NAJWYŻSZA IZBA KONTROLI
Departament Administracji Publicznej

KAP.410.005.03.2018
P/18/006

WYSTĄPIENIE POKONTROLNE

NAJWYŻSZA IZBA KONTROLI
ul. Filtrowa 57, 02-056 Warszawa
T +48 22 444 53 08, F +48 22 444 52 52
kap@nik.gov.pl
Adres korespondencyjny: Skr. poczt. P-14, 00-950 Warszawa 1

I. Dane identyfikacyjne kontroli

Numer i tytuł kontroli

P/18/006 – Zarządzanie bezpieczeństwem informacji w jednostkach samorządu terytorialnego

Jednostka przeprowadzająca kontrolę

Najwyższa Izba Kontroli
Departament Administracji Publicznej

Kontroler

Kamil Obłodecki, specjalista kontroli państwowej, upoważnienie do kontroli nr KAP/57/2018 z dnia 28 maja 2018 r.

(dowód: akta kontroli str. 1)

Jednostka kontrolowana

Urząd Miasta Józefowa, ul. Kardynała Wyszyńskiego 1, 05-420 Józefów (dalej: Urząd)

Kierownik jednostki kontrolowanej

Stanisław Kruszewski, Burmistrz Miasta Józefowa od 3 listopada 1998 r. (dalej: Burmistrz Miasta)

(dowód: akta kontroli str. 2-5)

II. Ocena kontrolowanej działalności

Ocena ogólna

Najwyższa Izba Kontroli ocenia pozytywnie mimo stwierdzonych nieprawidłowości[1] działalność Burmistrza Miasta Józefów w zakresie zarządzania bezpieczeństwem informacji.

Uzasadnienie oceny ogólnej

Powyższą ocenę uzasadnia fakt, że pomimo przyjęcia i wdrożenia rozwiązań organizacyjno-technicznych w celu zapewnienia bezpieczeństwa informacji, w działalności Urzędu stwierdzono nieprawidłowości, które w ocenie NIK wpływały na zapewnienie bezpieczeństwa informacji.

Pozytywnie należy ocenić, że w Urzędzie od 22 czerwca 2018 r. wdrożono System Zarządzania Bezpieczeństwem Informacji, na który składała się m.in. Polityka Bezpieczeństwa Informacji oraz szczegółowe procedury i instrukcje. Pracownicy Urzędu zostali zapoznani z obowiązującymi w Urzędzie wymogami w zakresie bezpieczeństwa informacji. Burmistrz powołał Inspektora Ochrony Danych zgodnie z wymogami określonymi w art. 37 ust. 1 *rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (ogólne rozporządzenie o ochronie danych)*[2] (dalej: RODO). Osoba pełniąca tą funkcję, a także inni pracownicy odpowiedzialni za bezpieczeństwo informacji, posiadali odpowiednie przygotowanie merytoryczne i doświadczenie zawodowe. Komputery Urzędu zostały zabezpieczone przed szkodliwym oprogramowaniem oraz, poza jednym przypadkiem, możliwością instalowania dowolnego oprogramowania przez

[1] Najwyższa Izba Kontroli stosuje 3-stopniową skalę ocen: pozytywna, pozytywna mimo stwierdzonych nieprawidłowości, negatywna.

[2] Dz. Urz. UE L 119 z 04.05.2016, s. 1.

użytkowników. Prowadzono aktualizację oprogramowania systemowego oraz sporządzano i weryfikowano prawidłowość kopii zapasowych. Spełniono również wymóg przechowywania kopii poza miejscem ich wytwarzania. Urząd posiadał także pełną informację o wykorzystywanych zasobach informatycznych Urzędu, obejmującą ich rodzaj i konfigurację.

W działalności Urzędu stwierdzono nieprawidłowości, w tym m.in.:

- do 21 czerwca 2018 r. w Urzędzie nie opracowano i nie wdrożono systemu zarządzania bezpieczeństwem informacji, w szczególności polityki bezpieczeństwa informacji, co było niezgodne z § 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*[3] (dalej: rozporządzenie KRI),
- jeden z 13 objętych badaniem pracowników Urzędu posiadał uprawnienia administratora systemu, pomimo iż nie był pracownikiem służb informatycznych, co było niezgodne z § 20 ust. 2 pkt 4 rozporządzenia KRI (nieprawidłowość została usunięta w trakcie kontroli),
- jeden spośród sześciu pracowników, którzy w okresie od 1 czerwca 2017 r. do 27 lipca 2018 r. zakończyli zatrudnienie w Urzędzie, posiadał aktywne uprawnienia dostępu do systemu informatycznego, co było niezgodne z § 20 ust. 2 pkt 5 rozporządzenia KRI,
- nie przestrzegano przyjętych wymagań dotyczących haseł dostępu do systemów informatycznych, co było niezgodne z § 20 ust. 2 pkt 7 rozporządzenia KRI (nieprawidłowość została usunięta w trakcie kontroli),
- w trzech z czterech badanych umów serwisowych, zawartych z podmiotami zewnętrznymi, nie zawarto zapisów mówiących o zobowiązaniu wykonawcy do zachowania w tajemnicy informacji do jakich może mieć dostęp w związku z realizacją przedmiotu umowy, co było niezgodne z § 20 ust. 2 pkt 10 rozporządzenia KRI,
- nie przeprowadzono w 2017 r. audytu bezpieczeństwa informacji, co było niezgodne z § 20 ust. 2 pkt 14 rozporządzenia KRI,
- do 21 czerwca 2018 r. nie uregulowano zasad i procedur korzystania przez pracowników ze sprzętu i urządzeń przenośnych Urzędu poza jego siedzibą, co było niezgodne z § 20 ust. 2 pkt 8 rozporządzenia KRI (nieprawidłowość została usunięta w trakcie kontroli).

Najwyższa Izba Kontroli zwróciła uwagę, że inne zadania i obowiązki wykonywane przez osobę pełniącą jednocześnie w Urzędzie funkcję Inspektora Ochrony Danych (dalej: IOD) i kierownika Referatu Informatyki mogą powodować konflikt interesów, o którym mowa w art. 38 ust. 6 RODO.

Ponadto, na podstawie wyników kontroli NIK sformułowała uwagi, dotyczące m.in. nieprowadzenia okresowych analiz ryzyka utraty integralności, dostępności lub poufności informacji.

[3] Dz. U. z 2017 r. poz. 2247.

III. Opis ustalonego stanu faktycznego

1. Organizacja bezpieczeństwa informacji.

Opis stanu faktycznego

1.1. Do 21 czerwca 2018 r. w Urzędzie Miasta Józefowa nie było opracowanego i wdrożonego systemu zarządzania bezpieczeństwem informacji, o którym mowa w § 20 ust. 1 w zw. z ust. 3 rozporządzenia KRI (dalszy opis w części *Ustalona nieprawidłowość*, str. 6).

(dowód: akta kontroli str. 6-155)

1.2. W okresie objętym kontrolą[4] w Urzędzie obowiązywały dokumenty dotyczące bezpieczeństwa przetwarzania danych osobowych. Do 21 czerwca 2018 r. były to dokumenty wprowadzone zarządzeniem nr 25 Burmistrza Miasta Józefowa z dnia 14 marca 2016 r.:

- *Polityka Bezpieczeństwa Informacji w Zakresie Przetwarzania Danych Osobowych w Urzędzie Miasta Józefów,*
- *Instrukcja Zarządzania Systemami Informatycznymi Służącymi do Przetwarzania Danych Osobowych,*
- *Instrukcja postępowania w sytuacji naruszenia ochrony danych osobowych.*

W dniu 22 czerwca 2018 r. na mocy zarządzenia nr 66/2018 Burmistrz Miasta Józefowa ustanowił politykę bezpieczeństwa informacji i ochrony danych osobowych (dalej: PBI).

Wszyscy pracownicy Urzędu zaangażowani w proces przetwarzania danych osobowych zostali zapoznani z obowiązującymi w Urzędzie do 21 czerwca 2018 r. uregulowaniami dotyczącymi bezpieczeństwa danych osobowych, a następnie z ustanowioną z dniem 22 czerwca 2018 r. PBI.

(dowód: akta kontroli str. 6-155, 164-166)

1.3. Na podstawie zarządzeń Burmistrza[5] zostali wyznaczeni pracownicy Urzędu na stanowiska odpowiedzialne za bezpieczeństwo informacji, tj. Administratora Bezpieczeństwa Informacji (do 24 maja 2018 r.) oraz Inspektora Ochrony Danych (od 25 maja 2018 r.). W zarządzeniach zostały określone podstawowe zakresy obowiązków na tych stanowiskach. Powyższe stanowiska podlegały bezpośrednio Burmistrzowi. Ponadto, w Urzędzie funkcjonował Referat Informatyki, w zakresie którego leżały m.in. sprawy związane z rozwojem, wdrażaniem i eksploatacją systemów informatycznych. Pracownicy Referatu dysponowali odpowiednimi kompetencjami (wykształcenie, praktyka zawodowa), umożliwiającymi prawidłowe wykonywanie powierzonych im zadań.

(dowód: akta kontroli str. 156-161)

[4] Od 1 czerwca 2017 r. do 27 lipca 2018 r.

[5] 1. Zarządzenie nr 57/2018 Burmistrza Miasta Józefowa z dnia 22 maja 2018 r. w sprawie wyznaczenia Inspektora Ochrony Danych Osobowych w Urzędzie Miasta Józefowa. 2. Zarządzenie nr 88/2015 Burmistrza Miasta Józefowa z dnia 25 czerwca 2015 r. w sprawie powołania Administratora Bezpieczeństwa Informacji.

1.4. Zgodnie z wymogami art. 37 ust. 1 RODO Burmistrz Miasta wyznaczył IOD. Dysponował on odpowiednimi kwalifikacjami do pełnienia tej funkcji.

(dowód: akta kontroli str. 160-161)

1.5. Według *zarządzenia nr 57/2018*, IOD podlegał bezpośrednio Burmistrzowi, co było zgodne z art. 38 ust. 3 RODO, jednakże osoba wyznaczona na IOD była jednocześnie kierownikiem Referatu Informatyki. Osoba pełniąca funkcję IOD podlegała Burmistrzowi Miasta (jako Inspektor Ochrony Danych) oraz jednocześnie Sekretarzowi Miasta (jako kierownik Referatu Informatyki) - dalszy opis w części *Uwagi dotyczące badanej działalności* w pkt. 1 na str. 6.

(dowód: akta kontroli str. 160-163)

1.6. W ramach wdrożenia PBI sporządzono niżej wskazaną dokumentację, zawierającą polityki i procedury, określające m.in. szczegółowe zasady wdrożenia zabezpieczeń technicznych:

- procedurę zgłaszania i obsługi incydentów naruszeń bezpieczeństwa informacji w Urzędzie Miasta Józefowa;
- regulamin określający zasady i procedury korzystania z zasobów informatycznych w Urzędzie Miasta Józefowa;
- instrukcję zarządzania systemami informatycznymi.

(dowód: akta kontroli str. 84-138)

1.7. PBI została udostępniona pracownikom do wglądu poprzez stronę intranetową Urzędu – *ABC pracownika Urzędu Miasta Józefowa*. Regulacje wewnętrzne, stanowiące dokumenty wykonawcze PBI, były dostępne dla wszystkich pracowników Urzędu, nie tylko dla osób odpowiedzialnych za realizację poszczególnych czynności wymaganych tymi dokumentami (dalszy opis w części *Uwagi dotyczące badanej działalności* w pkt. 2 na str. 6).

(dowód: akta kontroli str. 164-166)

1.8. W Urzędzie zidentyfikowano zbiory przetwarzanych danych podlegające zabezpieczeniu i ujęto je w *rejestrze zbiorów danych osobowych przetwarzanych przez Administratora Danych Osobowych w Urzędzie Miasta Józefowa*.

(dowód: akta kontroli str. 167-179)

1.9. Inwentaryzacja zasobów informatycznych, o której mowa w § 20 ust. 2 pkt 2 rozporządzenia KRI, rozumiana jako stałe posiadanie aktualnych informacji w zakresie posiadanego sprzętu informatycznego oraz jego konfiguracji, była prowadzona przy pomocy systemu OCS Inventory. Baza zawierała m.in. dane o: sprzęcie komputerowym, oprogramowaniu, urządzeniach sieciowych, drukarkach, innych urządzeniach peryferyjnych oraz mobilnych, a także o relacjach między jednostkami konfiguracyjnymi. Dane z bazy umożliwiały odtworzenie zasobów informatycznych po katastrofie lub innym zdarzeniu losowym. W wyniku badania, opartego o dobór celowy 15 użytkowanych urządzeń ustalono, że system ten nie zawierał informacji o jednym urządzeniu wielofunkcyjnym, wykorzystywanym jako

kserokopiarka (dalszy opis w części *Uwagi dotyczące badanej działalności* w pkt. 3 na str. 7).

(dowód: akta kontroli str. 180-214)

Ustalona nieprawidłowość

W działalności kontrolowanej jednostki w przedstawionym wyżej zakresie stwierdzono następującą nieprawidłowość:

W Urzędzie Miasta Józefów, w okresie od 1 czerwca 2017 r. do 21 czerwca 2018 r., nie opracowano i nie wdrożono polityki bezpieczeństwa informacji (PBI). Według wyjaśnień Krystyny Wasilewskiej – Sekretarz Miasta Józefowa - podjęto działania zmierzające do przygotowania polityki bezpieczeństwa informacji. W konsekwencji 22 czerwca 2018 r. Burmistrz Miasta Józefowa wydał *zarządzenie nr 66/2018 w sprawie wprowadzenia Polityki Bezpieczeństwa Informacji i Ochrony Danych Osobowych, Instrukcji Zarzadzania Systemami Informatycznymi oraz Procedury zgłaszania i obsługi incydentów naruszeń bezpieczeństwa informacji w Urzędzie Miasta Józefowa*.

(dowód: akta kontroli str. 6-155, 200-205)

W związku z wprowadzeniem z dniem 22 czerwca 2018 r. PBI w Urzędzie, NIK odstępuje od formułowania wniosku pokontrolnego w tym zakresie.

Uwagi dotyczące badanej działalności

1. NIK zwraca uwagę, że inne zadania i obowiązki wykonywane przez osobę pełniącą w Urzędzie funkcję IOD mogą powodować konflikt interesów, o którym mowa w art. 38 ust. 6 RODO, gdyż osoba powołana na IOD, będąc jednocześnie kierownikiem Referatu Informatyki, uczestniczy jako kierownik w określaniu celów i sposobów przetwarzania danych osobowych w Urzędzie, zatem nie spełnia wymogu określonego w ww. przepisie.

   W myśl art. 38 ust. 6 RODO, osoba wyznaczona na IOD może wykonywać inne zadania i obowiązki, jednak administrator danych (tj. Burmistrz) musi zapewnić, by takie zadania i obowiązki nie powodowały konfliktu interesów.

   Zdaniem NIK, biorąc pod uwagę art. 158 ust. 1 ustawy z dnia 10 maja 2018 r. o ochronie danych osobowych[6], gdzie wskazano, że osoba pełniąca w dniu 24 maja 2018 r. funkcję Administratora Bezpieczeństwa Informacji staje się IOD i pełni swoją funkcję do dnia 1 września 2018 r., po tym terminie funkcja IOD powinna być powierzona osobie, której podstawowe obowiązki z racji wykonywanych zadań nie będą powodować konfliktu interesów z zadaniami IOD.

   (dowód: akta kontroli str. 160-163)

2. Procedury i instrukcje będące elementem PBI nie powinny być udostępniane wszystkim pracownikom Urzędu, ponieważ zawierają szczegółowe zasady zarządzania środowiskiem informatycznym.

[6] Dz. U. poz. 1000.

Zdaniem NIK, treść dokumentów powinna być udostępniona wyłącznie pracownikom odpowiedzialnym za realizację zadań z niego wynikających, aby uniknąć ryzyka, że informacje zawarte w tych procedurach będą wykorzystane do przełamania ustanowionych zabezpieczeń.

(dowód: akta kontroli str. 164-166)

3. NIK zwraca uwagę na konieczność ujmowania w oprogramowaniu inwentaryzacyjnym w Urzędzie (OCS Inventory) wszystkich urządzeń informatycznych wykorzystywanych w Urzędzie, w tym także urządzenia wielofunkcyjnego wykorzystywanego jako kserokopiarka.

(dowód: akta kontroli str. 180-214)

Ocena cząstkowa

Najwyższa Izba Kontroli ocenia pozytywnie, mimo stwierdzonych nieprawidłowości, działalność Burmistrza Miasta w zakresie organizacji bezpieczeństwa informacji. W Urzędzie do dnia 21 czerwca 2018 r. nie opracowano i nie wdrożono systemu zarządzania bezpieczeństwem informacji (system ten wdrożono 22 czerwca 2018 r.). Ponadto, stwierdzono, że inne zadania i obowiązki wykonywane przez osobę będącą równocześnie IOD mogą powodować konflikt interesów gdyż osoba ta jako kierownik Referatu Informatyki uczestniczy w określaniu celów i sposobów przetwarzania danych osobowych w Urzędzie.

W okresie objętym kontrolą zidentyfikowano zbiory danych Urzędu podlegające zabezpieczeniu i prowadzono pełną inwentaryzację zasobów informatycznych. Pracownicy Urzędu zostali zapoznani z obowiązującymi w Urzędzie wymogami w zakresie bezpieczeństwa informacji. W Urzędzie wyznaczeni byli pracownicy Urzędu na stanowiska odpowiedzialne za bezpieczeństwo informacji, tj. Administratora Bezpieczeństwa Informacji oraz IOD.

2. Wdrożone i wykorzystywane rozwiązania organizacyjne i techniczne zapewniające bezpieczeństwo informacji

Opis stanu faktycznego

2.1. Uprawnienia użytkowników 11 komputerów stacjonarnych i dwóch laptopów objętych oględzinami nie pozwalały (poza jednym przypadkiem) na zainstalowanie nieautoryzowanego oprogramowania. Było to zgodne z § 20 ust. 2 pkt 4 rozporządzenia KRI (dalszy opis w części *Ustalone nieprawidłowości* w pkt. 1 na str. 11).

(dowód: akta kontroli str. 215-216)

2.2. Analiza zadań służbowych realizowanych przez 15 pracowników Urzędu wykazała, że pracownicy ci posiadają uprawnienia do pracy w systemach informatycznych adekwatnie do realizowanych zadań. Powyższe działania były zgodne z § 20 ust. 2 pkt 4 rozporządzenia KRI.

(dowód: akta kontroli str. 219)

2.3. Kontrolą objęto uprawnienia dostępu do systemów informatycznych 6 wybranych osób, które w okresie od 1 czerwca 2017 r. do 27 lipca 2018 r. zakończyły zatrudnienie w Urzędzie. Stwierdzono, że poza jednym przypadkiem,

na bieżąco odbierano uprawnienia dostępu do systemów informatycznych (dalszy opis w części *Ustalone nieprawidłowości* w pkt. 2 na str. 11).

(dowód: akta kontroli str. 220-222)

2.4. W ramach kontroli zabezpieczeń technicznych wykorzystywanych w trzech systemach informatycznych zbadano wdrożone w nich zasady dotyczące haseł. Badaniu poddano systemy przeznaczone do obsługi spraw związanych z:

- podatkami lokalnymi, księgowością budżetową, księgowaniem zdarzeń gospodarczych;
- świadczeniami rodzinnymi, wychowawczymi oraz alimentacyjnymi;
- gospodarowaniem odpadami na terenie gminy.

W przypadku dwóch pierwszych systemów wprowadzona została polityka haseł wymuszająca na użytkownikach wprowadzenie haseł zawierających minimum osiem znaków (duże, małe litery i cyfry, a także znaki specjalne), zaś okres ważności hasła został określony na 30 dni. W jednym systemie nie było ustawionych wymagań dotyczących złożoności (siły) hasła ani okresu jego ważności (dalszy opis w części *Ustalone nieprawidłowości* w pkt. 3 na str. 12).

(dowód: akta kontroli str. 223-224, 227-242)

2.5. W trakcie oględzin stwierdzono, że ustawienie monitorów na dwóch z sześciu kontrolowanych stanowisk pracy obsługujących obywateli w zakresie ewidencji ludności, dowodów osobistych, rejestracji stanu cywilnego oraz Biura Obsługi Klientów powodowało, że dane wyświetlane na ekranie tych monitorów były widoczne dla osób nieuprawnionych, co było niezgodne z § 20 ust. 2 pkt 7 rozporządzenia KRI (dalszy opis w części *Ustalone nieprawidłowości* w pkt. 4 na str. 12).

(dowód: akta kontroli str. 243-244)

2.6. W okresie objętym kontrolą (do 21 czerwca 2018 r.) nie ustanowiono procedur gwarantujących bezpieczne przetwarzanie informacji w przypadku wykonywania czynności poza Urzędem (dalszy opis w części *Ustalone nieprawidłowości* w pkt. 5 na str. 12).

Z dniem 22 czerwca 2018 r. została ustanowiona procedura w tym zakresie. Procedura ta została określona w ramach *Instrukcji Zarządzania Systemami Informatycznymi*, stanowiącej załącznik nr 2 do *zarządzenia nr 66/2018 z dnia 22 czerwca 2018 r. w sprawie wprowadzenia Polityki Bezpieczeństwa Informacji i Ochrony Danych Osobowych, Instrukcji Zarządzania Systemami Informatycznymi oraz Procedury zgłaszania i obsługi incydentów naruszeń bezpieczeństwa informacji w Urzędzie Miasta Józefowa.*

(dowód: akta kontroli str. 105-132, 247)

2.7. W Urzędzie zostało przyjęte jednolite podejście w zakresie szyfrowania urządzeń przenośnych, w celu minimalizowania ryzyka nieuprawnionego dostępu do informacji, o czym mowa w § 20 ust. 2 pkt 9 i 11 rozporządzenia KRI.

Szyfrowaniem objęto dyski twarde laptopów, wymagane było hasło dostępowe do systemu operacyjnego oraz hasło do systemu BIOS/UEFI.

(dowód: akta kontroli str. 247-248)

2.8. W serwerowni Urzędu zapewniono odpowiednie rozwiązania w zakresie podtrzymania zasilania oraz warunków środowiskowych pracy serwerów i urządzeń sieciowych. W okresie objętym kontrolą testowano oraz serwisowano znajdujące się w pomieszczeniu zasilacze awaryjne, klimatyzator i czujnik sygnalizacji pożaru. W trakcie oględzin serwerowni ustalono, że nie był prowadzony rejestr wejść/wyjść do tego pomieszczenia, co zostało opisane w części *Uwaga w zakresie badanej działalności* na str. 13.

(dowód: akta kontroli str. 249-277)

2.9. W wyniku badania czterech[7] obowiązujących w okresie objętym kontrolą umów serwisowych z podmiotami zewnętrznymi, w zakresie świadczenia usług informatycznych na rzecz Urzędu, ustalono, że w trzech umowach dotyczących:

- serwisu oprogramowania wykorzystywanego do pracy w Urzędzie,
- prowadzenia strony Biuletynu Informacji Publicznej,
- serwisu dwóch serwerów Urzędu,

nie zawarto zapisów gwarantujących odpowiedni poziom bezpieczeństwa informacji, co stanowiło naruszenie § 20 ust. 2 pkt 10 rozporządzenia KRI (dalszy opis w części *Ustalone nieprawidłowości* w pkt. 6 na str. 12).

Umowa dotycząca utrzymania strony internetowej i poczty e-mail Urzędu zawierała zapisy w zakresie ochrony informacji powierzonych wykonawcy.

(dowód: akta kontroli str. 278-317)

2.10. Według wyjaśnień Sekretarz Miasta w przypadku oddawania sprzętu komputerowego lub jego sprzedaży wymontowuje się dyski twarde, na których przetwarzane były informacje. Dyski podlegają utylizacji w taki sposób, aby nie było możliwe odczytanie informacji na nich. W przypadku awarii serwerów naprawa dokonywana jest w Urzędzie pod nadzorem pracownika Referatu Informatyki. Wdrożona z dniem 22 czerwca 2018 r. PBI zawiera procedurę regulującą zasady przekazywania sprzętu IT poza jednostkę.

(dowód: akta kontroli str. 84-104, 324-325)

2.11. W kontrolowanej jednostce zapewniono, aby na komputerach użytkowników zainstalowany był system operacyjny objęty wsparciem producenta.

[7] 1. Umowa nr 638/2016 z dnia 21 grudnia 2017 r. w sprawie prowadzenia Biuletynu Informacji Publicznej. 2. Umowa nr 233/2018 z dnia 2 lutego 2018 r. o udostępnienie przestrzeni dyskowej serwera internetowego oraz utrzymanie strony internetowej i poczty e-mail Urzędu Miasta Józefowa. 3. Umowa serwisowa nr 1/206/2017 z dnia 10 stycznia 2017 r. dot. serwisu oprogramowania wykorzystywanego do pracy w Urzędzie. 4. Umowa Świadczenia Serwisu nr 297/2018 z dnia 30 kwietnia 2018 r. dot. dwóch serwerów Urzędu.

Na 109 zbadanych komputerów, ujętych w bazie sprzętu IT Urzędu, tylko na jednym zainstalowany był system Windows XP, który od 8 kwietnia 2014 r. nie jest wspierany przez producenta.

(dowód: akta kontroli str. 326-327)

2.12. Zasady tworzenia kopii zapasowych zbiorów danych oraz programów i narzędzi służących do ich przetwarzania zostały określone w *Instrukcji zarządzania systemami informatycznymi służącymi do przetwarzania danych osobowych* (dla okresu przed 22 czerwca 2018 r.) oraz w *Instrukcji zarządzania systemami informatycznymi* (po 22 czerwca 2018 r.). W powyższych procedurach określono terminy na sporządzanie kopii bezpieczeństwa dla poszczególnych systemów informatycznych. Kontrolą NIK objęto sporządzanie kopii zapasowych dla następujących systemów informatycznych:

- system przeznaczony do obsługi spraw związanych z podatkami lokalnymi, księgowością budżetową, księgowaniem zdarzeń gospodarczych;
- system przeznaczony do obsługi spraw związanych ze świadczeniami rodzinnymi, wychowawczymi oraz alimentacyjnymi;
- system przeznaczony do obsługi spraw związanych z gospodarowaniem odpadami na terenie gminy.

Kopie bezpieczeństwa danych powyższych systemów informatycznych tworzone były każdego dnia roboczego na macierzy dyskowej, znajdującej się w serwerowni Urzędu. Następnie dane były replikowane na taśmy magnetyczne, które były przechowywane w zamkniętym sejfie znajdującym się poza serwerownią. Kopie zapasowe były testowane każdego dnia roboczego, a raporty z wyników testu przekazywane automatycznie do kierownika Referatu Informatyki. Dostęp do kluczy do sejfu posiadają uprawnieni pracownicy. Powyższe rozwiązania i działania zapewniały zgodność z § 20 ust. 2 pkt 7 oraz ust. 2 pkt 12 lit. b i e rozporządzenia KRI.

(dowód: akta kontroli str. 328, 411-414)

2.13. Na podstawie oględzin 11 komputerów (w tym czterech laptopów) ustalono, że był na nich zainstalowany i uruchomiony program antywirusowy, który wykorzystywał aktualną na moment badania wersję bazy definicji wirusów. Było to zgodne z § 20 ust. 2 pkt 12 lit. f rozporządzenia KRI.

(dowód: akta kontroli str. 413-414)

2.14. W ramach obowiązujących w Urzędzie uregulowań (do 21 czerwca 2018 r.) nie zostały określone zasady monitorowania stanu pojemności przestrzeni dyskowej w serwerach Urzędu. W związku z wprowadzoną 22 czerwca 2018 r. procedurą monitorowania pojemności nośników zobowiązano pracowników Referatu Informatyki do codziennego monitorowania logów systemu operacyjnego, zasobów kluczowych serwerów oraz wprowadzono obowiązek informowania administratora systemów informatycznych o ryzyku przekroczenia krytycznego poziomu zajętości dysku.

Na podstawie badania trzech wybranych serwerów ustalono, że na jednym z nich tj. serwerze aplikacji, zawierającym m.in. dane z aplikacji wspierających pracę

urzędników oraz kontroler domeny, zajętość dostępnej przestrzeni dyskowej[8] wyniosła 84%. W trakcie kontroli w Urzędzie podjęto działania w zakresie archiwizacji niepotrzebnych plików. Na pozostałych dwóch serwerach objętych badaniem zajętość przestrzeni dyskowej nie przekroczyła 80%.

(dowód: akta kontroli str. 84-132, 413-414)

2.15. Według wyjaśnień Sekretarz Miasta oraz Kierownika Referatu Informatyki dokumentacja związana z wprowadzanymi zmianami w konfiguracji oprogramowania i urządzeń prowadzona jest przez Referat Informatyki. Każdorazowa aktualizacja oprogramowania odnotowywana jest w dzienniku systemowym. Informacje o zmianach w krytycznych systemach informatycznych przesyłane są przez producentów oprogramowania na adres e-mail pracownika Referatu Informatyki z wnioskiem o wykonanie aktualizacji. Zmiany dokonywane są w środowisku produkcyjnym, przy czym przed wdrożeniem zmiany tworzone są kopie bezpieczeństwa, tak aby możliwe byłoby przywrócenie oprogramowania w przypadku awarii. Proponowane zmiany są akceptowane przez pracownika Referatu Informatyki.

(dowód: akta kontroli str. 329-332)

2.16. Stosownie do art. 30 ust. 1 RODO, w Urzędzie prowadzono rejestr czynności przetwarzania danych. Rejestr zawierał informacje, o których mowa w ww. przepisie.

(dowód: akta kontroli str. 333-344)

Ustalone nieprawidłowości

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

1. Na jednym z 13 poddanych oględzinom stanowiskach komputerowych stwierdzono, że pracownik Urzędu posiadał uprawnienia administratora, mimo iż nie był administratorem systemów informatycznych. Pracownikowi temu wbrew wymogom § 20 ust. 2 pkt 4 rozporządzenia KRI, umożliwiono instalowanie dowolnego oprogramowania.

Tomasz Kowalczyk – kierownik Referatu Informatyki - wyjaśnił, że przyczyną nieprawidłowości był problem z dzierżawą uprawnień w domenie dla użytkownika. W trakcie kontroli nieprawidłowość została usunięta, w związku z tym NIK odstępuje od formułowania wniosku pokontrolnego w tym zakresie.

(dowód: akta kontroli str. 215-218)

2. Stwierdzono, że według stanu na dzień zakończenia czynności kontrolnych (27 lipca 2018 r.) jedna spośród sześciu osób, które w okresie od 1 czerwca 2017 r. do 27 lipca 2018 r. zakończyły zatrudnienie w Urzędzie, posiadała aktywne uprawnienia do systemów informatycznych Urzędu. Było to niezgodne z § 20 ust. 2 pkt 5 rozporządzenia KRI, stanowiącym że zarządzanie bezpieczeństwem informacji realizowane jest w szczególności przez zapewnienie przez kierownictwo podmiotu publicznego warunków umożliwiających realizację i egzekwowanie bezzwłocznej zmiany uprawnień, w przypadku zmiany zadań osób zaangażowanych w proces przetwarzania informacji, w tym każdorazowego usuwania kont informatycznych pracowników, którzy zakończyli zatrudnienie w Urzędzie.

[8] Partycja „Profile"

Jak wyjaśnił kierownik Referatu Informatyki, na profilu domenowym byłego pracownika uruchomione były usługi dostępu do archiwalnych danych programu przeznaczonego do elektronicznego zarządzania dokumentami. W związku z tym, jak wskazał kierownik Referatu Informatyki, zrezygnowano z usunięcia konta, przy czym zmienione zostało hasło dostępu tak aby były pracownik nie miał możliwości zalogowania się w systemie.

(dowód: akta kontroli str. 220-222)

3. W systemie informatycznym Urzędu przeznaczonym do obsługi spraw związanych z gospodarowaniem odpadami na terenie gminy, nie było ustawionych wymagań dotyczących złożoności (siły) haseł ani jego okresu ważności. Możliwe było ustanowienie przez użytkowników hasła nie spełniającego standardów bezpieczeństwa – tj. zawierającego mniej niż 8 znaków, bez okresu ważności. Było to niezgodne z § 20 ust. 2 pkt 7 rozporządzenia KRI, stanowiącym, że zarządzanie bezpieczeństwem informacji realizowane jest w szczególności przez zapewnienie przez kierownictwo podmiotu publicznego warunków umożliwiających realizację i egzekwowanie działania polegającego na zapewnieniu ochrony przetwarzanych informacji przed ich kradzieżą, nieuprawnionym dostępem, uszkodzeniami lub zakłóceniami. Według wyjaśnień kierownika Referatu Informatyki przyczyną nieustawienia wymagań dotyczących siły było przeoczenie. W toku kontroli nieprawidłowość ta została usunięta, w związku z tym NIK odstępuje od formułowania wniosku pokontrolnego w tym zakresie.

(dowód: akta kontroli str. 223-226)

4. Oględziny 6 stanowisk pracy realizujących zadania obsługi obywateli w zakresie ewidencji ludności, dowodów osobistych i rejestracji stanu cywilnego wykazały, że dwa monitory usytuowane były w sposób umożliwiający wgląd do danych przez osoby nieuprawnione. Powyższe ustawienie nie spełniało wymogów § 20 ust. 2 pkt 7 rozporządzenia KRI.

Według wyjaśnień Marzeny Szcześniak - kierownika Referatu Ewidencji Ludności - przyczyną tego stanu rzeczy były ograniczone warunki lokalowe Referatu i brak w związku z tym możliwości przestawienia monitorów.

(dowód: akta kontroli str. 243-246)

5. Do 21 czerwca 2018 r. w Urzędzie nie ustanowiono procedur gwarantujących bezpieczną pracę przy przetwarzaniu mobilnym i pracy na odległość, o których mowa w § 20 ust. 2 pkt 8 rozporządzenia KRI.

Sekretarz wyjaśniła, że od 22 czerwca 2018 r. procedura pracy na odległość została określona w Instrukcji Zarządzania Systemami Informatycznymi, stanowiącej załącznik nr 2 do Zarządzenia 66/2018 z dnia 22 czerwca 2018 r. W związku z powyższym, NIK odstępuje od formułowania wniosku pokontrolnego w tym zakresie.

(dowód: akta kontroli str. 247-248)

6. W trzech z czterech badanych umów zawartych z podmiotami zewnętrznymi, tj w:

- umowie serwisowej nr 1/206/2017 z dnia 10 stycznia 2017 r. dot. serwisu oprogramowania wykorzystywanego do pracy w Urzędzie,
- umowie nr 638/2017 z dnia 21 grudnia 2017 r. w sprawie prowadzenia Biuletynu Informacji Publicznej,
- umowie nr 297/2018 z dnia 30 kwietnia 2018 r., dot. serwisu pogwarancyjnego, usuwania zgłoszonych awarii i usterek dwóch serwerów Urzędu,

nie zawarto zapisów zobowiązujących wykonawcę do zachowania w tajemnicy informacji do jakich może mieć dostęp w związku z realizacją umowy.

Było to niezgodne z § 20 ust. 2 pkt 10 rozporządzenia KRI, stanowiącym że zarządzanie bezpieczeństwem informacji realizowane jest w szczególności przez zapewnienie przez kierownictwo podmiotu publicznego warunków umożliwiających realizację i egzekwowanie zawierania w umowach serwisowych podpisanych ze stronami trzecimi zapisów gwarantujących odpowiedni poziom bezpieczeństwa informacji.

W złożonych wyjaśnieniach Burmistrz Miasta wskazał, że zapisy gwarancyjne umów są wystarczające dla spełnienia wymogów rozporządzenia KRI. Zdaniem NIK, zobowiązanie gwarancyjne nie regulują kwestii bezpieczeństwa informacji. W zawieranych umowach powinny być klauzule gwarantujące Urzędowi zachowanie w tajemnicy wszelkich informacji do jakich wykonawca może mieć dostęp w związku z realizowaniem umowy (z wyjątkiem informacji, których podanie wymagane jest obowiązującymi przepisami).

(dowód: akta kontroli str. 278-323)

Uwaga dotycząca badanej działalności

NIK zwraca uwagę na potrzebę prowadzenia ewidencji wejść i wyjść do serwerowni, co zdaniem NIK wpłynie na zwiększenie bezpieczeństwa infrastruktury IT zlokalizowanej w tym pomieszczeniu.

(dowód: akta kontroli str. 249-268)

Ocena cząstkowa

Najwyższa Izba Kontroli ocenia pozytywnie mimo stwierdzonych nieprawidłowości działalność Burmistrza Miasta w obszarze wdrożenia i wykorzystywania rozwiązań organizacyjnych i technicznych zapewniających bezpieczeństwo informacji. Komputery Urzędu zostały zabezpieczone programem antywirusowym przed szkodliwym oprogramowaniem oraz przed możliwością instalowania dowolnego oprogramowania przez większość użytkowników. W Urzędzie prowadzono na bieżąco aktualizację oprogramowania systemowego oraz sporządzano i weryfikowano prawidłowość kopii zapasowych. Spełniono również wymóg przechowywania kopii zapasowych poza miejscem ich wytwarzania. W powyższym zakresie nieprawidłowości dotyczyły m.in:

- nieuregulowania (do 21 czerwca 2018 r.) zasad i procedur korzystania przez pracowników ze sprzętu i urządzeń przenośnych Urzędu poza jego siedzibą (nieprawidłowość została usunięta w trakcie kontroli),;
- braku wdrożenia wymagań dotyczących złożoności (siły) hasła ani jego okresu ważności dla systemu przeznaczonego do obsługi spraw związanych z gospodarowaniem odpadami na terenie gminy (nieprawidłowość została usunięta w trakcie kontroli)*;*
- ustawienia dwóch monitorów objętych badaniem w ten sposób, że dane wyświetlane na ekranach były widoczne dla osób nieuprawnionych.

– nieuwzględnienia w trzech z czterech badanych umów z podmiotami zewnętrznymi, świadczącymi usługi informatyczne dla Urzędu, zapisów o zachowaniu w tajemnicy informacji uzyskanych/przetwarzanych w związku z jej realizacją.

3. Działania w celu zapobiegania incydentom bezpieczeństwa

Opis stanu faktycznego

3.1. W dniu 24 maja 2016 r. przeprowadzona została przez administratora danych osobowych analiza ryzyka utraty poufności, integralności i rozliczalności systemów informatycznych, o których mowa w § 20 ust. 2 pkt 3 rozporządzenia KRI. W okresie od 2017 r. do dnia zakończenia kontroli w Urzędzie nie prowadzono analiz w tym zakresie (dalszy opis w części *Uwaga dotycząca badanej działalności* na str. 15*).*

(dowód: akta kontroli str. 345-364)

3.2. W okresie objętym kontrolą w Urzędzie wdrożone były procedury wewnętrzne zgłaszania i obsługi incydentów naruszenia bezpieczeństwa informacji oraz danych osobowych. Ustanowiony został rejestr incydentów i zagrożeń, w którym na dzień zakończenia czynności kontrolnych wprowadzono trzy zapisy. W przypadku dwóch incydentów kierownik Referatu Informatyki dokonał ich zgłoszenia do Rządowego Zespołu Reagowania na Incydenty Komputerowe. Powyższe było zgodne z wymogami § 20 ust. 2 pkt 13 rozporządzenia KRI.

(dowód: akta kontroli str. 42-43, 79-82, 133-138, 370-376)

3.3. W 2016 r. odbyło się szkolenie dla 90 pracowników Urzędu, które dotyczyło m.in. zabezpieczenia danych osobowych przetwarzanych w postaci papierowej i elektronicznej, bezpieczne przechowywanie danych, niszczenie danych, ograniczenia dostępu do obszaru przetwarzania danych osobowych, bezpieczne korzystanie z komputerów, zasady tworzenia haseł i loginów, a także bezpieczne korzystanie z systemów informatycznych. Według wyjaśnień Sekretarz Miasta, w 2018 r. w Urzędzie planowane jest przeprowadzenie szkolenia dla pracowników z zakresu bezpieczeństwa informacji. Urząd zapewnił szkolenia dla 27 pracowników Urzędu (w tym dla Sekretarz Miasta oraz kierowników referatów Urzędu) z zakresu wymogów RODO.

(dowód: akta kontroli str. 365-369)

3.4. W 2017 r. w Urzędzie nie został przeprowadzony audyt z zakresu bezpieczeństwa informacji, co było niezgodne z § 20 ust. 2 pkt 14 rozporządzenia KRI (dalszy opis w części *Ustalona nieprawidłowość* na str. 14).

(dowód: akta kontroli str. 377-392)

3.5. W związku z art. 32 ust. 1 RODO przeprowadzono analizę procesów przetwarzania danych osobowych w Urzędzie.

(dowód: akta kontroli str. 393-410)

Ustalona nieprawidłowość

W działalności kontrolowanej jednostki w przedstawionym wyżej zakresie stwierdzono następującą nieprawidłowość:

W 2017 r. w Urzędzie nie został przeprowadzony audyt z zakresu bezpieczeństwa informacji. Było to niezgodne z § 20 ust. 2 pkt 14 rozporządzenia KRI, który stanowi, że zarządzanie bezpieczeństwem informacji realizowane jest w szczególności przez zapewnienie przez kierownictwo podmiotu publicznego okresowego audytu wewnętrznego w zakresie bezpieczeństwa informacji, nie rzadziej niż raz na rok. Według wyjaśnień Burmistrza Miasta w 2017 r. przeprowadzone zostały czynności sprawdzające z audytu *Bezpieczeństwo danych w systemie informatycznym, zakres i jakość obsługi zadań przez systemy informatyczne*. Rekomendacja i zalecenia wydane przez audytora w wyniku przeprowadzonych czynności były, według wyjaśnień Burmistrza Miasta, uwzględniane przy opracowywaniu i wdrażaniu oraz aktualizacji dokumentów i procedur związanych z bezpieczeństwem. Burmistrz wyjaśnił, że w dniach 20 kwietnia – 17 maja 2018 r. przeprowadzono audyt w zakresie bezpieczeństwa pozyskiwania i przetwarzania danych osobowych.

W opinii NIK, czynności sprawdzających nie można traktować jako przeprowadzenia okresowego audytu wewnętrznego w zakresie bezpieczeństwa informacji, gdyż ich zakres odnosi się wyłącznie do weryfikacji stanów nieprawidłowych, stwierdzonych w wyniku audytu z 2016 r., a przeprowadzony w 2018 r. audyt dotyczył wyłącznie danych osobowych i był związany z przygotowaniem Urzędu do spełnienia wymagań RODO. Powyższych działań nie można zatem traktować jako wypełnienie obowiązku wynikającego z § 20 ust. 2 pkt 14 rozporządzenia KRI.

(dowód: akta kontroli str. 377-392)

Uwaga dotycząca badanej działalności

NIK zwraca uwagę na konieczność dokonywania cyklicznych analiz ryzyka utraty poufności, integralności i rozliczalności systemów informatycznych, gdyż pozwala to na identyfikację istotnych ryzyk i umożliwia ustanowienie zabezpieczeń ograniczających możliwość ich wystąpienia.

(dowód: akta kontroli str. 345-364)

Ocena cząstkowa

Najwyższa Izba Kontroli ocenia negatywnie działalność Burmistrza Miasta w zakresie zapobiegania incydentom bezpieczeństwa informacji, ze względu na nieprzeprowadzenie w 2017 r. audytu bezpieczeństwa informacji, co było niezgodne z § 20 ust. 2 pkt 14 rozporządzenia KRI. W Urzędzie nie prowadzono także okresowych analiz ryzyka utraty integralności, dostępności lub poufności informacji.

NIK pozytywnie ocenia, że Burmistrz Miasta zapewnił szkolenia pracownikom zaangażowanym w proces przetwarzania danych osobowych oraz że opracowano w Urzędzie i wdrożono procedury zgłaszania incydentów z zakresu bezpieczeństwa informacji oraz danych osobowych.

IV. Wnioski

Wnioski pokontrolne

Przedstawiając powyższe oceny i uwagi wynikające z ustaleń kontroli, Najwyższa Izba Kontroli, na podstawie art. 53 ust. 1 pkt 5 ustawy z dnia 23 grudnia 1994 r. o Najwyższej Izbie Kontroli[9], wnosi o:

1. Zapewnienie, aby monitory pracowników obsługujących klientów w Referacie Ewidencji Ludności były zabezpieczone w taki sposób, aby nie był możliwy wgląd osób nieuprawnionych do danych wyświetlanych na monitorach.
2. Uwzględnianie w umowach serwisowych zawieranych z podmiotami zewnętrznymi zapisów gwarantujących odpowiedni poziom bezpieczeństwa informacji.
3. Zapewnienie prowadzenia nie rzadziej niż raz na rok okresowego audytu wewnętrznego z zakresu bezpieczeństwa informacji.

[9] Dz. U. z 2017 r. poz. 524, ze zm.

V. Pozostałe informacje i pouczenia

Prawo zgłoszenia zastrzeżeń

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

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 Departamentu Administracji Publicznej Najwyższej Izby Kontroli.

Obowiązek poinformowania NIK o sposobie wykorzystania uwag i wykonania wniosków

Zgodnie z art. 62 ustawy o NIK proszę o poinformowanie Najwyższej Izby 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.

Warszawa, dnia …… sierpnia 2018 r.

Najwyższa Izba Kontroli
Departament Administracji Publicznej

Kontroler
Kamil Obłodecki
Specjalista kontroli państwowej

.....
podpis

Dyrektor
Bogdan Skwarka

.....
Podpis