NAJWYŻSZA IZBA KONTROLI
Delegatura w Katowicach

LKA.410.013.03.2020

Pan
Marian Błachut
Burmistrz Miasta i Gminy Czechowice-Dziedzice
Plac Jana Pawła II 1
43-502 Czechowice-Dziedzice

WYSTĄPIENIE POKONTROLNE

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

NAJWYŻSZA IZBA KONTROLI
Delegatura w Katowicach
ul. Powstańców 29, 40-039 Katowice
T +48 32 784 42 00, F +48 32 784 42 30
lka@nik.gov.pl

I. Dane identyfikacyjne

Jednostka kontrolowana	Urząd Miejski w Czechowicach-Dziedzicach[1], Plac Jana Pawła II 1, 43-502 Czechowice-Dziedzice
Kierownik jednostki kontrolowanej	Marian Błachut, Burmistrz Miasta i Gminy Czechowice-Dziedzice[2] od 26 listopada 2006 r. (akta kontroli str. 2-5)
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 dnia zakończenia czynności kontrolnych[3]
Podstawa prawna podjęcia kontroli	Art. 2 ust. 2 ustawy z dnia 23 grudnia 1994 r. o Najwyższej Izbie Kontroli[4]
Jednostka przeprowadzająca kontrolę	Najwyższa Izba Kontroli Delegatura w Katowicach
Kontroler	Magdalena Śleziak, inspektor kontroli państwowej, upoważnienie do kontroli nr LKA/147/2020 z 15 czerwca 2020 r. oraz LKA/221/2020 z 24 sierpnia 2020 r. (akta kontroli str. 1-1a)

[1] Dalej: „Urząd".
[2] Dalej: „Burmistrz".
[3] Tj. do 4 września 2020 r.
[4] Dz. U. z 2020 r. poz. 1200; dalej: „ustawa o NIK".

II. Ocena ogólna[5] kontrolowanej działalności

OCENA OGÓLNA

W okresie objętym kontrolą w Urzędzie prawidłowo świadczono usługi publiczne w formie elektronicznej z wykorzystaniem platformy ePUAP.

Sprawy w formie elektronicznej zgłaszane przez obywateli były obsługiwane przez elektroniczną skrzynkę podawczą[6]. W sposób zrozumiały i łatwy do identyfikacji informowano interesantów na stronie internetowej o sposobie załatwiania spraw drogą elektroniczną, w tym o możliwości składania pism przez ESP. W Urzędzie udostępniono łącznie 75 usług elektronicznych, a wpływające sprawy, rozpatrywane w tradycyjnej formie (papierowej – wspomaganej programem elektronicznego zarządzania dokumentacją), realizowane były bez zwłoki, w formie zgodnej z wnioskami obywateli, z wykorzystaniem posiadanych informacji i danych zgromadzonych w rejestrach publicznych.

Pracownicy Urzędu uczestniczyli w szkoleniach związanych z bezpieczeństwem informacji. Odpowiednio zapobiegano instalacji nieautoryzowanego oprogramowania na sprzęcie informatycznym.

Stwierdzono jednak nieprawidłowości polegające na naruszeniu przepisów *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*[7], w szczególności:

– nie opracowano i nie wdrożono systemu zarządzania bezpieczeństwem informacji (SZBI), w szczególności polityki bezpieczeństwa informacji (PBI), wymaganego przepisem § 20 ust. 1 *rozporządzenia KRI*,

– w latach 2016-2019 (do grudnia) nie przeprowadzono audytu w zakresie bezpieczeństwa informacji wymaganego § 20 ust. 2 pkt 14 *rozporządzenia KRI*,

– nie prowadzono inwentaryzacji zasobów informatycznych zgodnie z wymaganiami § 20 ust. 2 pkt 2 *rozporządzenia KRI*, w zakresie obejmującym ich rodzaj oraz konfigurację,

– nie przeprowadzono całościowych, okresowych analiz ryzyka utraty integralności, dostępności lub poufności informacji, co było niezgodne § 20 ust. 2 pkt 3 *rozporządzenia KRI*,

– ze zwłoką (wynoszącą nawet 212 dni) blokowano lub usuwano dane kont dostępu do systemów informatycznych byłym pracownikom Urzędu, co było niezgodne z § 20 ust. 2 pkt 5 *rozporządzenia KRI*.

III. Opis ustalonego stanu faktycznego

Opis stanu faktycznego

1. W obowiązującej w okresie objętym kontrolą *Strategii rozwoju Gminy Czechowice-Dziedzice 2020+*[8] nie uwzględniono zagadnień dotyczących dostosowania Urzędu do elektronicznego świadczenia usług publicznych. W części Strategii dotyczącej *Misji i wizji* wskazano jedynie, że: *Mieszkańcy chętnie stosują współczesne technologie komunikacyjne do korzystania z szerokiego zakresu udostępnianych przez administrację i sektor gospodarczy e-usług*.

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

[6] Dalej: „ESP".

[7] Dz. U. z 2017 r. poz. 2247; dalej: „rozporządzenie KRI".

[8] Dalej: „Strategia". Strategia została przyjęta Uchwałą Nr XIII/105/15 Rady Miejskiej w Czechowicach-Dziedzicach w dniu 29 września 2015 r. W Strategii założono horyzont planistyczny obejmujący okres programowania Unii Europejskiej przypadający na lata 2014-2020.

(akta kontroli str. 6-19)

Burmistrz wyjaśnił: „*Program informatyzacji i rozwoju społeczeństwa informacyjnego został opracowany na lata 2008-2015 i przyjęty uchwałą(…) 9 grudnia 2008 r. Program ten zakładał realizację celów operacyjnych m.in. takich jak E-urząd – rozwój elektronicznych usług świadczonych przez administrację samorządową oraz E-gmina – rozwój elektronicznych usług świadczonych na obszarze gminy w ramach oświaty, kultury i sportu. Wynikiem realizacji tych celów było przystąpienie do platformy regionalnej Sekap(…). Zakres Projektu obejmował stworzenie teleinformatycznego środowiska dla świadczenia usług publicznych w formie elektronicznej. (…) W okresie objętym kontrolą nie powstał nowy program informatyzacji (...). Mając jednak pełną świadomość konieczności rozwoju e-usług, jeszcze przed rokiem 2016 jako partner platformy Sekap przystąpiono i wykonano integrację z platformą ePUAP*."

(akta kontroli str. 20-21, 24-27)

2. Według stanu na 31 maja 2020 r. Urząd udostępnił łącznie 75 usług elektronicznych poprzez ePUAP, w następujących kategoriach:

- pisma ogólne, skargi, wnioski, zapytania do Urzędu – dwie usługi[9];
- bezpieczeństwo i zarządzanie kryzysowe (imprezy masowe, zgromadzenia publiczne, sprawy obronne) - jedna usługa[10];
- budownictwo, architektura, urbanistyka - 18 usług[11];
- dowody osobiste, meldunki, wybory - sześć usług[12];
- geodezja, kartografia - trzy usługi[13];
- komunikacja, drogownictwo i transport - dwie usługi[14];
- nieruchomości, lokale mieszkalne i użytkowe - jedna usługa[15];
- ochrona środowiska - cztery usługi[16];
- podatki i opłaty - 26 usług[17];
- urodzenia, małżeństwa, zgony - trzy usługi[18];
- zdrowie i sprawy społeczne (pomoc społeczna, świadczenia rodzinne, zasiłki) - osiem usług[19];
- inne - jedna usługa[20].

[9] Pismo ogólne do Urzędu, Udostępnianie informacji publicznej.

[10] Wniosek o zasiłek powodziowy w kwocie do 2 tys. zł.

[11] M.in.: Planowanie przestrzenne; Budowanie domu; Uzyskanie wypisów i wyrysów; Ustalenie warunków zabudowy i zagospodarowania terenu; Uzyskanie zaświadczeń i opinii w zakresie planowania przestrzennego; Przyjmowanie wniosków i uwag do sporządzanych miejscowych planów zagospodarowania przestrzennego; Przyjmowanie wniosków i uwag do sporządzonego studium uwarunkowań i kierunków zagospodarowania przestrzennego; Wydanie wypisu i wyrysu ze studium uwarunkowań i kierunków zagospodarowania przestrzennego; Wypisy i wyrysy z miejscowego planu zagospodarowania przestrzennego; Zaświadczenia o przeznaczeniu terenu w planie miejscowym; Zaświadczenie o przeznaczeniu działki w miejscowym planie zagospodarowania przestrzennego;

[12] M.in.: Zamelduj się na pobyt stały lub czasowy; Uzyskaj dowód osobisty; Dopisanie się do spisu wyborców.

[13] M.in.: Ustalenie numeru porządkowego budynku; Zawiadomienie o wykonaniu zgłoszonych prac geodezyjnych lub prac kartograficznych.

[14] M.in.: Udzielenie licencji na wykonywanie krajowego transportu drogowego w zakresie przewozu osób taksówką; Zmiana licencji na wykonywanie transportu drogowego taksówką.

[15] Tj.: Ustalenie wysokości odszkodowania za przyjętą nieruchomość.

[16] M.in.: Informacje i dane o zakresie korzystania ze środowiska oraz o wysokości należnych opłat.

[17] M.in.: Umorzenia, odroczenia , rozkładanie na raty - łącznego zobowiązania pieniężnego - podatek rolny, od nieruchomości, leśny, od środków transportowych; Nadpłaty w podatkach i opłatach lokalnych; Odwołania i zażalenia.

[18] M.in.: Wnioskowanie o wydanie odpisu aktu stanu cywilnego; Zgłoszenie urodzenia dziecka.

[19] M.in.: Przyznanie dodatku mieszkaniowego; Przyznanie prawa do dodatku pielęgnacyjnego; Stypendium szkolne.

[20] Tj.: Złożenie, zmiana, wycofanie oferty oraz komunikacja Zamawiającego z Wykonawcą.

Wyżej wymienione usługi elektroniczne były również udostępnione na regionalnej platformie SEKAP (obejmującej swoim zasięgiem województwo śląskie) oraz część z nich na platformie Emp@tia (o zasięgu ogólnokrajowym).
W okresie objętym kontrolą Urząd nie udostępniał e-usług w następujących dziedzinach: 1. gospodarka komunalna; 2. kultura, sport, turystyka, oświata; 3. ochrona praw konsumentów; 4. rolnictwo, leśnictwo, łowiectwo, rybołówstwo; 5. rozwój regionalny.

(akta kontroli str. 90-94)

3. W okresie od 1 stycznia do 30 czerwca 2020 r. za pośrednictwem platformy ePUAP wpłynęło do Urzędu 613 dokumentów elektronicznych, z tego:

a) w I okresie – od 1 stycznia do 29 lutego 2020 r. – dotyczących 72 spraw,
b) w II okresie – od 1 marca do 30 kwietnia 2020 r. – dotyczących 116 spraw (wzrost o 61% w stosunku do I okresu),
c) w III okresie – od 1 maja do 30 czerwca 2020 r. – dotyczących 425 spraw (wzrost o 490% w stosunku do I okresu).

Większość spraw dotyczyła e-usług z następujących kategorii: *dowody osobiste, meldunki, wybory* (532 sprawy); *urodzenia, małżeństwa, zgony* (50 spraw); *pisma ogólne, skargi, wnioski, zapytania do urzędu* (15 spraw).

(akta kontroli str. 96-98, 141-144)

Znaczący wzrost zainteresowania mieszkańców e-usługami w II okresie w stosunku do I okresu odnotowano w zakresie usługi *zamelduj się na pobyt stały lub czasowy*, tj. o 450% (z 6 usług do 33). Natomiast w III okresie w stosunku do I okresu wzrost wykorzystania e-usług wystąpił w przypadku następujących usług: *uzyskaj dowód osobisty* o 48,9% (z 47 usług do 70), *dopisanie się do spisu wyborców* (z 0 do 220), *wpisanie się do rejestru wyborców* (z 0 do 16 usług), *zgłoszenie zamiaru głosowania korespondencyjnego* (z 0 do 64), *wnioskowanie o wydanie odpisu aktu cywilnego* o 69,2% (z 13 usług do 22).

(akta kontroli str. 141-144)

4. W sprawie prowadzenia monitoringu poziomu wykorzystania e-usług realizowanych poprzez ePUAP i SEKAP Burmistrz podał, że Urząd prowadził taki monitoring w okresach rocznych: *(…) dokonywano porównań okresów w stosunku do roku poprzedniego w zakresie korzystania przez klientów z usług świadczonych w formie elektronicznej na podstawie ilości korespondencji wpływającej w tej formie.*

Według wyjaśnienia Burmistrza Urząd nie dysponował *dokumentami w ww. zakresie z uwagi na fakt, iż opisywany proces monitoringu nie jest procesem sformalizowanym, jego wyniki były omawiane w ramach bieżącego informowania przełożonych przez pracowników Wydziału Informatyki*[21]*.* Burmistrz w wyjaśnieniach wskazał również, że nastąpił ponad trzykrotny wzrost ilości korespondencji wpływającej za pośrednictwem ePUAP, tj. z 825 spraw w 2016 r. do 2574 w 2019 r.[22] Natomiast w zakresie korespondencji przesyłanej za pośrednictwem platformy SEKAP odnotowano niewielki wzrost ilościowy dla analogicznego okresu – z 41 do 73 spraw.

(akta kontroli str. 20-21, 84-86)

5. W okresie objętym kontrolą do Urzędu nie wpłynęły skargi w sprawie jego działalności w zakresie świadczenia usług publicznych w formie elektronicznej, ani wnioski w sprawie usprawnienia tej formy komunikacji z Urzędem.

(akta kontroli str. 22-27)

[21] Dalej: „WI".
[22] Dane liczbowe odnoszące się do e-usług, z których korzystali obywatele i przedsiębiorcy.

6. W Urzędzie opracowano wewnętrzne procedury dotyczące obiegu dokumentów, wprowadzone Zarządzeniem Nr 120.62.2013 Kierownika Urzędu Miejskiego w Czechowicach-Dziedzicach z dnia 30 grudnia 2013 r. w sprawie zasad i trybu wykonywania czynności kancelaryjnych w Urzędzie Miejskim w Czechowicach-Dziedzicach. Zgodnie z § 1 ust. 1 i 4 ww. Zarządzenia podstawowym sposobem dokumentowania przebiegu załatwiania i rozstrzygania spraw w Urzędzie był *tradycyjny system wykonywania czynności kancelaryjnych* (papierowy), wspomagany programem elektronicznego zarządzania dokumentacją pn. FINN[23].
W ww. Zarządzeniu nie zawarto zasad postępowania z dokumentami wpływającymi, jak i wysyłanymi drogą elektroniczną za pośrednictwem ESP. Ustalono[24], że pisma wpływające na elektroniczną skrzynkę podawczą Urzędu były weryfikowane przez program FINN w zakresie ważności podpisu (w badanej próbie podpisy były prawidłowe), natomiast pisma wychodzące na elektroniczne skrzynki interesantów zostały podpisane przez upoważnione osoby, elektronicznie (kwalifikowanym podpisem).

(akta kontroli str. 20-21a, 24-44, 462)

Jak wyjaśnił Burmistrz, w jego ocenie zasady w ww. zakresie w sposób wystarczający i precyzyjny zostały określone w rozporządzeniu 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[25]. Wyjaśnił ponadto, że procedury określone w ww. Zarządzeniu nie zobowiązują pracowników do weryfikacji podpisów elektronicznych. Weryfikacja dokumentów elektronicznych co do aktualności podpisów elektronicznych dokonywana jest w sposób automatyczny przez program FINN, a wynik weryfikacji jest dołączany do przychodzącego dokumentu elektronicznego.

Podpisy elektroniczne w Urzędzie posiadali: Burmistrz, Zastępcy Burmistrza, Sekretarz Miasta, Skarbnik Miasta oraz kierownicy/naczelnicy wydziałów oraz osoby ich zastępujące. W okresie od 1 stycznia 2020 r. do 30 czerwca 2020 r. przez ww. osoby podpisanych elektronicznie zostało łącznie 210 pism.

(akta kontroli str. 20-21, 24-44, 84-86, 127)

W Urzędzie poszczególne etapy procesu elektronicznego obiegu spraw obejmowały[26]: wpływ pisma, automatyczną rejestrację pisma elektronicznego, dekretację pisma na wydział merytoryczny, odebranie pisma przez Naczelnika Wydziału, dekretację pisma przez Naczelnika Wydziału na pracownika merytorycznego, udzielenie odpowiedzi w formie elektronicznej i wysyłkę na elektroniczną skrzynkę obywatela.

(akta kontroli str. 369)

Najwyższa Izba Kontroli zauważa, że przepisy ws. instrukcji kancelaryjnej co prawda nie wymagają wprowadzenia osobnych procedur w jednostkach, które prowadzą papierowy system obiegu dokumentów, to jednak ustanowienie ich dla dokumentów elektronicznych byłoby korzystne przy wdrażaniu do pracy nowych pracowników oraz umożliwiłoby zapewnienie sprawnego świadczenia e-usług przez wszystkich pracowników. Ponadto, wprowadzenie procedur do elektronicznej obsługi spraw

[23] Dalej: „Program FINN".
[24] Na podstawie oględzin przeprowadzonych w dniu 3 września 2020 r. w systemie FINN, w zakresie prawidłowości podpisywania badanej korespondencji wpływającej o numerach: R.K.P. 11503.2020; R.K.P. 23 300.2020, R.K.P. 15006.2020 z 06.04.2020 r. oraz wychodzącej: R.K.W. 001555.2020 z 28.04.2020 r., R.K.W. 00182.2020 z 12.05.2020 r., R.K.W. 00193.2020 z 10.06.2020 r. .
[25] Dz.U. Nr 14 poz. 67, ze zm.
[26] Ustalono w oparciu o analizę załatwienia sprawy o numerze RKP.25720.2020 w ramach wykorzystania e-usługi.

może przyczynić się do sprawowania odpowiedniej kontroli pracy urzędników oraz ułatwić diagnozę wystąpienia ewentualnych nieprawidłowości.

7. Analiza wybranych losowo 20 spraw[27], które wpłynęły do Urzędu w formie elektronicznej poprzez ePUAP w okresie pomiędzy 1 stycznia 2020 r. a 30 czerwca 2020 r. i zostały zarejestrowane w programie FINN, wykazała że:

- od momentu wpływu i rejestracji sprawy do jej dekretacji na pracownika prowadzącego daną sprawę upłynęło od jednego do 10 dni w 19 przypadkach oraz 25 dni w jednym przypadku[28];
- od momentu rejestracji do załatwienia sprawy upłynęło: w 18 przypadkach od 0 do 10 dni oraz w dwóch przypadkach odpowiednio: 19[29] i 25 dni[30]. Wszystkie badane sprawy zostały załatwione w terminach zgodnych z obowiązującymi przepisami prawnymi;
- w badanych sprawach wnioski/formularze nie wymagały korekt;
- we wszystkich badanych sprawach system elektronicznego obiegu dokumentów nie komunikował się z innymi systemami informatycznymi w zakresie przesyłania danych niezbędnych dla załatwienia sprawy,
- Urząd nie komunikował się z inną jednostką administracji publicznej w celu uzyskania danych lub dokumentów;
- we wszystkich badanych sprawach nie było konieczności dostarczania przez wnioskodawców informacji będących w posiadaniu innego urzędu,
- w badanych sprawach obywatel nie występował o uzyskanie informacji o stanie załatwienia sprawy;
- w siedmiu[31] z 20 spraw Urząd korzystał z danych zgromadzonych w zewnętrznym systemie *Źródło*[32];
- w trzech[33] z 20 spraw petent mógł sprawdzić na jakim etapie jest sprawa związana z wydaniem dowodu osobistego poprzez stronę www.gov.pl[34];
- w 11 przypadkach Urząd udzielił odpowiedzi w formie papierowej, w trzech przypadkach w formie elektronicznej, a w sześciu przypadkach sprawy nie wymagały odpowiedzi.

(akta kontroli str. 459-461, 589)

W związku z zadekretowaniem sprawy (o numerze RKP.24423.2020) po upływie 25 dni od dnia jej wpływu do Urzędu, Naczelnik Wydziału Finansowo-Budżetowego w Urzędzie wyjaśnił, że zwłoka w przekazaniu sprawy do załatwienia spowodowana była przejściowymi problemami kadrowymi, przy czym nie spowodowało to

[27] Badane 20 spraw z obszarów życia publicznego dotyczyło: z kategorii spraw osobowych - 13 przypadków, z pism ogólnych - jedna sprawa, z geodezji cztery sprawy i dwie sprawy z kategorii podatki i opłaty. Numery badanych spraw: RKP.14126.2020, RKP.23525.2020, RKP.25956.2020, RKP.14799.2020, RKP.13005.2020, RKP.00475.2020, RKP. 03961.2020, RKP. 24423.2020, RKP.07433.2020, RKP.22968.2020, RKP.11122.2020, RKP.03175.2020, RKP.22659.2020, RKP.22344.2020, RKP.18903.2020, RKP.07130.2020, RKP.23636.2020, RKP. 20930.2020, RKP.18260.2020, RKP.16944.2020.

[28] R.K.P.24423.2020 – dzień dekretacji był jednocześnie dniem załatwienia sprawy

[29] R.K.P. 00475.2020 – wniosek o udostępnienie informacji publicznej, Urząd – poinformował o przesunięciu terminu (wskazał nowy termin i powód przesunięcia), na podstawie art. 13 ust. 2 ustawy z dnia 6 września 2001 r. o dostępie do informacji publicznej (Dz.U. z 2019 r. poz. 1429).

[30] R.K.P.24423.2020. zgodnie z art. 139 §1 ustawy z dnia 29 sierpnia 1997 r. Ordynacja podatkowa (Dz.U. z 2020 poz. 1325, ze zm.)

[31] R.K.P. 14799.2020; R.K.P. 18903.2020; R.K.P. 07130.2020; R.K.P. 23636.2020; R.K.P. 20930.2020; R.K.P. 18260.2020; R.K.P. 16944.2020.

[32] System do wydawania aktów stanu cywilnego w zakresie meldunków i wydawania dowodów osobistych.

[33] R.K.P.18903.2020; R.K.P. 07130.2020; R.K.P. 23636.2020.

[34] W spawach dotyczących wniosku o wydanie dowodu osobistego, obywatel mógł sprawdzić czy dowód osobisty jest gotowy na stronie www.gov.pl, na ePUAP-ie nie było takiej możliwości.

opóźnienia w jej rozpatrzeniu, tj. sprawa została załatwiona zgodnie z art. 139 § 1 ustawy z dnia 29 sierpnia 1997 r. Ordynacja podatkowa[35].

8. Zasady dokonywania zgłoszeń o problemach technicznych występujących w funkcjonowaniu platformy ePUAP zauważonych przez Urząd były zgłaszane do pracowników Wydziału Informatyki, następnie e-mailowo problem zgłaszany był do firmy zewnętrznej prowadzącej bieżący nadzór nad systemem obiegu dokumentów w Urzędzie, w tym ePUAP. Firma ta, jeżeli problem tego wymaga, zgłasza zauważone usterki do Centralnego Ośrodka Informatyki oraz monitoruje bieżące działanie ePUPAP-u, w tym zgłasza wszelkie nieprawidłowości w jego działaniu administratorowi ePUAP. W okresie od 1 stycznia 2020 r. do 30 czerwca 2020 r. wystąpiło łącznie siedem problemów w funkcjonowaniu platformy ePUAP. Problemy te dotyczyły m.in. wysyłki dokumentów ePUAP, źle działającej usługi zgłoszenia pobytu stałego, braku dostępności platformy ePUAP z powodu prac serwisowych, automatycznego blokowania skrytek ePUAP.

(akta kontroli str. 127, 129-137)

9. Urząd zapewnił sprawne i nieprzerwane działanie programu FINN, tj. systemu do elektronicznego obiegu dokumentów. W okresie objętym kontrolą pomiędzy Gminą Czechowice-Dziedzice a firmą zewnętrzną zostało zawartych pięć umów[36], których przedmiotem było wykonanie usług w zakresie serwisu i nadzoru autorskiego, w tym m.in. konsultacje w zakresie oprogramowania FINN obejmujące administratorów oraz operatorów (użytkowników), wykonane poprzez telefon oraz przy wykorzystaniu poczty elektronicznej. W umowach tych zobowiązano wykonawcę do usuwania usterek i awarii, a w każdej z nich określono czas usunięcia awarii (jeden dzień roboczy licząc od dnia zgłoszenia) oraz czas usunięcia usterki (trzy dni robocze licząc od dnia zgłoszenia). Równocześnie w umowach tych zawarto zapis, że (…) *podane terminy mogą ulec zmianie w wyniku ustaleń pomiędzy stronami*. Umowy te obowiązywały w całym okresie wykorzystywania oprogramowania w Urzędzie.

(akta kontroli str. 20-21, 24-27, 45-64)

10. Urząd informował obywateli o możliwości załatwiania spraw drogą elektroniczną. Na swojej stronie BIP Urząd zamieścił informacje o usługach elektronicznych świadczonych na dwóch platformach (SEKAP oraz ePUAP), w tym o sposobach autoryzacji dokumentów elektronicznych:

- w przypadku ePUAP: płatnym/kwalifikowanym podpisem elektronicznym lub podpisem potwierdzonym profilem zaufanym (link do profilu zaufanego na stronie BIP Urzędu);
- w przypadku SEKAP: opatrzonym bezpiecznym podpisem cyfrowym weryfikowanym za pomocą ważnego kwalifikowanego certyfikatu, wydanego przez jeden z podmiotów kwalifikowanych, świadczących usługi certyfikacyjne lub opatrzonym bezpiecznym podpisem cyfrowym weryfikowanym za pomocą ważnego niekwalifikowanego certyfikatu, wydanego przez Urząd Rejestracji Centrum Certyfikacji SEKAP.

Na stronie BIP zawarto informacje o metodach komunikowania się z Urzędem (za pomocą SEKAP/ePUAP) oraz określono wymagania w zakresie akceptowalnych

[35] Dz.U. z 2020 poz. 1325, ze zm.

[36] Dotyczy umów o numerach: WI.1333.3.2016 z dnia 4 stycznia 2016 r. zawartej na okres 01.01.2016 r. - 31.12.2016 r. WI.1333.17.2017 z dnia 2 stycznia 2017 r. zawartej na okres 01.01.2017 r. - 31.12.2017 r., WI.1333.4.2018 z dnia 3 stycznia 2018 r. zawartej na okres 01.01.2018 r. - 31.12.2018 r., WI.1333.6.2019 z dnia 2 stycznia 2019 r. zawartej na okres 01.01.2019 r. - 31.12.2019 r., WI.1333.7.2016 z dnia 2 stycznia 2020 r. zawartej na okres 01.01.2020 r. - 31.12.2020 r.

formatów załączników. W sekcji *Elektroniczna skrzynka podawcza* zawarto linki do platform SEKAP i ePUAP, w których znajdował się katalog dostępnych usług/spraw. Natomiast na stronie internetowej Urzędu[37] w sekcji *Warto wiedzieć/Do urzędu na skróty* był link do elektronicznej skrzynki podawczej, za pośrednictwem której następowało przekierowanie na stronę BIP Urzędu[38]. W toku kontroli dodatkowo na stronie internetowej Urzędu został umieszczony graficzny link (odnośnik) do ePUAP. W okresie objętym kontrolą Urząd (w zakładce *Aktualności*) na stronie www.czechowice-dziedzice.pl informował mieszkańców o możliwości załatwiania spraw drogą elektroniczną[39].

(akta kontroli str. 20-21, 24-27, 65-83)

Na stronie Urzędu brak było informacji o możliwości załatwiania spraw z wykorzystaniem dowodu osobistego z warstwą elektroniczną.
Zastępca Naczelnika Wydziału Spraw Obywatelskich w Urzędzie wyjaśnił, że (…) *pracownicy Wydziału Spraw Obywatelskich każdorazowo informują o możliwościach wykorzystania podpisu osobistego w wybranych usługach na platformie gov.pl oraz o ewentualnej możliwości jego wykorzystania w przyszłości na innych platformach. Sam proces wydawania dowodu osobistego wymaga podania przez petenta 6 cyfrowego kodu do aktywacji certyfikatu podpisu osobistego i wówczas niejednokrotnie padają pytania ze strony petenta o możliwości wykorzystania tego podpisu.*

(akta kontroli str. 590)

NIK zauważa, że z uwagi na zastosowanie e-dowodu, w tym możliwość zalogowania się do ePUAP lub elektroniczne podpisywanie dokumentów i wniosków, wskazanym jest umieszczenie informacji o nim w miejscu, w którym te sprawy będą załatwiane, tj. m.in. na stronie internetowej Urzędu.

11. W okresie od 1 lipca 2018 r. do 30 czerwca 2020 r. pracownicy Urzędu uczestniczyli w łącznie 18 szkoleniach, w ramach których przeszkolono 147 pracowników[40]. Szkolenia dotyczyły w szczególności ochrony danych osobowych oraz zapewnienia bezpieczeństwa informacji.

W ramach ww. szkoleń przeprowadzono cztery szkolenia wewnętrzne, tj.:

- „Wdrożenie przepisów RODO w Urzędzie Miejskim w Czechowicach-Dziedzicach”[41], w którym przeszkolono wszystkich pracowników świadczących pracę w okresie od dnia 1 lipca 2018 r. – 30 czerwca 2020 r. – 38 pracowników. W okresie wcześniejszym, tj. od 13 marca 2018 r. do 30 czerwca 2020 r. – przeszkolono łącznie 157 pracowników[42];

[37] www.czechowice-dziedzice.pl
[38] www.bip.czechowice-dziedzice.pl
[39] Przykładowe informacje (tytuły wiadomości): *Sprawdź ważność swojego dowodu osobistego* z dnia 26-01-2018; http://czechowice-dziedzice.pl/www_3.0/aktualnosc-2637-sprawdz_waznosc_swojego_dowodu.html; *Rodzicu, zarejestruj swoje dziecko online!* Komunikat Ministerstwa Cyfryzacji z dnia 21-06-2018; http://czechowice-dziedzice.pl/www_3.0/aktualnosc-2820-rodzicu_zarejestruj_swoje_dziecko.html; *Od 17 marca Urząd Miejski w Czechowicach-Dziedzicach wstrzymuje bezpośrednią obsługę mieszkańców* z dnia 16-03-2020 http://czechowice-dziedzice.pl/www_3.0/aktualnosc-3514-od_17_marca_urzad_miejski_w.html; *Wydłużone terminy naborów z PROW 2014-2020*; Komunikat ARMiR z dnia 27-04-2020 http://czechowice-dziedzice.pl/www_3.0/aktualnosc-3600-wydluzone_terminy_naborow_z_prow_2014.html; *Kasa Urzędu Miejskiego będzie otwarta. Od poniedziałku 11 maja* z dnia 07-05-2020 http://czechowice-dziedzice.pl/www_3.0/aktualnosc-3619-kasa_urzedu_miejskiego_bedzie_otwarta.html
[40] W tym w 4 szkoleniach wewnętrznych przeszkolono 136 pracowników, a w 14 szkoleniach zewnętrznych przeszkolono 11 pracowników.
[41] Zorganizowane były przez Biuro ds. Ochrony Informacji Niejawnych i Ochrony Danych Osobowych Urzędu (dalej: „OID”) - szkolenie w tym zakresie były przeprowadzane zbiorowo oraz indywidualnie przy przyjęciu do pracy.
[42] Z czego 12 pracowników będących Naczelnikami Wydziałów brało dwukrotnie udział w szkoleniu.

- dwukrotnie zorganizowano szkolenie pn. „Cyberterroryzm jako współczesne wyzwanie dla bezpieczeństwa teleinformatycznego jednostek organizacyjnych administracji publicznej”[43] - przeszkolono 58 pracowników Urzędu;
- „Oprogramowanie złośliwe zagrożeniem w cyberprzestrzeni”[44] – przeszkolono 40 pracowników Urzędu.

Pracownicy Urzędu brali także udział m.in. w następujących szkoleniach zewnętrznych:

- „Ustawa o krajowym systemie cyberbezpieczeństwa”[45] – przeszkolono dwóch pracowników, w tym jednego z OID oraz jednego z WI;
- „Monitorowanie użytkowników zgodnie z RODO”[46] – przeszkolono jednego pracownika OID;
- „Nadawanie uprawnień w systemach teleinformatycznych urzędu”[47] – przeszkolono jednego pracownika WI;
- „Ocena skutków oraz szacowanie ryzyka w bezpieczeństwie danych osobowych zgodnie z RODO”[48] – przeszkolono jednego pracownika WI;
- „System zarządzania bezpieczeństwem informacji ISO/IEC 27001:2017”[49] – przeszkolono jednego pracownika WI;
- „Wdrażanie, zarządzanie i zabezpieczanie sieci za pomocą zasad grupy”[50] – przeszkolono jednego pracownika WI.

(akta kontroli str. 498-530)

12. Zgodnie z § 20 ust. 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*.
Ww. wymagania uznaje się za spełnione (zgodnie z § 20 ust. 3 tego rozporządzenia), jeżeli SZBI 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[51].

W Urzędzie nie opracowano i nie wdrożono SZBI, w szczególności polityki bezpieczeństwa informacji, jak i nie przeprowadzono całościowo okresowych analiz ryzyka utraty integralności, dostępności lub poufności informacji oraz nie podejmowano działań minimalizujących to ryzyko, stosownie do wyników przeprowadzonej analizy w rozumieniu przepisów *rozporządzenia KRI*, co szerzej opisano w sekcji *Stwierdzone nieprawidłowości*. Obowiązujące w Urzędzie *Polityka Bezpieczeństwa* oraz *Instrukcja Zarządzania Systemem Informatycznym*[52] dotyczyły bezpieczeństwa danych osobowych.

---

[43] Szkolenie przeprowadzono 23 sierpnia 2018 r. oraz 24 czerwca 2020 r.
[44] Przeprowadzone 20 maja 2019 r.
[45] Przeprowadzone 24 październik 2018 r.
[46] Przeprowadzone 14 luty 2019 r.
[47] Przeprowadzone 20 marzec 2019 r.
[48] Przeprowadzone 24 kwietnia 2019 r.
[49] Przeprowadzone 18 września 2019 r.
[50] Przeprowadzone w dniach 16 grudnia - 20 grudnia 2019 r.
[51] 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.
[52] Oba dokumenty wprowadzone Zarządzeniem nr 120.31.2018 Kierownika Urzędu Miejskiego w Czechowicach-Dziedzicach z dnia 25 maja 2018 r. (odpowiednio załącznik nr 1 i nr 2). Zarządzenie uchylono i wprowadzono Zarządzenie nr 120.31.2018 Kierownika Urzędu Miejskiego w Czechowicach-Dziedzicach z dnia 25 maja 2018 r., którym Burmistrz wprowadził do stosowania i przestrzegania Politykę Ochrony Danych Osobowych jako dokumentację opisującą zasady ochrony danych osobowych w Urzędzie Miejskim w Czechowicach-Dziedzicach. Zarządzenie nr 120.7.2019 Kierownika Urzędu Miejskiego w Czechowicach-

(akta kontroli str. 157-274)

Burmistrz wyjaśnił, że w Urzędzie w celu zapewnienia bezpieczeństwa informacji opracowano i wdrożono szereg procedur, regulaminów i polityk ochrony danych, w tym:

- Polityka Ochrony Danych Osobowych (etapy jej wprowadzania opisane w przypisie nr 55);
- Plan ochrony i zapewnienia ciągłości działania Urzędu Miejskiego w Czechowicach-Dziedzicach: wprowadzony zarządzeniem nr 120.34.2013 Kierownika Urzędu Miejskiego w Czechowicach-Dziedzicach z dnia 30 lipca 2013 r. w sprawie planu ochrony i zapewnienia ciągłości działania Urzędu Miejskiego w Czechowicach-Dziedzicach, który został uchylony i wprowadzono kolejny zarządzeniem 120.24.2019 Kierownika Urzędu Miejskiego w Czechowicach-Dziedzicach z dnia 31 maja 2019 r. w sprawie planu ochrony i zapewnienia ciągłości działania Urzędu Miejskiego w Czechowicach-Dziedzicach (z uwagi na konieczność zmian w zakresie lokalizacji niektórych komórek, pojawienia się nowych obiektów oraz konieczności aktualizacji charakterystyki wybranych obiektów);
- zarządzenia dotyczące wydzielenia pomieszczeń podlegających szczególnej ochronie oraz określenia trybu postępowania z kluczami od pomieszczeń podlegających szczególnej ochronie i od pozostałych pomieszczeń w budynkach Urzędu oraz zabezpieczenia tych pomieszczeń[53];
- Procedura nadawania i cofania upoważnień dla pracowników i innych osób uczestniczących w procesie przetwarzania danych;
- Procedura przydzielania i cofania uprawnień do zasobów;
- Zasady nadawania identyfikatorów;
- Polityka haseł;
- Procedura rozpoczęcia, zawieszenia i zakończenia pracy;
- Zasady korzystania z systemu informatycznego;
- Zasady korzystania z internetu;
- Zasady korzystania z poczty elektronicznej;
- Zasady użytkowania przenośnych nośników danych;
- Zasady przetwarzania danych poza Urzędem;
- Zakup nowego oprogramowania;
- Procedura instalacji oprogramowania;

Dziedzicach z dnia 30 stycznia 2019 r. zmieniające ww. zarządzenie nr 120.31.2018 w sprawie wprowadzenia Polityki Ochrony Danych Osobowych w Urzędzie Miejskim w Czechowicach-Dziedzicach wprowadzono tekst jednolity Polityki Ochrony Danych Osobowych uwzględniając wprowadzone zmiany, które dotyczyły m.in.: polityki haseł; zasad korzystania z poczty elektronicznej; zasad użytkowania przenośnych nośników danych; procedury powierzenia przetwarzania danych osobowych podmiotom zewnętrznym.

[53] Zarządzenie nr 120. 30 .2011 Kierownika Urzędu Miejskiego w Czechowicach-Dziedzicach z dnia 21 lipca 2011 r. w sprawie wydzielenia pomieszczeń podlegających szczególnej ochronie oraz określenia trybu postępowania z kluczami od pomieszczeń podlegających szczególnej ochronie i od pozostałych pomieszczeń w budynkach Urzędu Miejskiego w Czechowicach-Dziedzicach oraz zabezpieczenia tych pomieszczeń, uchylone Zarządzeniem nr 120. 36 .2017 Kierownika Urzędu Miejskiego w Czechowicach-Dziedzicach z dnia 31 maja 2017 r. w sprawie wydzielenia pomieszczeń podlegających szczególnej ochronie oraz określenia trybu postępowania z kluczami od pomieszczeń podlegających szczególnej ochronie i od pozostałych pomieszczeń w budynkach Urzędu Miejskiego w Czechowicach-Dziedzicach oraz zabezpieczenia tych pomieszczeń, zmienione - Zarządzeniem nr 120.28.2018 r. Kierownika Urzędu Miejskiego w Czechowicach-Dziedzicach z dnia 22 maja 2018 r. - zmiany zarządzenia obejmowały pomieszczenia podlegające szczególnej ochronie, zmiany sposobu plombowania pomieszczeń podlegających szczególnej ochronie i doprecyzowania zapisów zarządzenia dot. zabezpieczenia kluczy od biurek.

- Procedura powierzenia przetwarzania danych osobowych podmiotom zewnętrznym;
- Procedura wykonywania przeglądów, konserwacji i napraw;
- Procedura wykonywania aktualizacji oprogramowania dziedzinowego,
- Procedura zarządzania kopiami zapasowymi;
- Procedurę postępowania w przypadku naruszenia bezpieczeństwa danych osobowych.

Wskazana wyżej dokumentacja określała m.in. szczegółowe zasady wdrożenia zabezpieczeń technicznych, jaki i organizacyjnych w Urzędzie w zakresie przetwarzania oraz bezpieczeństwa danych osobowych.

(akta kontroli str. 194-274, 321-333)

13. 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. W okresie objętym kontrolą w Urzędzie nie prowadzono elektronicznego rejestru zasobów teleinformatycznych. Dane o sprzęcie komputerowym Urzędu ujmowano w *kartach sprzętu komputerowego* oraz w zestawieniu środków trwałych (dla potrzeb rachunkowości). Nie zawierały one jednak szczegółowych informacji o konfiguracji technicznej urządzeń, czy też o zainstalowanym na nich oprogramowaniu. Powyższe opisano szerzej w dalszej części wystąpienia pokontrolnego, w sekcji *Stwierdzone nieprawidłowości*.

(akta kontroli str. 421-458)

14. W Urzędzie, stosownie do § 20 ust. 2 pkt 4 *rozporządzenia KRI*, podjęto działania mające na celu uniemożliwienie zainstalowania nieautoryzowanego oprogramowania na sprzęcie komputerowym.

Badanie przeprowadzone na wybranych losowo 10 komputerach[54] wykazało, że urządzenia były odpowiednio zabezpieczone przed zainstalowaniem na nich nieautoryzowanego oprogramowania przez użytkowników komputerów. Użytkownicy poddanego badaniu sprzętu komputerowego nie posiadali uprawnień administracyjnych do samodzielnej instalacji oprogramowania.

(akta kontroli str. 145-156)

15. W okresie od 1 stycznia 2016 r. do 30 czerwca 2020 r. pracę w Urzędzie zakończyło 41 pracowników (z czego 37 to pracownicy biurowi, a czterech to pracownicy obsługi).

(akta kontroli str. 588)

Na podstawie wytypowanej próby dotyczącej 15 byłych pracowników merytorycznych Urzędu (spośród ww. 37 pracowników biurowych) stwierdzono, że we wszystkich przypadkach usunięto lub zablokowano im dostęp do systemów informatycznych. Każdy z badanych byłych pracowników miał sporządzone „Wnioski o cofniecie uprawnień do zasobu”[55], jednakże analiza poszczególnych wniosków wykazała, że nie we wszystkich przypadkach nastąpiło bezzwłocznie cofnięcie

[54] Sprzęt wykorzystywany przez pracowników Urzędu, tj.: pięć komputerów stacjonarnych o numerach inwentarzowych: 750/4/2278; 750/4/2373; 750/4/2287; 750/4/2377; 750/4/2375 oraz pięć komputerów przenośnych - laptopów o numerach inwentarzowych: 11/35/0410; X1/35/410; 750/4/2290; 11/35/01154a; 750/4/2291.

[55] Liczba analizowanych cofnięć uprawnień do poszczególnych systemów informatycznych przypisanych do badanych 15 byłych pracowników Urzędu dotyczyła 103 wniosków o cofnięcie uprawnień do zasobu.

nadanych im uprawnień, co szerzej opisano w dalszej części wystąpienia pokontrolnego, w sekcji *Stwierdzone nieprawidłowości*.

(akta kontroli str. 139, 369-397, 531-586)

16. Stosownie do wymogów § 20 ust. 2 pkt *14 rozporządzenia KRI*, zarządzanie bezpieczeństwem informacji realizowane jest przez zapewnienie okresowego audytu wewnętrznego w zakresie bezpieczeństwa informacji, nie rzadziej niż raz na rok. W Urzędzie w latach 2016-2018 nie przeprowadzono takiego audytu (co przedstawiono szczegółowo w sekcji *Stwierdzone nieprawidłowości*).

W grudniu 2019 r. rozpoczęto badanie audytowe w tym zakresie, jednakże do dnia zakończenia niniejszej kontroli NIK, badanie to nie zostało zakończone. Z prowadzonego audytu, w toku kontroli, przedłożono dwie listy kontrolne sporządzone w 2020 r., które zostały uzupełnione przez Naczelnika WI oraz Administratora Systemu Informatycznego.

Zadanie przeprowadzenia audytu w zakresie bezpieczeństwa informacji ujmowano każdorazowo w planach audytu wewnętrznego, do realizacji jednokrotnie w poszczególnych latach 2016-2019 oraz dwukrotnie w 2020 r.

(akta kontroli str. 95-96, 99-126, 464-493)

Stwierdzone nieprawidłowości

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

1. W Urzędzie nie opracowano i nie wdrożonego SZBI (w szczególności PBI), o którym mowa w § 20 ust. 1 w związku z ust. 3 *rozporządzenia KRI*. Ponadto, nie przeprowadzono całościowych okresowych analiz ryzyka utraty integralności, dostępności lub poufności informacji oraz nie podjęto działań minimalizujących to ryzyko stosownie do wyników przeprowadzonej analizy, mimo że z § 20 ust. 2 pkt 3 tego rozporządzenia wynikał taki wymóg, a które powinny stanowić podstawę ustalenia i wdrożenia SZBI. Ustanowione i aktualizowane – w okresie objętym kontrolą – wewnętrzne uregulowania dotyczące *Polityki Ochrony Danych Osobowych* oraz *Instrukcji Zarządzania Systemem Informatycznym* nie stanowią realizacji obowiązku opracowania kompleksowego zestawu zasad i procedur bezpieczeństwa, o których mowa w przywołanych powyżej przepisach.

(akta kontroli str. 464-497)

Burmistrz wyjaśnił, że opracowane w Urzędzie procedury wpisują się w wymagania stawiane przez przepisy *rozporządzenia KRI* oraz regulują procesy bezpieczeństwa fizycznego obiektów. Dodał, że będąc jednak świadomym, że dokumenty w Urzędzie nie wyczerpują wymagań stawianych SZBI, podejmie działania zmierzające do dokonania analizy w tym zakresie i dokonana przeglądu istniejących dokumentów, mając na celu w pełni dostosowanie ich do wymogów wynikających z przepisów *rozporządzenia KRI*. Ponadto Burmistrz wyjaśnił, że analiza zagrożeń została opracowana w *Planie ochrony i zapewnienia ciągłości działania (…)* i została przeprowadzona w odniesieniu do bezpieczeństwa fizycznego obiektów. Wyjaśnił również, że okresowa analiza ryzyka utraty integralności, poufności, dostępności, o której mowa z § 20 ust. 2 pkt 3 *rozporządzenia KRI*, prowadzona była w Urzędzie w sposób niesformalizowany i nieudokumentowany, ale biorąc pod uwagę, że nie wszystkie obszary zostały nią objęte, w szczególności nie była to analiza o charakterze formalnym, podejmie działania zmierzające do przeprowadzenia analizy ryzyka w pełni zgodnej z wymaganiami *rozporządzenia KRI*.

(akta kontroli str. 464-497)

2. W Urzędzie nie prowadzono inwentaryzacji zasobów informatycznych w sposób określony w § 20 ust. 2 pkt 2 *rozporządzenia KRI*, który stanowi, że zarządzanie infrastrukturą informatyczną wymaga utrzymywania w urzędzie aktualności inwentaryzacji sprzętu i oprogramowania służącego do przetwarzania informacji obejmującej ich rodzaj i konfigurację.

Dane o sprzęcie komputerowym Urzędu ujmowano w *kartach sprzętu komputerowego* oraz w zestawieniu środków trwałych (dla potrzeb rachunkowości). Nie zawierały one jednak szczegółowych informacji o konfiguracji technicznej urządzeń, czy też o zainstalowanym na nich oprogramowaniu.

Przeprowadzone badanie, oparte o dobór celowy 15 użytkowanych urządzeń[56], wykazało, że dwa z 15 badanych urządzeń, tj. router[57] i drukarka[58] nie posiadały założonych *kart sprzętu komputerowego*. W 13 badanych *kartach sprzętu komputerowego* nie było określonej konfiguracji sprzętowej, natomiast rodzaj nie był podany w *kartach* dotyczących 10 badanych komputerów stacjonarnych. Ponadto, w badanych *kartach sprzętu komputerowego* nie było informacji dotyczącej osoby je sporządzającej oraz brak było dat: sporządzenia kart, instalacji oprogramowania, zakupu oraz ważności licencji.

(akta kontroli str. 421-458)

Burmistrz wyjaśnił, że prowadzona dokumentacja w zakresie inwentaryzacji nie obejmowała rodzaju i konfiguracji ponieważ wcześniej przeprowadzono analizę pod kątem informacji potrzebnych do odtworzenia sprzętu w wyniku różnych zdarzeń. Podał także: (…) *Biorąc pod uwagę jednak, że przeprowadzona powyżej analiza i ustalenia poczynione na jej bazie, mogą być niezgodne z przepisami KRI, podejmę działania w zakresie prowadzenia inwentaryzacji sprzętu i oprogramowania zgodnie z przepisami prawa w szczególności inwentaryzacji obejmującej informacje o rodzaju i konfiguracji sprzętu.* Natomiast w kwestii braku inwentaryzacji w formie elektronicznej, jako przyczynę wskazał brak narzędzia wspomagającego ten proces oraz podał, że dokonane zostanie rozeznanie możliwości zakupu i wdrożenia takiego oprogramowania biorąc pod uwagę możliwości finansowe w tym zakresie.

NIK zauważa, że na rynku istnieje alternatywa dla systemów i programów płatnych – aplikacje typu „open source”[59], posiadające funkcjonalności w zakresie inwentaryzacji sprzętu i oprogramowania.

(akta kontroli str. 464-474, 494-497)

3. W przypadku 12 z 15 badanych spraw dotyczących byłych pracowników Urzędu, w zakresie 33 *Wniosków o cofnięcie uprawnień do zasobu* (tj. 32% spośród 103 poddanych analizie wniosków) do poszczególnych systemów informatycznych, zablokowanie lub usunięcie danego konta nie nastąpiło bezzwłocznie, co było niezgodne z § 20 ust. 2 pkt 5 *rozporządzenia KRI*.

Konta byłych pracowników zostały zablokowane lub usunięte ze zwłoką[60], tj. po upływie od 4 do 10 dni w 26 przypadkach, w pięciu przypadkach po: 48 dniach, 68

---

[56] Oględzinom poddano: 10 komputerów stacjonarnych o numerach inwentarzowych: 750/4/2440, 750/4/2441, 750/4/2442, 750/4/2443, 750/4/2316, XI/35/407, XI/35/468, XI/35/469, 750/4/2189, XI/35/457; 2 komputery przenośne (typu notebook) o numerach inwent.: 750/4/2380, 750/4/2382; jedną drukarkę znajdująca się w Wydziale Spraw Obywatelskich o nr inwent.: XI/35/317 Drukarka Kyocera-Mita FS-2100DN , jak i jeden router: znajdujący się w pomieszczeniu Serwerowni o nr inwent.: XI/35/288 Router oraz jeden serwer znajdujący się w pomieszczeniu Serwerowni o nr inwent.: 780/4/2272 Serwer.

[57] Router: znajdujący się w pomieszczeniu Serwerowni o nr inwent.: XI/35/288 Router.

[58] Drukarki znajdującej się w Wydziale Spraw Obywatelskich o nr inwent.: XI/35/317 Drukarka Kyocera-Mita FS-2100DN.

[59] Idea wolnego oprogramowania, która daje możliwość użytkownikom legalnego oraz darmowego korzystania z określonych aplikacji i programów użytkowych (w szczególności swobodnego uruchamiania, rozpowszechniania i modyfikowania programów komputerowych).

dniach, 118 dniach, 202 dniach, 212 dniach oraz w dwóch przypadkach po 74 dniach.

(akta kontroli str. 139, 369-397, 531-586)

W związku z powyższym Burmistrz wyjaśnił, że procedura cofania uprawnień do zasobu była opisana w pkt 8.2 *Polityki Ochrony Danych Osobowych*, jednakże nie zawierała ona regulacji dotyczącej w jakim okresie należy dokonać czynności cofnięcia uprawnień do zasobu, co mogło stanowić przyczynę, że faktyczny okres cofania uprawnień różnił się od okresu określonego w § 20 ust. 2 pkt 5 rozporządzenia KRI. Wyjaśnił także, że niemożliwe jest wskazanie na jakim etapie nastąpiło opóźnienie w realizacji procesu cofania dostępu do zasobu.
Burmistrz w wyjaśnieniu podał, że mając na uwadze podniesienie bezpieczeństwa informacji, jaki i zapewnienie zgodności polityki z przepisami prawa, polecił pracownikom zaangażowanym w ten proces zaproponowanie zmian korygujących regulacje w powyższym zakresie.

(akta kontroli str. 398-418, 419-420)

4. W latach 2016-2019 (do grudnia 2019 r.) w Urzędzie nie przeprowadzono okresowego audytu wewnętrznego z zakresu bezpieczeństwa informacji, co było niezgodne z § 20 ust. 2 pkt 14 *rozporządzenia KRI*, który stanowi, że audyt taki powinien być przeprowadzony nie rzadziej niż raz na rok.

(akta kontroli str. 99-126)

Burmistrz w powyższym zakresie wyjaśnił m.in., że audytor wewnętrzny rozpoczął zadanie audytowe (grudzień 2019 r./kontynuacja w 2020 r.) pn. „Bezpieczeństwo informacji (system zarządzania bezpieczeństwem informacji SZBI)", jednak przeprowadzenie zadania zostało zawieszone na skutek otrzymania zlecenia innego zadania audytowego (w Wydziale Geodezji, Kartografii, Katastru i Gospodarki Nieruchomościami). Jednocześnie okoliczności związane z pandemią Covid-19 spowodowały dłuższą nieobecność audytora wewnętrznego w pracy. Ponadto wskazał, że oba ww. zadania są w toku realizacji oraz, że w 2018 r. *przeprowadzono audyt w zakresie zgodności z ogólnym rozporządzeniem o ochronie danych (RODO)*. Podał także, że ze względu na finansowy aspekt, nie zlecano przeprowadzenia audytu wymaganego § 20 ust. 2 pkt 14 *rozporządzenia KRI* podmiotowi zewnętrznemu. Zadanie było jednak każdorazowo ujmowanie w rocznym planie audytu a *niewykonanie wynikało z braku budżetu czasowego audytora wewnętrznego (tak rozbudowane zadanie audytowe wymaga innego przygotowania, szczególnie przy braku wystarczającej wiedzy merytorycznej w tym zakresie, brak szkoleń dedykowanych dla audytorów wewnętrznych w tym zakresie; brak szczegółowych wytycznych).*

(akta kontroli str. 99-100, 464-497)

Odnosząc się do powyższych wyjaśnień, NIK zauważa, że przedstawione powyżej okoliczności nie mogą usprawiedliwiać niedopełnienia obowiązków ustalonych przepisami *rozporządzenia KRI*, a wskazany przez Burmistrza audyt z 2018 r. był przeprowadzony w celu zdiagnozowania stanu przygotowania Urzędu do zmiany przepisów w zakresie danych osobowych (RODO), a nie dostosowania działalności Urzędu do przepisów *rozporządzenia KRI*.

[60] Sposób wyliczenia dni: uwzględniono tylko dni robocze, pominięto w wyliczaniu święta i dni wolne, w których Urząd miał dni wolne za dni świąteczne. Wykaz dni w których pracownicy Urzędu nie świadczyli pracy, został podany przez Burmistrza.

IV. Wnioski

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

Wnioski

1. **Opracowanie i wdrożenie systemu zarządzania bezpieczeństwem informacji (SZBI) zgodnego z normą PN-ISO/IEC 27001, w tym polityki bezpieczeństwa informacji.**
2. **Zaprowadzenie inwentaryzacji zasobów informatycznych, spełniającej wymogi *rozporządzenia KRI*.**
3. **Zapewnienie niezwłocznego odbierania dostępu do systemów informatycznych byłym pracownikom Urzędu.**
4. **Zapewnienie przeprowadzania okresowego audytu wewnętrznego w zakresie bezpieczeństwa informacji.**

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 Katowicach. 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.

Katowice, 6 listopada 2020 r.

Kontroler
Magdalena Śleziak
Inspektor kontroli państwowej

Najwyższa Izba Kontroli
Delegatura w Katowicach

.....