będzie analizował zagrożenia i ryzyko w celu weryfikacji zastosowania środków zabezpieczających w celu zapewnienia aktualności procedur i instrukcji przy przetwarzaniu danych osobowych. W Urzędzie co roku dokonywano przeglądu oraz sprawdzenia ww. dokumentacji oraz sporządzano dokumentację z tych czynności.

(akta kontroli str. 45-50, 310-365)

14. Dokumentacja *Polityk* obejmowała zakresem m.in. organizację przetwarzania danych osobowych, identyfikację zagrożeń (analiza ryzyk), infrastrukturę przetwarzania danych osobowych, zasady udostępniania tych danych i postępowania przy naruszeniu ich bezpieczeństwa, odpowiedzialność osób upoważnionych do przetwarzania danych osobowych, zasady funkcjonowania monitoringu wizyjnego. Integralnym dokumentem *Polityk* była *Instrukcja*, stanowiąca wytyczne w zakresie m.in.: nadawania i rejestrowania uprawnień, metod i środków uwierzytelniania, procedur podczas pracy użytkowników systemu, korzystania z internetu i poczty elektronicznej, tworzenia kopii zapasowych, zabezpieczania i dostępu do systemu informatycznego podmiotów zewnętrznych.

(akta kontroli str. 239-289)

15. Urząd został wyposażony w oprogramowanie dedykowane elektronicznej inwentaryzacji zasobów informatycznych, obejmujące ich rodzaj i konfigurację, a także zawierające informacje, w jaki sposób elementy te są ze sobą powiązane (tzw. bazę konfiguracji CMDB²⁴). Prowadzony wykaz sprzętu i oprogramowania informatycznego, spełniał wymagania określone w § 20 ust. 2 pkt 2 Rozporządzenia KRI, pod kątem utrzymywania aktualności inwentaryzacji sprzętu i oprogramowania służącego do przetwarzania informacji, obejmującej ich rodzaj i konfigurację. Na potrzeby wewnętrzne, Urząd posiadał dodatkowy wspomagający program w procesie inwentaryzacji.

Badanie przeprowadzone na podstawie 15 losowo wybranych pozycji zasobów informatycznych²⁵ wykazało, że wszystkie były zgodne z ww. programami w zakresie: numerów inwentarzowych, przypisanych użytkowników sprzętu oraz zainstalowanego oprogramowania. Ponadto, wszystkie sprzęty komputerowe, zostały odpowiednio przypisane do osób, które użytkowały dany sprzęt.

(akta kontroli str. 45-50, 62-66)

16. Weryfikacja²⁶ możliwości samodzielnego zainstalowania nieautoryzowanego oprogramowania na komputerach użytkowanych przez pracowników, niebędących pracownikami służb informatycznych Urzędu wykazała, że taka instalacja nie była możliwa na wszystkich losowo wybranych do badania komputerach oraz laptopach. Stwierdzony stan faktyczny stanowił o wystarczającej realizacji wymagań²⁷ określonych w § 20 ust. 2 pkt 4 Rozporządzenia KRI, pod kątem adekwatnego

²⁴ Ang. *Configuration Management Database*, która umożliwia m.in. odtworzenie infrastruktury teleinformatycznej po katastrofie lub innym zdarzeniu losowym.

²⁵ W tym: 10 komputerów, dwa laptopy, jeden serwer, jeden router i jedna drukarka, dobrane w sposób celowy spośród łącznie: 61 szt. komputerów stacjonarnych oraz serwerów, 10 szt. laptopów, 38 szt. drukarek, sześciu kserokopiarek i trzech routerów.

²⁶ Do próby wytypowano 10 komputerów, w tym: pięć komputerów stacjonarnych, wylonionych w sposób losowy w Urzędzie oraz pięć laptopów/notebooków, wybranych w sposób losowy.

²⁷ Wymóg nieprzyznawania praw administracyjnych do systemu operacyjnego, a co się z tym wiąże - zapobiegania możliwości dokonywania instalacji, wynikał ponadto z praktyki określonej w załączniku A normy PN-ISO/IEC 27001:2014-12 (punkt A.9.2.3) i stanowił, że przydzielanie i wykorzystywanie praw uprzywilejowanego dostępu należało ograniczyć i nadzorować.

przydzielania uprawnień osobom zaangażowanym w proces przetwarzania informacji.

(akta kontroli str. 60-61)

17. W przypadku wszystkich (15) losowo²⁸ zweryfikowanych kont pracowników, którzy w latach 2016-2020 rozwiązali stosunek pracy z Urzędem, zmiana uprawnień dostępu do zasobów komputera była realizowana zgodnie z § 20 ust. 2 pkt 5 Rozporządzenia KRI – konta zostały wygaszone/zablokowane – niezwłocznie, tj. od 0 do 7 dni po rozwiązaniu stosunku pracy z pracownikiem.

W zakresie blokowania kont lub odbierania uprawnień dostępu, w latach 2016-2019 w Urzędzie nie sporządzano formalnych wniosków - dyspozycja była przekazywana ustnie przez Dyrektorów poszczególnych Wydziałów do administratora systemów informatycznych w Urzędzie. Od 1 stycznia 2020 r. istniała formalna procedura nadawania, modyfikacji i odbierania uprawnień pracownikom, polegająca na złożeniu właściwego dokumentu. Powyższa procedura została opisana w rozdziale XII pkt 2 i 3 *Polityki*.

(akta kontroli str. 45-50, 67-72)

18. Do prowadzenia audytu wewnętrznego z zakresu bezpieczeństwa informacji, oprócz Audytora Wewnętrznego, upoważnionym był także Inspektor Ochrony Danych²⁹, w którego kompetencjach leżał audyt zgodności przetwarzania danych z przepisami o ochronie danych osobowych.

W latach 2016-2020 przeprowadzano coroczne audyty z zakresu bezpieczeństwa informacji, wymagane § 20 ust. 2 pkt 14 Rozporządzenia KRI. Każdy z protokołów audytu zawierał stosowne rekomendacje, których wprowadzenie było sprawdzane podczas następnego audytu. W każdym analizowanym przypadku wystosowane rekomendacje zostały zrealizowane.

(akta kontroli str. 45-50, 310-365)

Stwierdzone
nieprawidłowości

W działalności kontrolowanej jednostki w przedstawionym wyżej zakresie nie stwierdzono nieprawidłowości.

IV. Uwagi i wnioski

W związku z niestwierdzeniem nieprawidłowości Najwyższa Izba Kontroli nie formułuje uwag ani wniosków.

V. Pozostałe informacje i pouczenia

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

Prawo zgłoszenia
zastrzeżeń

Zgodnie z art. 54 ustawy o NIK kierownikowi jednostki kontrolowanej przysługuje prawo zgłoszenia na piśmie umotywowanych zastrzeżeń do wystąpienia pokontrolnego, w terminie 21 dni od dnia jego przekazania. Zastrzeżenia zgłasza się do dyrektora Delegatury NIK w Łodzi. Prawo zgłaszania zastrzeżeń, zgodnie z art. 61b ust. 2 ustawy o NIK, nie przysługuje do wystąpienia pokontrolnego zmienionego zgodnie z treścią uchwały w sprawie zastrzeżeń.

²⁸ Weryfikacją objęto próbę 15 byłych pracowników Urzędu, dobranych w sposób losowy.

²⁹ Odpowiednio przed 2018 r. - Administrator Bezpieczeństwa Informacji.

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

Łódź, dnia 12 października 2020 r.

Kontroler
Adam Markiewicz
Specjalista kontroli państwowej


podpis

Najwyższa Izba Kontroli
Delegatura w Łodzi
Dyrektor
Przemysław Szewczyk


podpis