NAJWYŻSZA IZBA KONTROLI
Delegatura w Łodzi

LLO.410.009.02.2020

Waldemar Chałat
Burmistrz Koluszek
Urząd Miejski w Koluszkach
Ul. 11 Listopada 65, 95-040 Koluszki

WYSTĄPIENIE POKONTROLNE

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

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

I. Dane identyfikacyjne

Jednostka kontrolowana	Urząd Miejski w Koluszkach[1], ul. 11 Listopada 65 95-040 Koluszki
Kierownik jednostki kontrolowanej	Waldemar Chałat, Burmistrz Koluszek, od 24 listopada 2014 r.[2]
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	Okres 2016-2020 (do dnia zakończenia kontroli)
Podstawa prawna podjęcia kontroli	Art. 2 ust. 2 ustawy z dnia 23 grudnia 1994 r. o Najwyższej Izbie Kontroli[3]
Jednostka przeprowadzająca kontrolę	Najwyższa Izba Kontroli Delegatura w Łodzi
Kontroler	Katarzyna Kaczkowska, doradca techniczny, upoważnienie do kontroli nr LLO/83/2020 z dnia 10 czerwca 2020 r. (akta kontroli str. 1-3)

[1] Zw. dalej Urzędem.
[2] Zw. dalej Burmistrzem.
[3] Dz. U. z 2020 r. poz. 1200, zw. dalej ustawą o NIK.

II. Ocena ogólna[4] kontrolowanej działalności

OCENA OGÓLNA

Najwyższa Izba Kontroli negatywnie ocenia działalność kontrolowanej jednostki w zakresie realizacji zadań związanych z usługami publicznymi świadczonymi na rzecz obywateli z wykorzystaniem platformy ePUAP. Ujawnione w toku kontroli nieprawidłowości uzasadniają zastosowanie oceny negatywnej, w szczególności z uwagi na:

- nierzetelne dokumentowanie czynności w ramach prowadzonych spraw wpływających poprzez platformę ePUAP,
- przypadki realizowania e-usług z dużym opóźnieniem, wynoszącym nawet 120 dni od dnia wpływu wniosku na platformę ePUAP,
- nieopracowanie i niewdrożenie Systemu Zarządzania Bezpieczeństwem Informacji, a w szczególności Polityki Bezpieczeństwa Informacji. W Urzędzie ustanowione zasady dotyczyły wyłącznie bezpieczeństwa przetwarzania danych osobowych oraz dostępu do pomieszczeń służbowych,
- niezapewnienie należytej i terminowej realizacji zadań dotyczących odbierania uprawnień do systemów informatycznych osobom, które zakończyły zatrudnienie w Urzędzie,
- nieprzeprowadzanie w 2016 r. i w 2018 r. obowiązkowego audytu wewnętrznego w zakresie bezpieczeństwa informacji,
- nieorganizowanie szkoleń z zakresu bezpieczeństwa informacji dla pracowników Urzędu obsługujących bądź realizujących e-usługi.

III. Opis ustalonego stanu faktycznego

OBSZAR

1. Świadczenie przez Urząd e-usług. Rozwiązania organizacyjne i techniczne w zakresie zapewnienia bezpieczeństwa przetwarzania informacji w Urzędzie i ich stosowanie

Opis stanu faktycznego

1. W latach 2016-2020 (do 17 czerwca) w Urzędzie nie zostały opracowane dokumenty strategiczne Gminy Koluszki, które uwzględniałyby zagadnienia dotyczące dostosowania Urzędu do elektronicznego świadczenia usług publicznych oraz inne dokumenty, które wskazywałyby kierunki rozwoju na najbliższe lata.
Sekretarz Gminy (z up. Burmistrza) wyjaśniła, że nie opracowano dokumentów strategicznych uwzględniających zagadnienia elektronicznego świadczenia usług publicznych z uwagi na nadal małe zainteresowanie mieszkańców korzystaniem z tego rodzaju usług.

(akta kontroli str. 178-183)

2. Według stanu na dzień 31 maja 2020 r. Urząd udostępnił mieszkańcom – poprzez ogólnopolską platformę ePUAP – 10 usług elektronicznych w poszczególnych grupach:

- „Pismo ogólne, skargi, wnioski, zapytania do Urzędu" – 1 usługę,

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

- „Bezpieczeństwo i zarządzanie kryzysowe" (imprezy masowe, zgromadzenia publiczne, sprawy obronne) – 1 usługę: „Przyjmowanie zawiadomień o organizacji zgromadzenia publicznego",
- „Budownictwo, architektura, urbanistyka" – 1 usługę: „Wydawanie wypisu i wyrysu ze studium uwarunkowań i kierunków zagospodarowania przestrzennego",
- „Dowody osobiste, meldunki, wybory" – 4 usługi: 1) „Zameldowanie na pobyt stały i czasowy", 2) „Wniosek o dowód osobisty", 3) „Zgłoszenie zamiaru głosowania korespondencyjnego dla osób głosujących w Polsce", 4) „Dopisanie się do spisu wyborców",
- „Urodzenia, małżeństwa, zgony" – 1 usługę: „Wnioskowanie o wydanie odpisu aktu stanu cywilnego",
- „Inne" – 2 usługi: 1) „Objęcie patronatem imprez o charakterze lokalnym i ponadlokalnym", 2) „Rozpatrywanie wniosków o wyrażenie zgody na używanie herbu miasta".

W Urzędzie nie funkcjonowała inna platforma (np. regionalna, miejscowa) udostepniająca mieszkańcom usługi drogą elektroniczną.

(akta kontroli str. 175-176)

3. W I półroczu 2020 r. poprzez platformę ePUAP do Urzędu wpłynęło 271 spraw. Najwięcej spraw (185) Urząd zarejestrował w okresie od 1 maja do 30 czerwca[5], 56 – od 1 marca do 30 kwietnia[6], a 30 – od 1 stycznia do 29 lutego[7].

Zarejestrowane w I półroczu 2020 r. sprawy dotyczyły wniosków: o zameldowanie na pobyt stały i czasowy (20 wniosków), o wydanie odpisu aktu stanu cywilnego (29), o wydanie dowodu osobistego (54 wnioski), a także pism ogólnych, zapytań (43 wnioski) i zgłoszenia zamiaru głosowania korespondencyjnego dla osób głosujących w Polsce oraz dopisania się do spisu wyborców (122 wnioski). O wydanie wypisu i wyrysu ze studium uwarunkowań i zagospodarowania przestrzennego złożono 2 wnioski, a zgłoszenie urodzenia dziecka – 1 wniosek.

Znaczny wzrost (ponad 15%) usług wpływających do Urzędu w okresie II i III w stosunku do okresu I nastąpił w następujących grupach usług:

- pisma ogólne, skargi, wnioski, zapytania do Urzędu – odpowiednio o 18% i 73%,
- wnioskowanie o wydanie dowodu osobistego – odpowiednio o 33% i 117%,
- zameldowanie na pobyt stały i czasowy – odpowiednio o 400% i 300%,
- zgłoszenie zamiaru głosowania korespondencyjnego oraz dopisania się do rejestru wyborców – odpowiednio o 800% i 11.100%,
- wydanie odpisu aktu stanu cywilnego – odpowiednio o 100% i 325%.

(akta kontroli str. 413)

Zdaniem Sekretarz Gminy (z up. Burmistrza), brak zainteresowania ze strony obywateli usługami świadczonymi przez platformę ePUAP może wynikać z faktu pochodzenia społecznego obywateli (gmina miejsko-wiejska) oraz może być spowodowana trudnościami w posługiwaniu się internetem. Ponadto wyjaśniła, że dla osób już korzystających z platformy dużym zniechęceniem jest jej nieprawidłowe działanie, np. zawieszanie się systemu, wyrzucanie zalogowanego pracownika, trudności z dodaniem załączników oraz czas oczekiwania na wysyłkę pisma – od 40 min do nawet 3 godzin.

(akta kontroli str. 533-542)

---

[5] Zw. dalej okres III.
[6] Zw. dalej okres II.
[7] Zw. dalej okres I.

4. W Urzędzie w latach 2016-2020 (do 3 lipca) bieżący monitoring poziomu wykorzystania e-usług realizowanych poprzez ePUAP – jak wyjaśniła Sekretarz Gminy (z up. Burmistrza) – sprawują poszczególni pracownicy na stanowiskach merytorycznych. Natomiast nie analizują oni informacji na temat korzystania przez obywateli i przedsiębiorców z usług świadczonych w formie elektronicznej.

(akta kontroli str. 205-212)

5. W okresie od 1 stycznia 2016 r. do 7 lipca 2020 r. do Urzędu poprzez platformę ePUAP wpłynęła jedna skarga od obywatela (w dniu 23 czerwca 2020 r.) na brak działań Dyrektora Przedszkola nr 3 w Koluszkach[8]. Skarga została załatwiona w ciągu 3 dni przez pracownika komórki organizacyjnej Urzędu odpowiedzialnego za sprawy oświaty.

NIK zwraca uwagę, że pomimo uznania tej skargi za zasadną, nie odnotowano jej w rejestrze skarg. Burmistrz wyjaśnił, że dokument ten został potraktowany jako pismo ogólne.

W ww. okresie do Urzędu nie wpłynęły wnioski w sprawie usprawnienia elektronicznej formy komunikacji mieszkańców z Urzędem.

(akta kontroli str. 178-183, 249, 486-492, 569)

6. Według stanu na 9 lipca 2020 r. w Urzędzie funkcjonował – jako podstawowy – tradycyjny system obiegu dokumentów. Elektroniczny obieg dokumentów (wpływających poprzez platformę ePUAP) funkcjonował jedynie jako system pomocniczy i obejmował rejestrację spraw wpływających do Urzędu.

W praktyce, czynności kancelaryjne, w tym rejestrowanie korespondencji przychodzącej – mailowo lub poprzez platformę ePUAP – dokonywane było w systemie tradycyjnym, tj. korespondencja była drukowana przez pracownika sekretariatu, a następnie przedkładana Burmistrzowi do dekretacji i przekazywana do poszczególnych pracowników Urzędu.

Obieg dokumentów w Urzędzie regulowało, jak wyjaśniła Sekretarz Gminy (z up. Burmistrza), rozporządzenie Rady Ministrów z 18 stycznia 2011 r. w sprawie instrukcji kancelaryjnej, jednolitych rzeczowych wykazów akt oraz instrukcji w sprawie organizacji i zakresu działania archiwów zakładowych.

(akta kontroli str. 178-183, 205-212, 393-394)

Rejestracja korespondencji przychodzącej w dzienniku kancelaryjnym oraz obsługa w zakresie odbioru korespondencji przychodzącej na skrzynkę ePUAP należały do obowiązków pracownika sekretariatu Urzędu.

(akta kontroli str. 4-5, 393-394)

Według stanu na dzień 30 czerwca 2020 r. podpis elektroniczny posiadało 29 pracowników Urzędu. Byli to m.in. Burmistrz Koluszek, Skarbnik Gminy, Sekretarz Gminy, Kierownik Urzędu Stanu Cywilnego, audytor wewnętrzny oraz inspektorzy poszczególnych referatów Urzędu.

W okresie od 1 stycznia 2020 r. do 30 czerwca 2020 r. z wykorzystaniem podpisu elektronicznego do petentów wysłanych zostało łącznie siedem pism: pięć przez Kierownika USC i dwa – przez Inspektora Referatu Planowania Przestrzennego i Gospodarki Nieruchomościami.

(akta kontroli str. 398-399)

Analiza obu spraw załatwionych przez Inspektora Referatu Planowania Przestrzennego i Gospodarki Nieruchomościami z wykorzystaniem elektronicznego obiegu dokumentów wykazała, że korespondencja wpływająca do Urzędu poprzez platformę ePUAP była: 1) rejestrowana przez pracownika sekretariatu, 2) drukowana i przedkładana Burmistrzowi do dekretacji na Dyrektora Wydziału Inwestycji i Rozwoju, 3) Dyrektor dekretował korespondencję na kierownika referatu,

[8] Sprawa nr EDŚ.4424.29.2020 – skarżący złożył do Dyrektora Przedszkola nr 3 w Koluszkach pisma: 26 lutego 2020 r. i 27 kwietnia 2020 r. i do dnia 26 czerwca 2020 r. nie uzyskał na nie odpowiedzi.

a ten – na pracownika merytorycznego, 4) pracownik ten dokonywał analizy sprawy oraz w razie potrzeby przygotowywał projekt pisma wychodzącego do akceptacji przez kierownika komórki organizacyjnej, 5) pracownik przygotowywał dokument końcowy, 6) podpisywał go podpisem elektronicznym oraz 6) wysyłał do petenta, z zaznaczeniem opcji: „potwierdzenie odbioru".
Dokumentacja wpływająca od osób fizycznych poprzez platformę ePUAP do Urzędu miała obieg dwutorowy, tj., pracownik merytoryczny zadekretowaną korespondencję otrzymywał w wersji papierowej oraz również miał możliwość załatwienia sprawy w wersji elektronicznej na platformie ePUAP.

Pracownik merytoryczny, by mógł wysłać platformą ePUAP dokumenty podpisane swoim podpisem elektronicznym musiał do programu wprowadzić kod autoryzacyjny, który otrzymywał sms-em na telefon komórkowy. Analizowane dokumenty zostały podpisane przez pracownika faktycznie obsługującego sprawę.
(akta kontroli str. 393-394, 400-412)

7. Analiza 20 spraw[9] wpływających poprzez ePUAP wykazała, że:
- w 15 sprawach pisma/wnioski obywateli rejestrowane były przez Urząd w dniu wpływu sprawy na platformę ePUAP,
- w siedmiu sprawach dekretacja na stanowisko merytoryczne nastąpiła w dniu następnym po dacie rejestracji pisma/wniosku obywatela w Urzędzie, a w jednej sprawie – w tym samym dniu,
- w 17 przypadkach analizowane wnioski/formularze nie wymagały korekt i uzupełnień; w pozostałych sprawach wystąpiła konieczność uzupełnienia wniosków o numery ewidencyjne nieruchomości oraz potwierdzenia wniesienia opłaty skarbowej,
- w 19 przypadkach obywatel mógł załatwić swoją sprawę bez konieczności dostarczania danych, będących w posiadaniu innego urzędu administracji publicznej. Nie wystąpiła konieczność komunikowania się z inną jednostką administracji publicznej za pośrednictwem platformy ePUAP w celu uzyskania koniecznych informacji/danych,
  W przypadku spraw prowadzonych przez Urząd Stanu Cywilnego, USC po otrzymaniu wniosku o wydanie odpisu aktu stanu cywilnego zwracał się poprzez aplikację Źródło do urzędu stanu cywilnego, w zasobach którego znajdowała się księga o migracji żądanego aktu,
- w Urzędzie możliwe było uzyskanie informacji na temat aktualnego stanu wydania dowodu osobistego. W pozostałych przypadkach obywatel mógł uzyskać informacje na temat załatwianej sprawy drogą telefoniczną, elektroniczną lub poprzez sms,
- wszystkie sprawy załatwiane były w formie papierowej, tj. drukowane w sekretariacie Urzędu i przekazywane do poszczególnych Wydziałów/ Referatów,
- system elektronicznego obiegu dokumentów w Urzędzie nie komunikował się automatycznie z innymi systemami informatycznymi Urzędu w zakresie przesyłania danych finansowych, gdyż – jak wyjaśniła Sekretarz Gminy (z up. Burmistrza) – w Urzędzie obowiązuje tradycyjny, tj. papierowy obieg dokumentów.

(akta kontroli str. 403-411, 414-531, 560, 561-568)

8. W okresie od 1 stycznia 2016 r. do 30 czerwca 2020 r. w Urzędzie nie zostały opracowane – w sposób sformalizowany – zasady dokonywania zgłoszeń

[9] Analizy dokonano na próbie 20 spraw z następujących obszarów: sprawy osobowe (dowód osobisty, meldunki, akty stanu cywilnego, wybory); pismo ogólne, skargi, wnioski, zapytania do Urzędu; geodezja. W Urzędzie nie świadczono przez ePUAP usług elektronicznych w grupach: gospodarka komunalna oraz podatki i opłaty.

o problemach technicznych występujących w funkcjonowaniu platformy ePUAP oraz tryb ich załatwiania.
Platforma ePUAP – jak wyjaśniła Sekretarz Gminy (z up. Burmistrza) – traktowana była przez pracowników Urzędu jak każdy inny system informatyczny.

(akta kontroli str. 178-183, 205-212)

Zasady w przypadku odbiegającego od normy działania systemu informatycznego zostały opisane w § 79 pkt 8 „Polityki bezpieczeństwa przetwarzania danych osobowych[10] (zw. dalej polityką bezpieczeństwa przetwarzania danych osobowych), zgodnie z którą użytkownik systemu informatycznego przetwarzającego dane osobowe niezwłocznie powiadamia Administratora Systemu Informatycznego[11]. Każde zakłócenie pracy systemu zauważone przez użytkownika wymaga zgłoszenia ASI osobiście lub telefonicznie. Brak było natomiast zapisów dotyczących trybu działania (tj. trybu załatwienia spraw) przez ASI.
Polityka bezpieczeństwa Urzędu Miejskiego w Koluszkach, ze szczególnym uwzględnieniem ochrony danych osobowych"[12] (zw. dalej Polityką z 2016 r.) nie zawierała zapisów dotyczących zasad dokonywania zgłoszeń o problemach technicznych występujących w funkcjonowaniu systemów informatycznych, w tym platformy ePUAP oraz trybu ich załatwiania. W § 7 pkt 4 wskazano jedynie, że *„gdy zachodzi podejrzenie naruszenia bezpieczeństwa systemu informatycznego, użytkownicy bezzwłocznie muszą o tym fakcie powiadomić ASI."*

(akta kontroli str. 69-134)

Sekretarz Gminy (z up. Burmistrza) wyjaśniła, że Urząd nie jest właścicielem ani administratorem platformy ePUAP, więc nie może dokonywać czynności mających na celu dbanie o sprawne i bezawaryjne działanie platformy. Służby informatyczne mogą dbać tylko o prawidłowy dostęp do platformy ePUAP po stronie użytkownika, czyli zapewnić sprawne i bezpieczne działanie sieci komputerowej Urzędu oraz urządzeń w niej się znajdujących. Utrudnienia w dostępie do platformy występują często, ze względu na przeciążenie jej serwerów oraz bardzo częste prace serwisowe. Spiętrzenie problemów występowało przeważnie podczas okresów sprawozdawczych, czy akcji wyborczych. Urząd nie ewidencjonuje problemów związanych z działaniem platformy ePUAP.

(akta kontroli str. 205-212)

9. W latach 2016-2020 Urząd corocznie zawierał umowy, zapewniające stałe działanie elektronicznego obiegu dokumentów oraz usuwania ewentualnych usterek. W umowach Urząd zagwarantował sobie reakcję dostawcy usług asysty technicznej i opieki autorskiej w zakresie Programu FINN 8 SQL na problemy w działaniu elektronicznego obiegu dokumentów. W § 2 analizowanych umów określono terminy naprawy błędów:

- przy awarii krytycznej (niepoprawne działanie oprogramowania uniemożliwiające świadczenie przez Urząd podstawowych usług, w szczególności powodujące utratę danych lub naruszenie ich spójności) – 2 dni robocze od otrzymania zgłoszenia; w sytuacji, gdy dostawca wprowadzi rozwiązanie tymczasowe, doraźnie rozwiązujące problem – usunięcie błędu nastąpi w terminie 9 dni roboczych od otrzymania formalnego zgłoszenia (pkt 4),
- przy awarii niekrytycznej (niepoprawne działanie oprogramowania negatywnie wpływające na wydajność i funkcjonalność systemu, ale umożliwiające

[10] Zarządzenie nr 42/2019 Burmistrza Koluszek z dnia 12 marca 2019 r. w sprawie wdrożenia „Polityki bezpieczeństwa przetwarzania danych osobowych w Urzędzie Miejskim w Koluszkach".
[11] Zw. dalej ASI.
[12] Zarządzenie nr 30/2016 Burmistrza Koluszek z dnia 29 lutego 2016 r. w sprawie ochrony danych osobowych w Urzędzie Miejskim w Koluszkach, wprowadzenia dokumentacji przetwarzania danych osobowych oraz warunków technicznych i organizacyjnych, jakim powinny odpowiadać urządzenia i systemy informatyczne służące do przetwarzania danych osobowych.

świadczenie przez Urząd podstawowych usług) – 3 dni robocze od otrzymania zgłoszenia; w sytuacji, gdy dostawca wprowadzi rozwiązanie tymczasowe, doraźnie rozwiązujące problem – usunięcie błędu nastąpi w terminie 14 dni roboczych od otrzymania formalnego zgłoszenia (pkt 6),
- przy zgłoszeniu usterki, w którym uszkodzeniu uległ jeden (lub więcej) element systemu, niewpływający na funkcjonalność i wydajność systemu, czas naprawy usterki wynosi 14 dni roboczych (pkt 7),
- w przypadku wystąpienia usterki, która powoduje nieprawidłowe działanie nieistotnych funkcji użytkowych oprogramowania komputerowego, zostanie ona usunięta w następnej wersji oprogramowania komputerowego (pkt 8).

Zgodnie z pkt 2 i pkt 3 § 2 umów dostawca przyjmuje zgłoszenia w dni robocze w godz. 8.00-16.00. W przypadku, gdy:
- formularz zgłoszenia zostanie przyjęty w godzinach 16.01-24.00 dnia roboczego – traktowany jest jak przyjęty o godz. 8.00 następnego dnia roboczego,
- formularz zgłoszenia zostanie przyjęty w godzinach 0.00-07.59 dnia roboczego – traktowany jest jak przyjęty o godz. 8.00 danego dnia roboczego.

(akta kontroli str. 335-359)

10. Oględziny strony internetowej Gminy www.koluszki.pl[13] wykazały, że informacje dla obywateli o możliwości załatwienia spraw drogą elektroniczną dostępne były w zakładce Strefa mieszkańca → e-usługi. Zamieszczono tam informacje o możliwości wnioskowania o: wydanie dowodu osobistego, wydanie odpisu aktu stanu cywilnego, zgłoszenie utraty lub uszkodzenia dowodu osobistego.
Informacje o innych usługach (w tym część on line) w zakresie m.in.: dokumentów i danych osobowych (w tym e-dowodu), edukacji, nieruchomości i środowiska, podatków, rodziny i małżeństwa, zaświadczeń i odpisów, zasiłków i pomocy finansowej, obywatel mógł uzyskać na stronie www.obywatel.gov.pl, do której link przekierowujący znajdował się Strefie mieszkańca. Zawarto tu informacje o sposobie uzyskania „nowego" dowodu osobistego z warstwą elektroniczną oraz konieczności jego posiadania w przypadku skorzystania z e-usługi.
Ponadto w zakładce „Strefa mieszkańca" podzakładce „ePUAP"[14] wskazano adres skrytki ePUAP Gminy Koluszki[15], służący do przesyłania pism w formie dokumentów elektronicznych. Ponadto, w podzakładce ePUAP informowano o:
- warunkach, niezbędnych do spełnienia by skorzystać z Elektronicznej Skrzynki Podawczej Gminy Koluszki, dostępnej na ePUAP, tj.: obowiązku założenia indywidualnego (darmowego) konta i w razie potrzeby podpisania przesłanego pisma za pomocą posiadanego tzw. profilu zaufanego lub certyfikatu kwalifikowanego,
- możliwości załatwiania spraw drogą elektroniczną poprzez elektroniczne formularze usług Gminy Koluszki lub formularz ogólny złożenia pisma do Gminy Koluszki,
- sposobie uzyskania profilu zaufanego, zakładania konta, wysyłania dokumentów i ich podpisywania (w dziale Pomoc serwisu ePUAP).

(akta kontroli str. 202-203)

Na tablicy ogłoszeń Urzędu, obywatelom udostępniono ulotkę pn. „Co to jest e-dowód", w której zawarto informacje m.in. o sprawach możliwych do załatwienia przy użyciu dowodu z warstwą elektroniczną, obejmujących:
- logowanie się do portali administracji publicznej (np. ePUAP),
- elektroniczne podpisywanie dokumentów (podpis osobisty),

---

[14] http://koluszki.pl/epuap/
[15] /umkoluszki/skrytka

– korzystanie z automatycznych bramek granicznych, np. na lotniskach.

(akta kontroli str. 204)

11. Szkolenie z zakresu zarządzania systemem informatycznym oraz przetwarzania informacji w Urzędzie Miejskim w Koluszkach dla pracowników Urzędu odbyło się w dniu 13 grudnia 2016 r. Trwało ono cztery godziny i obejmowało następujące zagadnienia:

– prawo i ważne definicje w bezpieczeństwie informacji oraz podstawowe zasady bezpieczeństwa,
– ochrona danych osobowych,
– systemy informatyczne i praca na komputerze,
– bezpieczeństwo w internecie, zagrożenia w internecie,
– zabezpieczenia elektroniczne i fizyczne,
– szyfrowanie przesyłanych informacji za pomocą środków komunikacji elektronicznej.

W szkoleniu brało udział 50 osób, co stanowiło 60% wszystkich wówczas zatrudnionych pracowników Urzędu.

Szkolenie to, jak wyjaśniła Sekretarz Gminy (z up. Burmistrza), miało charakter szkolenia ogólnego z zakresu bezpieczeństwa przetwarzania informacji w systemach informatycznych i było prowadzone przez Informatyka Urzędu.

(akta kontroli str. 165-169, 178-183)

W okresie od 1 lipca 2018 r. do 30 czerwca 2020 r. Informatyk przeszedł trzy szkolenia z zakresu: świadczenia usług zapewniających w obszarze ochrony danych osobowych; roli audytu wewnętrznego w ocenie spełniania wymogów KRI i RODO; cyberbezpieczeństwa, KRI i RODO.

(akta kontroli str. 533-542)

Przed przystąpieniem do użytkowania systemów komputerowych i sieci teleinformatycznej nowi pracownicy Urzędu byli zapoznawani z zagadnieniami związanymi z bezpieczeństwem przetwarzania informacji. Odbycie szkolenia potwierdzał pracownik Urzędu.

(akta kontroli str. 170-175, 178-183)

12. W Urzędzie nie było opracowanej i wdrożonej polityki bezpieczeństwa informacji, o której mowa w § 20 ust. 1 w związku z ust. 3 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[16]. Obowiązująca w Urzędzie polityka bezpieczeństwa dotyczyła bezpieczeństwa przetwarzania danych osobowych i ustanowiona została na podstawie przepisów RODO.

Oświadczenie o zapoznaniu się z polityką bezpieczeństwa przetwarzania danych osobowych zostało potwierdzone przez pracowników w dniu 1 kwietnia 2019 r. Za ocenę, przegląd i modyfikację procedur związanych z Polityką bezpieczeństwa przetwarzania danych osobowych odpowiadał Inspektor Danych Osobowych.

(akta kontroli str. 69-146, 178-183)

Poza Polityką bezpieczeństwa przetwarzania danych osobowych, w okresie objętym kontrolą w Urzędzie funkcjonowała „Polityka kluczy w Urzędzie Miejskim w Koluszkach"[17]. Oświadczenie o zapoznaniu się z polityką kluczy zostało potwierdzone przez pracowników w dniu 1 kwietnia 2019 r. Polityka kluczy nie określała dokumentów wykonawczych.

---

[16] Dz. U. z 2017 r. poz. 2247, zw. dalej KRI.

[17] Polityka kluczy wdrożona zarządzeniem nr 44/2019 Burmistrza Koluszek z dnia 12 marca 2019 r. oraz zarządzeniem nr 15/2020 Burmistrza Koluszek z dnia 29 stycznia 2020 r.

Poza ww., w Urzędzie nie opracowano innych polityk, regulaminów i procedur w zakresie bezpieczeństwa informacji, które stanowiłyby SZBI.

(akta kontroli str. 156-164, 178-183)

13. Obowiązująca we wcześniejszym okresie w Urzędzie Polityka z 2016 r. została ustanowiona wyłącznie na podstawie ustawy o ochronie danych osobowych i dotyczyła tylko przetwarzania danych osobowych.

W 2019 r. Urząd dokonał jej aktualizacji z uwagi m.in. na potrzebę uzupełnienia dokumentacji dotyczących ochrony danych osobowych o niezbędne klauzule informacyjne oraz zgody, na podstawie wyników raportu z częściowego audytu ochrony danych osobowych w zakresie zgodności z rozporządzeniem RODO.

Polityka z 2016 r. nie określała dokumentów wykonawczych.

(akta kontroli str. 6-65, 205-248)

Najwyższa Izba Kontroli zwraca uwagę, że szkolenie w zakresie ochrony danych osobowych w Urzędzie, w tym w zakresie trybu postępowania przy przetwarzaniu tych danych dla pracowników Urzędu, odbyło się w dniu 13 grudnia 2016 r., tj. po blisko 10 miesiącach od wdrożenia Polityki z 2016 r.(29 lutego 2016 r.).

Sekretarz Gminy (z up. Burmistrza) wyjaśniła, że zmiany miały charakter kosmetyczny i polegały na uzupełnieniu Polityki m.in. o definicję bezpieczeństwa informacji, jego ogólnych celów i zakresu oraz znaczenia bezpieczeństwa, jako mechanizmu umożliwiającego współużytkowanie informacji. Zmiany te nie miały wpływu na procedury zawarte we wcześniejszym dokumencie polityki bezpieczeństwa.

(akta kontroli str. 6-68, 205-212)

14. Obowiązujące w Urzędzie zasady przetwarzania danych osobowych zawierały m.in.

- procedury rozpoczęcia, zawieszenia i zakończenia pracy przez użytkowników systemu; procedury tworzenia kopii zapasowych zbiorów danych oraz programów i narzędzi programów służących do przetwarzania (Polityka z 2016 r.);
- procedury analizy ryzyka i oceny skutków dla ochrony danych osobowych; procedury współpracy z podmiotami zewnętrznymi; procedury odbierania zgód oraz informowania osób; procedury nadawania, modyfikacji i odbierania uprawnień do przetwarzania danych osobowych w systemach informatycznych (Polityka bezpieczeństwa przetwarzania danych osobowych).

Ponadto, zgodnie z założeniami Polityki bezpieczeństwa przetwarzania danych osobowych, w Urzędzie opracowany został regulamin ochrony danych osobowych[18], zawierający m.in. zasady ochrony tych danych oraz skróconą instrukcję postępowania w przypadku naruszenia ochrony danych osobowych.

(akta kontroli str. 69-134, 147-155, 178-183)

15. Według stanu na dzień 14 lipca 2020 r. inwentaryzacja sprzętu informatycznego prowadzona była w Urzędzie w wersji papierowej i elektronicznej. Oględziny systemu informatycznego w zakresie zasobów informatycznych Urzędu wykazały, że system ten zawierał informacje o urządzeniach komputerowych i ich oprogramowaniu. Baza zawierała 132 rekordy urządzeń, w tym komputerów stacjonarnych, laptopów, drukarek, urządzenia peryferyjnego – plotera, urządzeń sieciowych, oprogramowania. W bazie zawarto m.in. informacje o adresie IP, zasobach sprzętowych danego komputera, producentach karty, o usługach, które są aktywne i uruchomione na danym komputerze, o stanie włączenia/wyłączenia

[18] Zarządzenie nr 43/3029 Burmistrza Koluszek z dnia 12 marca 2019 r. w sprawie wdrożenia Regulaminu „Zasady ochrony danych osobowych w Urzędzie Miejskim w Koluszkach", zmieniony zarządzeniem nr 16/2020 Burmistrza Koluszek z dnia 29 stycznia 2020 r. w sprawie wdrożenia Regulaminu „Zasady ochrony danych osobowych w Urzędzie Miejskim w Koluszkach".

sprzętu. Zewidencjonowane były również komputery, które pracownik posiadał wcześniej.

Analiza w zakresie inwentaryzacji wybranego sprzętu informatycznego (15 urządzeń)[19] wykazała, że posiadane zasoby informatyczne przypisane były do poszczególnych pracowników bądź do poszczególnych referatów Urzędu. Każdy pracownik (bądź referat) miał nadany swój kod numeryczny (np. K107) oraz utworzoną własną bazę o zasobach informatycznych. Rekordy tej bazy zawierały informacje m.in. o rodzaju sprzętu, jego wydajności, oprogramowaniu, zasobach, plikach, czy podłączonych urządzeniach. Jednakże w 13 przypadkach[20] (na 15 analizowanych) w elektronicznej ewidencji nie odnotowano numerów inwentarzowych poszczególnych sprzętów, co wynikało – jak wyjaśniła Sekretarz Gminy (z up. Burmistrza) – z faktu modernizowania i udoskonalania zasobów sprzętowych i programowych. Numer inwentarzowy zapisany był w wersji papierowej.

(akta kontroli str. 360-392, 533-542)

16. Oględziny 10 komputerów pracowników Urzędu, niebędących pracownikami służb informatycznych, w zakresie możliwości samodzielnej instalacji nieautoryzowanego przez Urząd oprogramowania wykazały, że nie było możliwości zainstalowania takiego oprogramowania – po próbie zainstalowania oprogramowania pojawiał się komunikat: „*Zgodnie z polityką bezpieczeństwa Urzędu Miejskiego w Koluszkach, pobranie pliku typu exe zostało zablokowane*". Pracownicy nie posiadali uprawnień administracyjnych (za wyjątkiem Z-cy Burmistrza). W trakcie oględzin każdy pracownik zalogowany był na swoim koncie.

(akta kontroli str. 395-397)

17. W latach 2016-2020 (do 30 czerwca) 20 osób zakończyło zatrudnienie w Urzędzie. Analiza dokumentacji 15 byłych pracowników Urzędu wykazała, że:

- dla 13 ówczesnych pracowników wystawione były wnioski bezpośrednich przełożonych o odebranie uprawnień w systemie informatycznym,
- w dwóch przypadkach wnioski były wystawione dzień przed ustaniem stosunku pracy z pracownikiem oraz w tym samym dniu.

Ponadto,

- dla dwóch użytkowników, którzy zakończyli zatrudnienie w 2018 r. i w 2019 r. bezpośredni przełożeni nie wystąpili do ASI z wnioskami o odebranie uprawnień do systemu informatycznego,
- pięć wniosków wystawionych było w dniu następnym po ukończeniu zatrudnienia,
- cztery wnioski wystawione były w terminach od 2 dni do ponad 1 miesiąca od dnia ustania zatrudnienia,

co zostało szczegółowo opisane w sekcji „Stwierdzone nieprawidłowości".

(akta kontroli str. 6-40, 69-134, 185-201)

Oględziny systemu serwerowego Windows usługa Active Directory Użytkownicy i Komputery wykazały, że w przypadku 14 byłych pracowników ich nazwiska znajdowały się w folderze: pracownicy UM – nieaktywni, a ich konta w systemie informatycznym były zablokowane. System ten nie informował natomiast, kiedy (w jakiej dacie) zablokowano w systemie konto pracownika, który zakończył zatrudnienie. Wskazywał jedynie, czy konto jest aktywne, czy nie.

---

[19] Sprzęt wybrany na podstawie doboru celowego, tj. 10 komputerów, jeden serwer, dwa laptopy, router i jedna drukarka.

[20] Jedna drukarka, dwa laptopy, dziewięć komputerów stacjonarnych, SERWER.

Konto jednej osoby zostało usunięte z systemu informatycznego, z uwagi na – jak wyjaśniła Sekretarz Gminy (z up. Burmistrza) – migrację, reorganizację i testowanie systemu.

(akta kontroli str. 184, 533-542)

18. W 2017 r. i w 2019 r. przez audytora wewnętrznego zostały przeprowadzone audyty wewnętrzne z zakresu bezpieczeństwa informacji, zgodnie z planem audytu wewnętrznego na 2017 r. i 2019 r.
Ogólna ocena adekwatności, skuteczności i efektywności kontroli zarządczej w obszarze działalności jednostki objętym zadaniem została wydana jako ocena pozytywna z zastrzeżeniami. Ponadto, w sprawozdaniu z audytu wewnętrznego za 2017 r. audytor wskazał: „(...) W audytowanym procesie zidentyfikowano istotne słabości, jednakże proces ma miejsce, ale wymaga dużych usprawnień".

W związku z uzyskanymi rezultatami badań, audytor wydał po 8 zaleceń w sprawie wyeliminowania słabości kontroli zarządczej lub wprowadzenia usprawnień. Według stanu na dzień 9 lipca 2020 r. w Urzędzie zrealizowano część rekomendacji poaudytowych, jak również podjęto działania w celu wyeliminowania istotnych słabości i ich realizacji. Nie zrealizowano natomiast wniosku polegającego na przeprowadzeniu szkoleń dla kierowników referatów w zakresie ich obowiązków polegających na zgłaszaniu odchodzących z pracy pracowników Urzędu.

Sekretarz Gminy (z up. Burmistrza) wyjaśniła, że *„nie widzieliśmy potrzeby przeprowadzania szkoleń w tym zakresie"*.

W 2016 r. i w 2018 r. w Urzędzie nie został przeprowadzony audyt wewnętrzny w zakresie bezpieczeństwa informacji, co zostało opisane w sekcji „Stwierdzone nieprawidłowości".

(akta kontroli str. 250-334, 561-568)

Stwierdzone nieprawidłowości

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

1. Według § 2 załącznika nr 1 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[21], czynności kancelaryjne są wykonywane w systemie tradycyjnym lub w systemie EZD, a przepis zawarty w § 3 zobowiązuje kierownika podmiotu do wskazania, który z systemów wykonywania czynności kancelaryjnej jest podstawowym sposobem dokumentowania przebiegu i rozstrzygania spraw dla danego podmiotu.

   W latach 2016-2020 (do 20 lipca) Burmistrz formalnie nie określił, jaki z systemów wykonywania czynności kancelaryjnych w Urzędzie jest podstawowym sposobem dokumentowania przebiegu i rozstrzygania spraw.

   Sekretarz Gminy wyjaśniła, że nie został opracowany wewnętrzny dokument, formalnie określający szczegółowe zasady i tryb wykonywania czynności kancelaryjnych w Urzędzie, z uwagi na przeoczenie i nieprzeanalizowanie treści rozporządzenia po objęciu przez nią stanowiska Sekretarza Gminy.

   W trakcie kontroli nieprawidłowość ta została usunięta poprzez dokonanie w dniu 21 lipca 2020 r. odpowiednich zmian w regulaminie organizacyjnym Urzędu, w którym wskazany został tradycyjny system kancelaryjny, jako podstawowy sposób dokumentowania przebiegu załatwiania i rozstrzygania

[21] Dz. U. z 2011 r. Nr 14, poz. 67, zw. dalej rozporządzeniem w sprawie instrukcji kancelaryjnej.

spraw, przy wykorzystaniu narzędzi informatycznych do rejestracji korespondencji przychodzącej.

(akta kontroli str. 393-394, 533-553)

2. W Urzędzie, nierzetelnie i z naruszeniem §§ 39, 40, 48, 49 rozporządzenia w sprawie instrukcji kancelaryjnej, podejmowano zadania dotyczące realizacji usług elektronicznych wpływających od obywateli poprzez platformę ePUAP.

   Spośród objętych analizą 20 spraw w zakresie realizowania usług elektronicznych wpływających poprzez ePUAP:

   - w czterech sprawach pisma/wnioski obywateli zostały zarejestrowane w dniu następnym, pomimo wpływu na platformę ePUAP w godzinach pracy Urzędu[22],
   - w sześciu sprawach brak było daty rejestracji w Urzędzie oraz dekretacji na komórkę organizacyjną Urzędu bądź stanowisko/pracownika merytorycznego[23],
   - w siedmiu sprawach dekretacja na stanowisko/pracownika merytorycznego nie była dokonywana niezwłocznie: od momentu wpływu wniosku/pisma na platformę ePUAP bądź rejestracji sprawy przez Urząd do dekretacji tych wniosków/pism na stanowisko merytoryczne upłynęło od 2 do 4 dni roboczych[24],
   - w jednej sprawie[25] warunkiem jej załatwienia było dostarczenie przez obywatela numerów ewidencyjnych nieruchomości[26], niezbędnych do uzyskania wypisu i wyrysu z miejscowego planu zagospodarowania przestrzennego – pracownik merytoryczny obsługujący sprawę nie komunikował się z inną jednostką administracji publicznej za pośrednictwem platformy ePUAP w celu uzyskania tych informacji, co było niezgodne z art. 220 § 1 Kpa[27],
   - załatwienie dwóch spraw (w tym w jednostce organizacyjnej Urzędu)[28] nastąpiło w terminach wynoszących 47 dni i 122 dni od daty wpływu kompletnego wniosku/pisma na platformę ePUAP. W jednym przypadku (GP.6727.164.2020) sprawa została załatwiona dopiero po skierowaniu przez wnioskodawcę do Urzędu ponaglenia w trybie art. 35 Kpa w celu niezwłocznego jej zrealizowania,
   - w aktach pięciu spraw[29] brak było pisemnego potwierdzenia działań pracownika merytorycznego w zakresie załatwianej sprawy, przez co niemożliwa była bieżąca i obiektywna informacja na temat okoliczności, terminowości i efektów realizacji tych spraw.

   (akta kontroli str. 403-411, 414-532)

   Sekretarz Gminy (z up. Burmistrza) wyjaśniła, że wydruk spraw wpływających następuje co do zasady raz dziennie, więc można przyjąć, że rejestracja wpływających przez ePUAP spraw nastąpiła niezwłocznie. Stwierdzone przypadki braku rejestracji i dekretacji spowodowane był potrzebą szybkiego przekazania pisma na stanowisko merytoryczne. Dostarczanie informacji przez obywatela nie jest czynnością w znaczny sposób absorbującą wnioskodawcę

[22] Sprawa L.dz. 00717, EDŚ.4424.29.2020, L.dz. 10886, GG.6840.1.5.2020.
[23] Sprawa Diany B., Anny K., Karoliny K., Marty O., L.dz. 00717, L.dz. 06301.
[24] GG.6831.3.2020, GP.6727.96.2020, GP.6727.164.2020, GII.713.368.2020.MF, L.dz. 00717, L.dz. 10886, GG.6840.1.5.2020.
[25] GP.677.96.2020.
[26] Obywatel we wniosku podał dokładny adres nieruchomości.
[27] Ustawa z dnia 14 czerwca 1960 r. Kodeks postępowania administracyjnego (zw. dalej Kpa); Dz. U. z 2020 r. poz. 256.
[28] GP.6727.164.2020 – data wpływu do Urzędu – 10 czerwca 2020 r., i EDŚ.4424.29.2020 – data wpływu – 26 lutego 2020 r.
[29] GP.6727.96.2020, USC.5362.116.2020, USC.5362.259.2020, L.dz. 08252, GG.6840.1.5.2020.

i taki sposób pozyskania informacji bezpośrednio od wnioskodawcy będzie najszybszy. Długi termin załatwiania spraw wynika z art. 15 zzs ust. 1 ustawy z dnia 2 marca 2020 r. o szczególnych rozwiązaniach związanych z zapobieganiem, przeciwdziałaniem i zwalczaniem COVID-19 (...) – bieg terminów procesowych i sądowych nie rozpoczyna się, a rozpoczęty ulega zawieszeniu na ten okres. Przepis ten został uchylony z dniem 16 maja, co oznacza, że bieg terminów procesowych rozpoczął się dopiero z dniem 23 maja 2020 r.

(akta kontroli str. 560-568, 570)

Powyższe miało miejsce w sytuacji, gdy w Urzędzie nie opracowano oraz nie wdrożono wewnętrznych procedur/zasad dotyczących elektronicznego obiegu dokumentów, regulujących komunikację elektroniczną z obywatelami i załatwiania spraw w formie elektronicznej oraz zarządzania tymi dokumentami, pomimo że taka komunikacja funkcjonowała. Nie opracowano również zasad postępowania z przesyłkami wpływającymi na Elektroniczną Skrzynkę Podawczą, w tym zasad zobowiązujących pracowników do weryfikacji opatrzenia wpływających do Urzędu dokumentów elektronicznych aktualnym podpisem elektronicznym, pomimo że taka skrzynka w Urzędzie funkcjonowała.

Sekretarz Gminy (z up. Burmistrza) wyjaśniła, że korespondencja wpływająca do Urzędu na Elektroniczną Skrzynkę Podawczą jest traktowana tak samo, jak pozostała korespondencja i podlega takiemu samemu obiegowi. W Urzędzie obowiązuje rozporządzenie Prezesa Rady Ministrów z dnia 18 stycznia 2011 r. w sprawie instrukcji kancelaryjnej, jednolitych rzeczowych wykazów akt (...).

(akta kontroli str. 178-183, 205-212)

Zdaniem NIK, pracownicy merytoryczni realizujący analizowane sprawy nie wykonywali swoich obowiązków z należytą starannością. Stwierdzona w wyniku kontroli dowolność dokumentowania przebiegu wpływających spraw, przebiegającego w sposób sprzeczny z postanowieniami rozporządzenia w sprawie instrukcji kancelaryjnej, zwłaszcza w sytuacji braku uregulowań wewnętrznych ściśle określających procedury elektronicznego obiegu dokumentów i załatwiania spraw wpływających poprzez platformę ePUAP utrudniała monitorowanie biegu sprawy i uniemożliwiała dokonanie oceny terminowości ich załatwiania. Należy szczególnie podkreślić, że wyżej wskazane nieprawidłowości były przede wszystkim skutkiem braku procedur/zasad postępowania z dokumentami wpływającymi drogą elektroniczną.

3. Zamieszczone na stronie internetowej Urzędu[30] informacje o możliwości załatwienia spraw drogą elektroniczną były niekompletne, a zamieszczone tam odnośniki nie działały prawidłowo.

   Nieprawidłowe działanie dotyczyło: linku w zakładce Strefa mieszkańca podzakładce e-usługi odnoszącego się do złożenia drogą elektroniczną wniosku o wydanie dowodu osobistego: (klikając „załatw sprawę" pojawiał się komunikat: „podana usługa nie istnieje"[31]), a w podzakładce ePUAP[32] brak było możliwości wejścia do systemu elektronicznej skrzynki podawczej (po kliknięciu linku: Wejście do systemu elektronicznej skrzynki podawczej pojawiał się komunikat „Błąd Nieprawidłowe żądanie http").

---

[30] www.koluszki.pl.

[31] https://epuap.gov.pl/wps/portal/strefa-klienta/katalog-spraw/najnowsze-uslugi/najnowsze-uslugi-centralne-2/wnioskowanie-o-wydanie-dowodu-osobistego-2.

[32] http://koluszki.pl/epuap/.

Ponadto w podzakładce ePUAP nie zostały zawarte informacje o sposobie uzyskania „nowego" dowodu osobistego z warstwą elektroniczną, jak również nie zamieszczono informacji, że w celu skorzystania z e-usługi konieczne jest posiadanie „nowego" dowodu osobistego z warstwą elektroniczną.

Sekretarz Gminy (z up. Burmistrza) wyjaśniła, że przyczynami niedogodności były prawdopodobnie: zmiany lokalizacji na platformie ePUAP i w efekcie zmiana adresu podpiętego pod odpowiedni przycisk przekierowujący; błędne zlinkowanie napisu podczas przenoszenia strony na nowy serwer hostingujący w 2019 r.

Nieprawidłowości te zostały usunięte podczas kontroli NIK.

(akta kontroli str. 202-203, 205-212)

4. Burmistrz, z naruszeniem zasad legalności podejmował działania związane z zarządzaniem bezpieczeństwem informacji.

   a. Zgodnie z § 20 ust. 2 pkt 1 rozporządzenia KRI 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.

      W latach objętych kontrolą Burmistrz nie opracował i nie wdrożył SZBI, a w szczególności Polityki Bezpieczeństwa Informacji. W Urzędzie system zarządzania bezpieczeństwem informacji został ustanowiony bowiem wyłącznie w zakresie zasad pobierania kluczy do pomieszczeń służbowych oraz w zakresie przetwarzania danych osobowych – na podstawie ustawy o ochronie danych osobowych. Dokumenty te nie regulowały jednak całościowych procedur związanych z bezpieczeństwem informacji.

      Sekretarz Gminy (z up. Burmistrza) wyjaśniła, że pełny system zarządzania bezpieczeństwem informacji nie był i nie jest wymagany, nie jest to system obligatoryjny.

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

      Najwyższa Izba Kontroli zauważa, że w Urzędzie nie został wdrożony SZBI na podstawie Polskiej Normy PN-ISO/IEC 27001. Również ustanowienie zabezpieczeń, zarządzanie ryzykiem oraz audytowanie nie odbywało się na podstawie Polskich Norm związanych z tą normą[33].

      (akta kontroli str. 6-40, 69-134, 178-183, 561-568)

[33] 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.

b. Zgodnie z § 20 ust. 2 pkt 5 rozporządzenia KRI, kierownictwo podmiotu publicznego zapewnia warunki umożliwiające realizację i egzekwowanie m.in. bezzwłocznej zmiany uprawnień, w przypadku zmiany zadań osób, o których mowa w pkt 4.
Ponadto, zgodnie z obowiązującą w Urzędzie Polityką bezpieczeństwa przetwarzania danych osobowych w przypadku ustania stosunku pracy, wniosek odbierający wszystkie uprawnienia powinien być wystawiony natychmiast, najpóźniej ostatniego dnia pracy zatrudnionego (§ 76).
Analiza wniosków o odebranie uprawnień do systemu informatycznego 15 byłych pracowników wykazała, że:
- dla dwóch użytkowników, z którymi zakończono zatrudnienie w 2018 r. i w 2019 r. bezpośredni przełożeni nie wystąpili z przedmiotowym wnioskiem do ASI,
- w dziewięciu przypadkach wnioski zostały wystawione z opóźnieniem, z czego cztery – w terminach od 2 dni do ponad 1 miesiąca od daty ustania zatrudnienia, a pięć – w dniu następnym po ukończeniu zatrudnienia co stanowiło również naruszenie § 76 Polityki bezpieczeństwa przetwarzania danych osobowych,
- sześć wniosków nie posiadało akceptacji Inspektora Ochrony Danych, a w jednym przypadku brak było podpisu osoby wnioskującej, do czego zobowiązywały postanowienia funkcjonujących w Urzędzie polityk ochrony danych osobowych (§§ 8-11 Polityki z 2016 r. oraz § 76 pkt 2a Polityki bezpieczeństwa przetwarzania danych osobowych),
- sześć wniosków było wypełnionych na innym formularzu, niż ten obowiązujący w Urzędzie – wskazany w załączniku F do Polityki z 2016 r. i w załączniku nr 9 do Polityki bezpieczeństwa przetwarzania danych osobowych.

(akta kontroli str. 6-40, 69-134, 185-201, 554-559)

Sekretarz Gminy (z up. Burmistrza) wyjaśniła, że brakujące w aktach danej sprawy wnioski prawdopodobnie się zgubiły, a brak akceptacji Inspektora Ochrony Danych Osobowych wynikał z faktu zatrudnienia firmy zewnętrznej z siedzibą poza Koluszkami, którego wizyty w Urzędzie miały miejsce ok. 2 razy w miesiącu. Wyjaśniła ponadto, że wzór formularza odbierającego uprawnienia załączony do polityki bezpieczeństwa przetwarzania danych osobowych jest nieaktualny, ponieważ Administrator Bezpieczeństwa Informacji nie funkcjonuje od dłuższego czasu.

Najwyższa Izba Kontroli zauważa, że na brak kierowania przez bezpośrednich przełożonych do ASI wniosków o odebranie uprawnień do systemu informatycznego dla osób kończących zatrudnienie w Urzędzie zwrócił uwagę audytor wewnętrzny, realizując zadanie audytowe w 2017 r. W sprawozdaniu z audytu wewnętrznego napisał: „*Niezgłaszanie przez kierowników referatów nowych i odchodzących z pracy pracowników uniemożliwia w odpowiednim czasie nadanie lub cofnięcie wszelkich uprawnień dostępowych i wydanie lub cofnięcie odpowiednich upoważnień*". Na tej podstawie sformułował zalecenie przeprowadzenia w 2018 r. szkolenia dla Lokalnych Administratorów Bezpieczeństwa Informacji w zakresie zgłaszania do Administratora Bezpieczeństwa Informacji nowych i odchodzących z pracy pracowników.
Należy szczególnie podkreślić, że zalecenie to nie zostało zrealizowane, gdyż – jak wyjaśniła Sekretarz Gminy (z up. Burmistrza) – „*nie widzieliśmy potrzeby przeprowadzania szkoleń w tym zakresie*".

(akta kontroli str. 281-307, 533-542, 561-568)

a. Zgodnie z § 20 ust. 2 pkt 14 rozporządzenia KRI, kierownictwo podmiotu publicznego zapewnia warunki umożliwiające realizację i egzekwowanie m.in. okresowego audytu wewnętrznego w zakresie bezpieczeństwa informacji, nie rzadziej niż raz na rok.

W 2016 r. i w 2018 r. w Urzędzie nie został przeprowadzony audyt wewnętrzny w zakresie bezpieczeństwa informacji.

Sekretarz Gminy (z up. Burmistrza) wyjaśniła, że brak audytu w 2016 r i w 2018 r. wynikał z faktu pilnej potrzeby przeprowadzenia audytu bezpieczeństwa informacji w jednostkach organizacyjnych Urzędu.

(akta kontroli str. 250-251, 533-542)

Ponadto Zgodnie z § 19 ust. 2 § 19 ust. 2 rozporządzenia Ministra Finansów z dnia 4 września 2015 r. w sprawie audytu wewnętrznego oraz informacji o pracy i wynikach tego audytu[34], w terminie 14 dni kalendarzowych od dnia otrzymania sprawozdania audytowany ustala sposób i termin realizacji oraz wyznacza osoby odpowiedzialne za realizację zaleceń, powiadamiając o tym na piśmie kierownika komórki audytu wewnętrznego i kierownika jednostki.

Sekretarz Gminy w ciągu 14 dni od otrzymania sprawozdania z audytu, nie poinformowała audytora wewnętrznego o sposobie i terminie realizacji zaleceń audytu przeprowadzonego w 2017 r., gdyż – jak wyjaśniła – zapomniała o tym fakcie i nie dokonała formalności.

(akta kontroli str. 250-251, 281-307, 393-394)

b. Zgodnie z § 20 ust. 2 pkt 6 rozporządzenia KRI, kierownictwo podmiotu publicznego zapewnia warunki umożliwiające realizację i egzekwowanie m.in. szkolenia osób zaangażowanych w proces przetwarzania informacji, z uwzględnieniem zagrożenia jej bezpieczeństwa, skutków naruszenia zasad bezpieczeństwa, konsekwencji prawnych i środków zapewniających jej bezpieczeństwo.
W latach 2018-2020 (do 30 czerwca) dla pracowników Urzędu obsługujących lub realizujących e-usługi nie były przeprowadzane szkolenia w zakresie bezpieczeństwa informacji.

Sekretarz Gminy (z up. Burmistrza) wyjaśniła, że do celów szybkiego informowania pracowników o mogących wystąpić zagrożeniach wykorzystywany jest w Urzędzie wewnętrzny komunikator tekstowy, działający w sieci komputerowej Urzędu. Ponadto podała, że w Urzędzie funkcjonuje tzw. Baza wiedzy, czyli udostępniony zasób sieciowy, w którym publikowane są materiały związane z tematyką bezpieczeństwa w sieciach informatycznych oraz informacje o zagrożeniach, jakie występują w trakcie korzystania ze sprzętu komputerowego i sieci Internet.

(akta kontroli str. 178-183, 205-212)

c. Zgodnie z § 20 ust. 2 pkt 2 rozporządzenia KRI, zarządzanie infrastrukturą informatyczną wymaga utrzymywania w urzędzie aktualności inwentaryzacji sprzętu i oprogramowania służącego do przetwarzania informacji obejmującej ich rodzaj i konfigurację.
Oględziny systemu informatycznego w zakresie zasobów informatycznych Urzędu wykazały, że dane o sprzęcie informatycznym jednego pracownika nie były na bieżąco aktualizowane, tj. w systemie informatycznym użytkownik nie miał przypisanego komputera, na którym aktualnie pracował.
Sekretarz Gminy (z up. Burmistrza) wyjaśniła, że użytkownikowi w dniu 25 czerwca 2020 r. został wymieniony sprzęt z komputera stacjonarnego na

[34] Dz. U. z 2018 r. poz. 506.

laptopa. W takiej sytuacji laptop ma zainstalowanego „agenta" programu Axecce nVision w wersji zewnętrznej i jest przypisany do zewnętrznego adresu IP innego niż sieć wewnętrzna.

(akta kontroli str. 360-382, 533-542)

IV. Uwagi i wnioski

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 pokontrolne

1. rozważyć – celem jednolitego postępowania z przesyłkami wpływającymi do Urzędu drogą elektroniczną – wdrożenie wewnętrznych procedur/zasad dotyczących elektronicznego obiegu dokumentów oraz zasad postępowania z przesyłkami wpływającymi na elektroniczną skrzynkę podawczą;
2. egzekwować od pracowników Urzędu niezwłocznej rejestracji przesyłek wpływających do Urzędu poprzez platformę ePUAP oraz dekretacji ich na właściwe stanowiska merytoryczne;
3. terminowo realizować sprawy wpływające od obywateli poprzez platformę ePUAP, w tym bez żądania od obywateli danych/informacji będących już w posiadaniu innej komórki organizacyjnej lub innego urzędu administracji publicznej;
4. opracować i wdrożyć system zarządzania bezpieczeństwem informacji, zgodnie z § 20 ust. 1, w zw. z ust. 3 rozporządzenia KRI;
5. niezwłocznie dokonywać zmiany uprawnień do systemów informatycznych pracownikom, którzy zakończyli zatrudnienie w Urzędzie;
6. zapewnić okresowe szkolenia dla pracowników Urzędu w zakresie bezpieczeństwa informacji;
7. zapewnić rzetelność informacji o wykorzystywanych zasobach informatycznych, obejmujących ich rodzaj i konfigurację, stosownie do wymogów § 20 ust. 2 pkt 2 rozporządzenia KRI;
8. zapewnić okresowy audyt wewnętrzny w zakresie bezpieczeństwa informacji, o którym mowa w § 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 w Łodzi. Prawo zgłaszania zastrzeżeń, zgodnie z art. 61b ust. 2 ustawy o NIK, nie przysługuje do wystąpienia pokontrolnego zmienionego zgodnie z treścią uchwały w sprawie zastrzeżeń.

Obowiązek poinformowania NIK o sposobie wykorzystania uwag i wykonania wniosków

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

Łódź, 29 września 2020 r.

Kontroler
Katarzyna Kaczkowska
Doradca techniczny

podpis

Najwyższa Izba Kontroli
Delegatura w Łodzi
Dyrektor
Przemysław Szewczyk

podpis