NAJWYŻSZA IZBA KONTROLI
Delegatura w Białymstoku

LBI.410.023.12.2017
P/17/062

02268517

WYSTĄPIENIE POKONTROLNE

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

I. Dane identyfikacyjne kontroli

Numer i tytuł kontroli	P/17/062 – Bezpieczeństwo elektronicznych zasobów informacyjnych w jednostkach samorządu terytorialnego w województwie podlaskim
Jednostka przeprowadzająca kontrolę	Najwyższa Izba Kontroli Delegatura w Białymstoku
Kontrolerzy	Tomasz Pomian – główny specjalista kontroli państwowej, upoważnienie do kontroli nr LBI/165/2017 z 27 listopada 2017 r. (dowód: akta kontroli str. 1-2)
Jednostka kontrolowana	Urząd Miejski w Szczuczynie, Plac 1000-lecia 23, 19-230 Szczuczyn (zwany dalej: „Urzędem")
Kierownik jednostki kontrolowanej	Artur Kuczyński – Burmistrz Szczuczyna[1] (dowód: akta kontroli str. 3)

II. Ocena kontrolowanej działalności[2]

Ocena ogólna

Najwyższa Izba Kontroli ocenia pozytywnie mimo stwierdzonych nieprawidłowości zapewnienie przez Urząd właściwej ochrony elektronicznych zasobów informacyjnych przed nieuprawnionym dostępem, przejęciem lub zniszczeniem[3].

Uzasadnienie oceny ogólnej

Pozytywna ocena wynika w szczególności z wystarczającego poziomu zabezpieczeń odpowiedzialnych za autoryzację dostępu do sieci Urzędu, opracowania dokumentacji dotyczącej ochrony danych osobowych oraz sposobu przechowywania i zabezpieczenia tych danych, który odpowiadał przepisom oraz przyjętym procedurom.

Stwierdzono również nieprawidłowości, polegające w szczególności na:

- nieanalizowaniu i niezabezpieczeniu przed modyfikacją lub zniszczeniem logów systemów operacyjnych komputerów,
- nieprzeprowadzeniu okresowych analiz ryzyka utraty integralności, dostępności lub poufności informacji,
- niewywiązaniu się z obowiązku zgłoszenia GIODO[4] do zarejestrowania pięciu z 36 przetwarzanych w Urzędzie zbiorów danych osobowych,
- nierealizowaniu zadań określonych w art. 36a ust. 2 ustawy z dnia 29 sierpnia 1997 r. o ochronie danych osobowych[5], tj. prowadzenia rejestru zawierającego wykaz zbiorów danych osobowych przetwarzanych przez ABI[6] oraz planu sprawdzeń zgodności przetwarzania danych osobowych z przepisami o ochronie tych danych, wymaganego § 3 ust. 5 rozporządzenia Ministra Administracji Cyfryzacji z dnia 11 maja 2015 r. w sprawie trybu i sposobu realizacji zadań w celu zapewnienia przestrzegania przepisów o ochronie danych osobowych przez administratora bezpieczeństwa informacji[7],
- nieprowadzeniu corocznych audytów wewnętrznych z zakresu bezpieczeństwa informacji, o których mowa w rozporządzeniu 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[8].

---

[1] Od 2010 roku.
[2] Najwyższa Izba Kontroli stosuje 3-stopniową skalę ocen: pozytywna, pozytywna mimo stwierdzonych nieprawidłowości, negatywna.
[3] Okres objęty kontrolą: od 1 stycznia 2016 r. do dnia zakończenia czynności kontrolnych oraz działania wcześniejsze mające wpływ na kontrolowaną działalność.
[4] Generalny Inspektor Ochrony Danych Osobowych („GIODO").
[5] Dz. U. z 2016 r. poz. 922.
[6] Administrator Bezpieczeństwa Informacji („ABI").
[7] Dz. U. z 2015 r. poz. 745. Rozporządzenie zwane dalej: „rozporządzeniem w sprawie sposobu realizacji zadań ABI".
[8] Dz. U. z 2017 r. poz. 2247. Rozporządzenie zwane dalej: „rozporządzeniem KRI".

III. Opis ustalonego stanu faktycznego

Opis stanu faktycznego

1. Skuteczność przyjętych rozwiązań dotyczących zabezpieczenia dostępu do poszczególnych systemów informatycznych i usług sieciowych przed nieuprawnionym dostępem, przejęciem lub zniszczeniem danych

1.1. System informatyczny Urzędu zbudowany jest w architekturze gwiazdy. Sieć jest zarządzana przez domenę Windows. Centralną jednostką sieci jest serwer pracujący na systemie operacyjnym Microsoft Windows Serwer 2012, na którym posadowiono kontroler domeny. Drugim serwerem obsługującym sieć LAN jest maszyna, na której zainstalowano serwer plików i serwer bazy danych. Równolegle, bez podłączenia do sieci LAN Urzędu, działają trzy serwery – serwer Dziennika Elektronicznego (PPE – Podlaska Platforma Edukacyjna), serwer elektronicznego obiegu dokumentów (EZD) oraz powiązany z nim serwer określany mianem „szyny komunikacyjnej". Wymienione urządzenia, wraz z urządzeniami sieciowymi, zostały umieszczone w klimatyzowanej i wydzielonej serwerowni, która dostępna była tylko uprawnionemu personelowi.

Sieć komputerowa w Urzędzie zarządzana jest przez router ASUS RT-N184. Równolegle do wspomnianego routera pracuje router CISCO, obsługujący serwery EZD, który administrowany jest przez Urząd Marszałkowski Województwa Podlaskiego („UMWP"). Monitorowanie pracy wspomnianego urządzenia leży po stronie Urzędu Marszałkowskiego. Do tego celu zestawiono VPN do UMWP.

Dostęp do Internetu realizowany jest poprzez łącze światłowodowe. Sieć odseparowana jest od Internetu firewallem, stanowiącym integralną część routerów ASUS i CISCO. Sieć zbudowana została na stałej adresacji IP, bez wsparcia protokołu DHCP i bez filtracji MAC adresów urządzeń sieciowych. (dowód: akta kontroli str. 4-9)

Do prowadzenia zbiorów danych osobowych w wersji elektronicznej wykorzystywanych było 11 systemów informatycznych, tj.: SRP ŹRÓDŁO, SELWIN, EMUiA, SIO, CEIDG, EZD, Fiskus (Gospodarka odpadami), Podatki (Pakiet), Besti@, QNT (Pakiet), Internet Banking oraz oprogramowanie biurowe – arkusze programu MS-Word i MS-Excel.
(dowód: akta kontroli str. 10-22)

W budynku Urzędu pracowało 25 komputerów (24 stacje robocze i laptop), z tego 23 wchodziły w skład sieci LAN, jeden służył do obsługi aplikacji ŹRÓDŁO (aplikacja do obsługi Systemu Rejestrów Państwowych), a laptop pełnił funkcję urządzenia umożliwiającego wyświetlanie prezentacji w sali konferencyjnej. Na wszystkich zainstalowano system Windows 10 Pro.

Oględziny wszystkich 22 komputerów wykorzystywanych do przetwarzania danych osobowych wykazały m.in., że:

- na każdym urządzeniu dostęp do systemu operacyjnego możliwy był jedynie po wprowadzeniu nazwy użytkownika i hasła[9],
- comiesięczna zmiana hasła wymuszana była w sposób automatyczny,
- we wszystkich komputerach zapewniono bieżącą aktualizację systemów operacyjnych,
- we wszystkich jednostkach skonfigurowano wygaszacz ekranu, uruchamiany po upływie pięciu minut (powrót do systemu operacyjnego wymagał podania loginu i hasła użytkownika),
- nie stwierdzono przypadków wykorzystywania jednego konta użytkownika systemu operacyjnego przez więcej niż jedna osobę. (dowód: akta kontroli str. 10-22)

1.2. W latach 2016 – 2017 w Urzędzie nie przeprowadzano okresowych analiz ryzyka utraty integralności, dostępności lub poufności informacji, co szerzej opisano w dalszej części wystąpienia pokontrolnego, w sekcji „Ustalone nieprawidłowości".
(dowód: akta kontroli str. 56)

---

[9] O złożoności odpowiadającej warunkom określonym w rozporządzeniu Ministra Spraw Wewnętrznych i Administracji z dnia 29 kwietnia 2004 r. w sprawie dokumentacji przetwarzania danych osobowych oraz warunków technicznych i organizacyjnych, jakim powinny odpowiadać urządzenia i systemy informatyczne do przetwarzania danych osobowych (Dz. U. Nr 100, poz. 1024), zwanym dalej: „rozporządzeniem w sprawie dokumentacji oraz warunków technicznych".

1.3. Według stanu na 12 stycznia 2018 r., wszyscy pracownicy Urzędu zaangażowani byli w proces przetwarzania danych osobowych w stopniu adekwatnym do realizowanych zadań, wynikających z ich zakresów obowiązków. Oględziny wszystkich komputerów będących w administracji Urzędu wykazały, że wydzielono konta administratora i użytkownika (bez uprawnień administracyjnych), które zostały zabezpieczone hasłem. Zastosowano okresowe wymuszenie zmiany hasła. Użytkownicy komputerów nie posiadali uprawnienia do instalacji oprogramowania, zmiany uprawnień czy usuwania plików systemowych. Wszystkie zbadane komputery posiadały aktualne systemy operacyjne, bazy zagrożeń aplikacji bezpieczeństwa i oprogramowanie specjalistyczne. Aktualizacje odbywały się automatycznie, zgodnie z harmonogramem założonym przez ich producentów. (dowód: akta kontroli str. 4-22)

1.4. Ustalenia biegłego z zakresu bezpieczeństwa systemów informatycznych (powołanego przez NIK), wskazują że w Urzędzie nie był prowadzony zbiorczy rejestr dostępu do systemu w formie elektronicznej. Każda z końcówek klienckich zapisywała logi związane ze swoją pracą. Tryb zarządzania logami (ich zawartość i czas przechowywania) był zgodny z ustawieniami domyślnymi przewidzianymi przez producenta, router ASUS zapisywał na serwerze swoje logi na bieżąco. Logi te raz w miesiącu zgrywano na dysk przenośny. Nie znany był zakres ustawień routera CISCO, gdyż był on administrowany poza Urzędem. Informacje zawarte w logach nie były przetwarzane automatycznie przez administratora sytemu. Logi routera, serwera i aplikacji na nim działających zabezpieczono przed dostępem użytkowników systemu. Szerzej nieprawidłowości w zakresie monitorowania dostępu do systemu opisano w dalszej części wystąpienia pokontrolnego, w sekcji „Ustalone nieprawidłowości". (dowód: akta kontroli str. 4-9)

1.5. Ustalenia biegłego wskazują, że wszystkie komputery miały założone konto administratora i użytkownika. Każde z nich zabezpieczono hasłem. Wdrożona była procedura okresowej zmiany hasła. Urządzenia sieciowe chronione były przed nieautoryzowanym fizycznym dostępem, poprzez umieszczenie ich w zamkniętej serwerowni. Urządzenia pracujące w serwerowni zabezpieczono hasłem, co wyklucza nieautoryzowany dostęp do nich. Na terenie Urzędu nie była uruchomiona sieć WI-FI. Do sieci LAN nie był zestawiony VPN. (dowód: akta kontroli str. 4-9)

1.6. W Urzędzie nie wprowadzono regulacji umożliwiających wykorzystanie przez pracowników prywatnego sprzętu komputerowego do pracy nad zadaniami powierzonymi w ramach obowiązków służbowych. Biegły stwierdził, że konfiguracja sieciowa umożliwiała podłączenie do infrastruktury jednostki sprzętu (laptopy, telefony, tablety) niestanowiącego własności pracodawcy. Informacje o podłączeniu do komputerów nośników pamięci (np. pendrive lub dysk przenośny) były domyślnie zapisywane w logach systemu komputerowego. Dostęp do zasobów sieciowych uwierzytelniany był na poziomie użytkownika. (dowód: akta kontroli str. 4-9)

1.7. W okresie objętym kontrolą w Urzędzie nie wykryto przypadków nieautoryzowanego działania związanego z przetwarzaniem informacji. Nie wystąpiła również konieczność przywrócenia danych z wykonanych kopii bezpieczeństwa. (dowód: akta kontroli str. 56)

1.8. Biegły stwierdził, że w Urzędzie nie przewidziano zdalnego dostępu do zasobów sieci lokalnej przez pracowników. Na routerze CISCO zestawiony był VPN do sieci UMWP. Zdaniem biegłego obawy budzić może wykorzystanie aplikacji pulpitu zdalnego TeamViewer, której działanie nie było ewidencjonowane, co szerzej opisano w dalszej części wystąpienia pokontrolnego, w sekcji „Ustalone nieprawidłowości". Z aplikacji tej korzystali pracownicy ZETO Białystok S.A. przy realizacji prac serwisowych. (dowód: akta kontroli str. 4-9)

1.9. Urząd, na dzień kontroli, miał zawarte z podmiotami zewnętrznymi cztery umowy w sprawie serwisu oprogramowania. W trzech z nich zawarto regulacje zobowiązujące wykonawców umów do zachowania w tajemnicy i nieudostępniania danych osobowych przekazanych przez Urząd. Ponadto wykonawcy zobowiązali się w szczególności do: [1] zastosowania środków technicznych i organizacyjnych zapewniających ochronę przetwarzania danych osobowych, a w szczególności zabezpieczenia danych przed udostępnieniem osobom nieupoważnionym, zabraniem przez osobę nieuprawnioną,

przetwarzaniem z naruszeniem ustawy, zmianą, utratą, uszkodzeniem lub zniszczeniem; [2] dopuszczenia do przetwarzania danych wyłącznie osób posiadających upoważnienia; [3] prowadzenia ewidencji osób upoważnionych do przetwarzania danych osobowych; [4] zapewnienia, aby osoby, które będą miały dostęp do danych, zachowywały je w tajemnicy. Brak tych regulacji w czwartej umowie szerzej opisano w dalszej części wystąpienia pokontrolnego, w sekcji „Ustalone nieprawidłowości".

(dowód: akta kontroli str. 23-50)

1.10. Wszystkie komputery (23) wchodzące w skład sieci lokalnej zabezpieczono dedykowanym do tego celu oprogramowaniem antywirusowym. Wszystkie komputery posiadały aktualne bazy zagrożeń[10]. Wprawdzie dostęp do sieci lokalnej kontrolowany był przez firewall zainstalowany na routerze ASUS, to – zdaniem biegłego – wdrożenie modułu centralnego zarządzania oprogramowaniem bezpieczeństwa pozwoliło by na znacznie większą kontrolę nad działaniem systemu. (dowód: akta kontroli str. 4-22)

1.11. Urząd posiadał zawartą umowę z lokalnym operatorem na usługę hostingu serwera strony www oraz hostingu poczty elektronicznej. Ustawienia poczty pozwalały na zabezpieczenie przed wiadomościami typu SPAM, a programy antywirusowe chroniły przed przesyłaniem plików zawierających szkodliwe oprogramowanie.

(dowód: akta kontroli str. 51-55)

1.12. Sposób i częstotliwość wykonywania kopii bezpieczeństwa danych znajdujących się w systemach Urzędu został określony w § 2 pkt IV Instrukcji Zarządzania. Zgodnie z jej postanowieniami, codziennie tworzone były kopie bezpieczeństwa baz danych aplikacji dziedzinowych. Backupy zapisywano na serwerze i raz w tygodniu kopiowano na dysk przenośny. Logi routera na bieżąco zapisywano na serwerze i kopiowano z niego raz w miesiącu na dysk przenośny. (dowód: akta kontroli str. 4-9, 99-103)

1.13. Biegły stwierdził, że pracownicy Urzędu dysponowali możliwością ściągania aplikacji i plików wykonalnych, ale nie posiadali uprawnień pozwalających na instalowania ich na stacjach komputerowych, do których mieli dostęp. Uprawnienia do konfiguracji systemów komputerów działających w Urzędzie posiadał tylko administrator. Oględziny wszystkich komputerów Urzędu wykazały, że zainstalowane na nich systemy operacyjne były aktualne i objęte wsparciem technicznym producenta. W Urzędzie prowadzono też zestawienie, w którym ewidencjonowano programy zainstalowane na stacjach komputerowych.

(dowód: akta kontroli str. 4-22)

1.14. Biegły stwierdził, że wszystkie zbadane komputery posiadały aktualne wersje systemu operacyjnego. Aktualne były aplikacje dziedzinowe i aplikacje bezpieczeństwa. Aktualizacje były wykonywane zgodnie z harmonogramem domyślnie ustawionym przez dostawców.

(dowód: akta kontroli str. 4-9)

1.15. W Urzędzie nie realizowano płatności drogą elektroniczną. Były one realizowane przez specjalistyczny program komputerowy. Wyznaczony pracownik (operator) logował się do programu wprowadzając dane przelewu, które następnie były zatwierdzane przez osoby uprawnione (Skarbnik lub jego zastępca, wspólnie z Burmistrzem lub Sekretarzem). Kolejnym krokiem było wygenerowanie szyfrowanego pliku (zawierającego dane przelewu), który był nagrywany na nośnik przenośny. Nośnik ten był zanoszony do oddziału banku, gdzie następowało wczytanie przelewów do systemu informatycznego banku.

(dowód: akta kontroli str. 56)

Ustalone nieprawidłowości

W działalności kontrolowanej jednostki w przedstawionym wyżej zakresie stwierdzono niżej wymienione nieprawidłowości.

1. W Urzędzie nie przeprowadzano okresowych analiz ryzyka utraty integralności, dostępności lub poufności informacji, mimo takiego wymogu zawartego w § 20 ust. 2 pkt 3 rozporządzenia KRI. W wyjaśnieniu ABI podał, że: *„nie przeprowadzano takiej pisemnej analizy bowiem na bieżąco prowadzono nadzór i analizę zagrożeń utraty danych na stanowiskach przetwarzających dane osobowe".*

(dowód: akta kontroli str. 56-60)

[10] Na komputerze do Źródła – program antywirusowy od 15 stycznia 2018 r.

2. W Urzędzie nierzetelnie monitorowano dostęp do informacji. Nie był bowiem prowadzony zbiorczy rejestr dostępu do systemu, informacje zawarte w logach nie były przetwarzane automatycznie przez ASI, a logi zapisywane na końcówkach klienckich nie były zabezpieczone przed modyfikacją i zniszczeniem. Ponadto ABI nie nadzorował korzystania przez pracowników firmy ZETO (podczas realizacji prac serwisowych) z zainstalowanej na dwóch komputerach aplikacji pulpitu zdalnego TeamViewer.

   Natomiast zgodnie z § 20 ust. 2 pkt. 7 lit. a rozporządzenia KRI zarządzanie bezpieczeństwem informacji realizowane powinno być przez zapewnienie ochrony przetwarzanych informacji przed ich kradzieżą, nieuprawnionym dostępem, uszkodzeniami lub zakłóceniami, poprzez monitorowanie dostępu do informacji.

   ABI wyjaśnił, że: „*uprawnienia standardowego użytkownika uniemożliwiają ingerencję w logi systemowe. Na każdym stanowisku pracuje jeden użytkownik. Nie był prowadzony zbiorczy rejestr dostępu do systemu ze względu na ograniczenia techniczne i finansowe. Połączenie zdalne wymaga uprawnień administracyjnych, więc musiało być ustalane z administratorem systemu. W trakcie takiego połączenia żadnemu z pracowników ZETO nie powierzano bazy danych. Dostęp był jedynie w celach aktualizacyjnych bądź serwisowych*". (dowód: akta kontroli str. 4-9, 186-187)

3. W okresie objętym kontrolą w jednej (z czterech) zawartych przez Urząd umów dotyczących świadczenia usługi serwisu eksploatacyjnego oprogramowania komputerowego nie ujęto regulacji zobowiązujących wykonawcę do zapewnienia bezpieczeństwa informacji, w tym do zachowania w tajemnicy informacji, jakie mógł uzyskać przy świadczeniu serwisu. Było to sprzeczne z przepisem § 20 ust. 2 pkt 10 rozporządzenia KRI, w myśl którego w umowach serwisowych podpisanych ze stronami trzecimi zawiera się zapisy gwarantujące odpowiedni poziom bezpieczeństwa informacji. W wyjaśnieniu Burmistrz podał, że: „*podczas podpisywania umowy dotyczącej opieki serwisowej użytkowanego oprogramowania komputerowego, nie przewidywano sytuacji umożliwienia dostępu do programu i baz danych dla pracowników firmy zewnętrznej. W razie zaistnienia konieczności takiej pomocy zawarto by odrębną umowę zobowiązującą wykonawcę do przestrzegania ustawy o ochronie danych osobowych oraz o ochronie informacji niejawnych w ramach konkretnej pracy serwisowej*". (dowód: akta kontroli str. 23-33, 61-62)

Ocena cząstkowa

Najwyższa Izba Kontroli ocenia pozytywnie, mimo stwierdzonych nieprawidłowości, skuteczność przyjętych w Urzędzie rozwiązań dotyczących zabezpieczenia dostępu do poszczególnych systemów informatycznych i usług sieciowych przed nieuprawnionym dostępem, przejęciem lub zniszczeniem danych.

2. Dokumentacja i procedury dotyczące ochrony danych osobowych

2.1. Urząd zgłosił do rejestracji GIODO 13 zbiorów danych osobowych, z których zarejestrowanych zostało 12[11]. Analiza tych zbiorów wykazała, że:

- w pięciu zbiorach zaprzestano przetwarzania danych, w związku z czym 4 listopada 2015 r. Urząd wniósł o wykreślenie tych zbiorów z rejestru, ale do dnia zakończenia kontroli zbiory te nie zostały z niego wykreślone,
- zakres danych w siedmiu zarejestrowanych zbiorach odpowiadał zakresowi, w jakim były one przetwarzane. Natomiast w przypadku pięciu z tych zbiorów nie zgłoszono dodatkowej formy ich prowadzenia (oprócz formy papierowej, również elektronicznej), co szerzej opisano w dalszej części wystąpienia pokontrolnego, w sekcji „Ustalone nieprawidłowości".

Dane w Urzędzie przetwarzane były w 35 zbiorach danych (27 w wersji elektronicznej), z których siedem było zarejestrowanych przez GIODO. Zgłoszenia w tych sprawach zawierały elementy wymagane art. 41 ust. 1 ustawy o ochronie danych osobowych. Nie zostało zgłoszonych 21 zbiorów, z tego 16 zbiorów, których przetwarzanie rozpoczęto po powołaniu ABI, co szerzej opisano w dalszej części wystąpienia pokontrolnego, w sekcji „Ustalone nieprawidłowości.

[11] Jeden zbiór *Karta dużej rodziny* zgłoszono w sierpniu 2017 roku i do dnia zakończenia kontroli nie został on umieszczony w rejestrze.

W okresie objętym kontrolą Urząd nie aktualizował danych rejestracyjnych zbiorów zgłoszonych do GIODO. Nie wystąpiły również przypadki odmowy rejestracji zbioru.
(dowód: akta kontroli str. 63-78)

2.2. Burmistrz Szczuczyna z dniem 16 lutego 2015 r. wyznaczył ABI, o którym mowa w art. 36a ust. 1 ustawy o ochronie danych osobowych oraz w Polityce bezpieczeństwa. Zgłosił również, w myśl przepisu art. 46b ust. 1 ustawy o ochronie danych osobowych, do rejestracji GIODO fakt powołania ABI. Do zakończenia kontroli NIK nie dokonywano zmian na tym stanowisku. (dowód: akta kontroli str. 79-81, 133)

2.3. Zakres działania ABI określono w załączniku Nr 1 do zarządzenia Burmistrza z 16 lutego 2015 r. Zobowiązano go do stosowania środków technicznych i organizacyjnych zapewniających ochronę przetwarzania danych odpowiednią do zagrożeń oraz kategorii danych objętych ochroną, a w szczególności zabezpieczenie danych przed udostępnieniem osobom nieupoważnionym, zabraniem przez osobę nieupoważnioną, przetwarzaniem z naruszeniem ustawy, utratą uszkodzeniem lub zniszczeniem. Wyznaczono również szczegółowe zadania, tj.: [1] zapewnienie przestrzegania przepisów o ochronie danych osobowych, o których mowa w art. 36a ust. 2 ustawy o ochronie danych osobowych; [2] prowadzenie rejestru zbiorów danych przetwarzanych przez administratora; [3] nadzór nad fizycznym zabezpieczeniem pomieszczeń, w których przetwarzano dane osobowe oraz kontrola przebywających w nich osób; [4] zapewnienie awaryjnego zasilania komputerów oraz innych urządzeń mających wpływ na bezpieczeństwo przetwarzania danych osobowych; [5] nadzór nad naprawami, konserwacją oraz likwidacją urządzeń komputerowych, na których zapisywano dane osobowe; [6] nadzór nad zarządzaniem hasłami użytkowników i przestrzeganiem procedur określających częstotliwość ich zmiany; [7] nadzór nad czynnościami związanymi ze sprawdzaniem systemu pod kątem obecności wirusów komputerowych; [8] nadzór nad wykonywaniem kopii awaryjnych; [9] nadzór nad systemem komunikacji w sieci komputerowej; [10] Przeciwdziałanie dostępowi osób niepowołanych do przetwarzania danych osobowych; [11] kontrola nad danymi osobowymi wprowadzanymi do zbiorów; [12] podejmowanie odpowiednich działań w przypadku wykrycia naruszeń lub podejrzenia naruszenia zabezpieczeń; [13] nadzór nad obiegiem oraz przechowywaniem dokumentów zawierających dane osobowe; [14] nadzór nad prawidłowością archiwizacji oraz usuwania danych osobowych; [15] monitorowanie zabezpieczeń wdrożonych w celu ochrony danych osobowych.

ABI w odniesieniu do zadań określonych w zarządzeniu Burmistrza oraz w art. 36a ust. 2 ustawy o ochronie danych osobowych:

- dokonał sprawdzeń zgodności przetwarzania danych osobowych z przepisami o ich ochronie oraz zapoznał osoby upoważnione do przetwarzania danych osobowych z przepisami o ich ochronie,
- nie wywiązał się z: [1] prowadzenia rejestru zawierającego wykaz zbiorów danych osobowych przetwarzanych w Urzędzie; [2] opracowania planu sprawdzeń z zakresu przestrzegania przepisów o ochronie danych osobowych w Urzędzie Gminy na lata 2016 i 2017, co opisano w dalszej części wystąpienia pokontrolnego, w sekcji „Ustalone nieprawidłowości". (dowód: akta kontroli str. 56, 79-80, 213-214)

2.4. W Urzędzie, w myśl przepisu art. 39 ust. 1 ustawy o ochronie danych osobowych, prowadzono ewidencję osób upoważnionych do przetwarzania danych osobowych. Zawierała ona elementy określone w art. 39 ust. 1 pkt 1 – 3 ww. ustawy tj.: imię i nazwisko osoby upoważnionej, datę nadania i ustania upoważnienia oraz zakres upoważnienia i identyfikator.

Analiza zakresów obowiązków wszystkich 22 pracowników merytorycznych Urzędu i wydanych dla nich (przez ABI) upoważnień do przetwarzania danych osobowych wykazała, że wszyscy zostali upoważnieni do przetwarzania danych osobowych niezbędnych do realizacji zadań wynikających z zakresu czynności. Natomiast w ośmiu (z 22) przypadkach, wymieniając w upoważnieniach dostęp do zbiorów danych, nie ujęto wszystkich zbiorów, w których osoby posiadające upoważnienie przetwarzali dane osobowe. W wyjaśnieniu ABI podał, że: *„powodem takiej sytuacji było niedopatrzenie i błędne przeświadczenie, iż upoważnienia do przetwarzania danych osobowych obejmują*

jedynie zbiory przetwarzane w specjalistycznych programach, a nie wszystkie zbiory, tj. przetwarzane w formie papierowej czy programach biurowych".

(dowód: akta kontroli str. 134-187)

2.5. W Urzędzie nie były wydawane wewnętrzne akty prawne dotyczące ochrony danych osobowych, poza opisanymi w dalszej części wystąpienia pokontrolnego, w pkt. 2.10.

(dowód: akta kontroli str. 82-132)

2.6. Obowiązki Administratora Systemu Informatycznego („ASI") – zgodnie z załącznikiem Nr 1 do zarządzenia Burmistrza z 16 lutego 2015 r. – powierzono osobie zatrudnionej na stanowisku informatyka (pełniącego również funkcję ABI). Do jego obowiązków należało m.in.: [1] formułowanie, w uzgodnieniu z Administratorem Danych Osobowych („ADO"), sposobu określania uprawnień w systemach informatycznych; [2] realizacja decyzji ADO odnośnie nadania osobom uprawnień dostępu do danych i wybranych funkcji narzędzi służących do ich przetwarzania, w środowisku IT Urzędu, tj.: tworzenie kont użytkowników w systemach informatycznych, przypisywanie do kont startowych haseł uwierzytelniających użytkowników tych kont, przypisywanie do założonych kont polityk odnośnie jakości haseł i częstotliwości ich zmiany, resetowanie utraconych haseł, usuwanie kont i uprawnień dla kont osób, które zakończyły pracę w Urzędzie, dostarczanie ABI informacji potrzebnych do oceny prawidłowości funkcjonowania sprzętowo-programowych; [3] planowanie inwestycji oraz dostaw i usług niezbędnych dla utrzymania i rozwoju środowiska IT w Urzędzie; [4] planowanie i wykonywanie zadań związanych z tworzeniem kopii bezpieczeństwa systemów i danych; [5] automatyzacja zadań konserwacyjnych w systemie – w tym wykonywania kopii zapasowych oprogramowania i danych; [6] monitorowanie stanu środowiska IT, stanu sprzętu IT i wykorzystywanego oprogramowania oraz aktywności sieciowej użytkowników; [7] monitorowanie legalności oprogramowania systemowego, aplikacyjnego i ochronnego; [8] zapewnienie serwerom i stacjom roboczym niezbędnych licencji programowych; [9] systematyczne aktualizowanie oprogramowania systemowego, aplikacyjnego i ochronnego; [10] zapewnienie eksploatowanym systemom opieki serwisowej producenta – zawieranie umów regulujących formy tej opieki; [11] prowadzenie szkoleń na temat bezpiecznych zachowań użytkowników w środowisku systemów IT.

(dowód: akta kontroli str. 79-81)

2.7. Od 1 stycznia 2016 r. do 31 grudnia 2017 r. w Urzędzie nie przeprowadzano okresowych (co najmniej rocznych) audytów wewnętrznych z zakresu bezpieczeństwa informacji, wynikających z § 20 ust. 2 pkt. 14 rozporządzenia KRI, co szerzej opisano w dalszej części wystąpienia pokontrolnego, w sekcji „Ustalone nieprawidłowości".

(dowód: akta kontroli str. 56)

2.8. Do dnia zakończenia kontroli NIK trzech (z 22 zaangażowanych w proces przetwarzania danych osobowych) pracowników Urzędu nie zostało przeszkolonych z zakresu bezpieczeństwa przetwarzania informacji, co szerzej opisano w dalszej części wystąpienia pokontrolnego, w sekcji „Ustalone nieprawidłowości".

Ostatnie takie szkolenie (pt. „Ochrona danych osobowych"), w którym uczestniczyło 19 (nadal zatrudnionych) pracowników Urzędu odbyło się w maju 2014 roku.

(dowód: akta kontroli str. 56, 134-139)

2.9. Od 1 stycznia 2016 r. do 31 grudnia 2017 r. nie prowadzono w Urzędzie zewnętrznych kontroli w zakresie bezpieczeństwa danych oraz nie wpłynęły skargi dotyczące przypadków związanych z ujawnieniem danych osobowych lub naruszeniem przepisów związanych z ich ochroną. (dowód: akta kontroli str. 56)

2.10. W Urzędzie opracowano i wdrożono dokumentację związaną z przetwarzaniem i ochroną danych osobowych. I tak:

- zarządzeniem Nr 14/15 Burmistrza z 25 lutego 2015 r. wprowadzono: *„Politykę Bezpieczeństwa Danych Osobowych"* i *„Instrukcję Zarządzania Systemem Informatycznym"*,
- zarządzeniem Nr 101/15 Burmistrza z 31 grudnia 2015 r. wprowadzono procedury postępowania z kluczami oraz dostępu do pomieszczeń biurowych w Urzędzie,

- zarządzeniem Nr 102/15 Burmistrza z 31 grudnia 2015 r. wprowadzono regulamin organizacji i przetwarzania danych osobowych,
- zarządzeniem Nr 103/15 Burmistrza z 31 grudnia 2015 r. dopuszczono do stosowania w Urzędzie legalne programy komputerowe,
- zarządzeniem Nr 104/15 Burmistrza z 31 grudnia 2015 r. wprowadzono procedurę alarmową w Urzędzie. (dowód: akta kontroli str. 82-132)

Polityka bezpieczeństwa zawierała elementy określone w § 4 rozporządzeniu w sprawie dokumentacji oraz warunków technicznych: [1] wykaz budynków, pomieszczeń lub części pomieszczeń, tworzących obszar, w którym przetwarzane są dane osobowe, [2] wykaz zbiorów danych osobowych wraz ze wskazaniem programów zastosowanych do przetwarzania tych danych, [3] opis struktury zbiorów danych wskazujący zawartość poszczególnych pól informacyjnych i powiązania między nimi oraz sposób przepływu danych pomiędzy poszczególnymi systemami, [4] określenie środków technicznych i organizacyjnych niezbędnych dla zapewnienia poufności, integralności i rozliczalności przetwarzanych danych. Od przyjęcia Polityki bezpieczeństwa ww. wykazów nie aktualizowano, co szerzej opisano w dalszej części wystąpienia pokontrolnego, w sekcji „Ustalone nieprawidłowości".

Przyjęta Instrukcja zarządzania zawierała wszystkie elementy wymagane przepisem § 5 rozporządzenia w sprawie dokumentacji oraz warunków technicznych, tj. m.in.: [1] procedury nadawania uprawnień do przetwarzania danych i rejestrowania tych uprawnień w systemie informatycznym oraz wskazanie osoby odpowiedzialnej za te czynności; [2] stosowane metody i środki uwierzytelnienia oraz procedury związane z ich zarządzaniem i użytkowaniem; [3] procedury rozpoczęcia, zawieszenia i zakończenia pracy przeznaczone dla użytkowników systemu; [4] procedury tworzenia kopii zapasowych zbiorów danych oraz programów i narzędzi programowych służących do ich przetwarzania; [5] sposób, miejsce i okres przechowywania: elektronicznych nośników informacji zawierających dane osobowe oraz kopii zapasowych danych; [6] sposób zabezpieczenia systemu informatycznego przed działalnością oprogramowania, którego celem jest uzyskanie nieuprawnionego dostępu do systemu informatycznego [7] procedury wykonywania przeglądów i konserwacji systemów oraz nośników informacji służących do przetwarzania danych.

W Instrukcji zarządzania wprowadzony został wysoki poziom bezpieczeństwa (przynajmniej jedno urządzenie systemu informatycznego związane z przetwarzaniem danych osobowych były połączone z siecią publiczną[12]), co odpowiadało wymaganiom określonym w § 6 rozporządzenia w sprawie dokumentacji i warunków technicznych.

Przyjęte uregulowania i procedury związane z użytkowaniem systemów informatycznych służących do przetwarzania danych dotyczyły jedynie danych osobowych. Nie odnosiły się one do ochrony innych informacji będących w posiadaniu jednostki. Nie spełniały zatem wymogu określonego w § 2 pkt 15 w związku z § 20 ust. 1 rozporządzenia KRI, co szerzej opisano poniżej, w sekcji „Ustalone nieprawidłowości". (dowód: akta kontroli str. 82-103)

Ustalone nieprawidłowości

W działalności kontrolowanej jednostki w przedstawionym wyżej zakresie stwierdzono niżej wymienione nieprawidłowości.

1. Nie zgłoszono GIODO do rejestracji pięciu[13] z 35 zbiorów danych prowadzonych w Urzędzie, co naruszało wymogi art. 40 ustawy o ochronie danych osobowych. Dane osobowe w tych zbiorach były przetwarzane przed powołaniem ABI[14]. Ponadto w przypadku pięciu już zgłoszonych GIODO zbiorów nie zgłoszono dodatkowej formy ich prowadzenia (oprócz formy papierowej, również elektronicznej). Burmistrz wyjaśnił, że: *„przyczyną tego był wieloletni brak nadzoru nad wypełnianiem zapisów ustawy o ochronie danych osobowych w Urzędzie. Dlatego też w lutym 2015 r. powołałem ABI, do którego obowiązków należy prowadzenie jawnego rejestru zbiorów danych*

[12] Poza stanowiskami wydzielonymi do obsługi Systemu Rejestrów Państwowych.
[13] Prowadzonych w Urzędzie: od 1999 roku „Rejestr na wycinkę drzew", od 2005 roku „SIO", od 2007 roku „Dokształcanie młodocianych", od 2008 roku „Wyprawka szkolna" oraz od 2013 roku „Śmieci".
[14] Zgodnie z art. 43 ust. 1a ustawy o ochronie danych osobowych, obowiązkowi rejestracji zbiorów danych nie podlega administrator danych, który powołał ABI i zgłosił go do rejestracji GIODO.

osobowych oraz informowanie mnie o konieczności aktualizacji lub zgłoszenia zbiorów danych do rejestracji GIODO". (dowód: akta kontroli str. 63-64,77-78, 188)

2. ABI nie realizował zadań określonych w art. 36a ust. 2 ustawy o ochronie danych osobowych, tj. prowadzenia rejestru zbiorów danych przetwarzanych przez administratora oraz nadzorowania opracowania i aktualizowania dokumentacji, o której mowa w art. 36 ust. 2 tej ustawy. ABI wyjaśnił, że pełnoprawny rejestr zbiorów danych przetwarzanych przez ADO został utworzony w grudniu 2017 roku (tj. w trakcie kontroli NIK) Do czasu kontroli za rejestr zbiorów był uważany wykaz zbiorów danych osobowych stanowiący załącznik do Polityki bezpieczeństwa.

   Ponadto ABI nie sporządził w latach 2016 i 2017 planu sprawdzeń zgodności przetwarzania danych osobowych z przepisami o ochronie danych osobowych. Było to niezgodne z § 3 ust. 5 rozporządzenia w sprawie sposobu realizacji zadań ABI. Zgodnie z tym przepisem, plan sprawdzeń jest przygotowywany przez ABI na okres nie krótszy niż kwartał i nie dłuższy niż rok. Następnie jest przedstawiany kierownikowi jednostki (ADO) nie później niż na dwa tygodnie przed dniem rozpoczęcia okresu objętego planem i obejmuje co najmniej jedno sprawdzenie. W wyjaśnieniu ABI podał, że: „*w związku z bieżącym sprawdzaniem poprawności przetwarzania danych osobowych na stanowiskach pracy nie sporządzałem takich planów. Od 2018 roku zostanie corocznie sporządzony pisemny plan sprawdzeń i przedstawiony Burmistrzowi do akceptacji*". (dowód: akta kontroli str. 56, 189-191)

3. W okresie objętym kontrolą w Urzędzie nie przeprowadzano okresowych (co najmniej rocznych) audytów wewnętrznych z zakresu bezpieczeństwa informacji, wynikających z § 20 ust. 2 pkt. 14 rozporządzenia KRI. Burmistrz wyjaśnił, że: „*w związku z trudną sytuacją finansową gminy w badanym okresie nie zlecano wykonania audytu z zakresu bezpieczeństwa informacji. Wykonanie audytu planowane jest w I kwartale 2018 r.*".
   (dowód: akta kontroli str. 56, 61-62)

4. Do dnia zakończenia kontroli NIK nie przeszkolono trzech pracowników Urzędu z zagadnień związanych z ochroną danych osobowych oraz bezpieczeństwem informacji. W ostatnim takim szkoleniu w maju 2014 roku uczestniczyło 19 (z 22) obecnie zatrudnionych pracowników. Obowiązek zapewnienia szkoleń osobom zaangażowanym w proces przetwarzania informacji, z uwzględnieniem zagrożenia jej bezpieczeństwa, skutków naruszenia zasad bezpieczeństwa, konsekwencji prawnych i środków zapewniających jej bezpieczeństwo wynika z § 20 ust. 2 pkt 6 rozporządzenia KRI. W wyjaśnieniu Burmistrz podał, że: „*każdy pracownik upoważniony do przetwarzania danych osobowych zapoznał się z przepisami o ich ochronie. Uzyskał niezbędną dokumentację i indywidualne przeszkolenie, został również pouczony w kwestii odpowiedzialności i podpisał stosowne oświadczenie*".
   (dowód: akta kontroli str. 56, 134-139, 215-216)

5. Od przyjęcia 25 lutego 2015 roku do 31 grudnia 2017 r. Polityka bezpieczeństwa oraz Instrukcja zarządzania systemem informatycznym nie były aktualizowane, w tym m.in.:
   - *Wykaz budynków, pomieszczeń lub części pomieszczeń, tworzących obszar w którym przetwarzane są dane osobowe* (stanowiący załącznik Nr 2 do Polityki bezpieczeństwa), który nie zawierał jednego[15] z 24 pomieszczeń, w których przetwarzano dane,
   - *Wykaz zbiorów danych osobowych wraz ze wskazaniem programów zastosowanych do przetwarzania tych danych* (załącznik Nr 3 do Polityki bezpieczeństwa), który nie zawierał 24 z 35 prowadzonych przez Urząd zbiorów danych,
   - *Opis struktury zbiorów danych wskazujących zawartość pól informacyjnych i powiązania między nimi oraz sposób przepływu danych pomiędzy poszczególnymi systemami* (załącznik Nr 4 do Polityki bezpieczeństwa), który nie zawierał 24 z 35 prowadzonych przez Urząd zbiorów danych.

[15] Pokoju Nr 15A – Kierownika Referatu Rozwoju i Inwestycji.

Było to sprzeczne z przepisem § 20 ust. 2 pkt 1 rozporządzenia KRI, zgodnie z którym zapewnia się aktualizację regulacji wewnętrznych w zakresie dotyczącym zmieniającego się otoczenia. Ponadto przyjęte w Urzędzie uregulowania i procedury składające się na politykę bezpieczeństwa informacji dotyczyły jedynie ochrony danych osobowych. Nie odnosiły się one do innych danych będących w posiadaniu jednostki. W konsekwencji nie spełniono wymogu określonego w § 2 pkt 15 w związku z § 20 ust. 1 rozporządzenia KRI. W wyjaśnieniu ABI podał, że: *„brak aktualizacji wykazów wynikał z obciążenia pracą i obowiązkami. W Urzędzie pełnię funkcję również informatyka i administratora systemów informatycznych. Ponadto wszystkie obowiązki staram się realizować na bieżąco, a powstałe opóźnienia wynikają z okresowego nawarstwiania się zadań, które muszą być zrealizowane w pokrywających się terminach"*. (dowód: akta kontroli str. 186-187, 192-203)

Ocena cząstkowa

Najwyższa Izba Kontroli ocenia pozytywnie, mimo stwierdzonych nieprawidłowości, opracowanie i wdrożenie dokumentacji i procedur wymaganych przepisami ustawy o ochronie danych osobowych.

3. Sposób przechowywania oraz zabezpieczenia danych

3.1. W załączniku nr 2 do Polityki bezpieczeństwa *„Wykaz budynków, pomieszczeń lub części pomieszczeń, tworzących obszar, w których przetwarzane są dane osobowe"* określony został sposób ich zabezpieczenia: [1] system alarmowy; [2] drzwi z zamkiem; [3] okno antywłamaniowe z zamkiem. W wyniku przeprowadzonych oględzin stwierdzono, że zastosowane zabezpieczenia były zgodne z przyjętymi regulacjami wewnętrznymi. (dowód: akta kontroli str. 82-98)

Oględziny pomieszczeń Urzędu, w których przetwarzane były zbiory danych osobowych wykazały, że: [1] przetwarzanie danych osobowych odbywało się w miejscach do tego wyznaczonych; [2] urządzenia (stacje komputerowe) znajdowały się w pomieszczeniach zabezpieczonych zamkami; [3] stacje komputerowe wykorzystywane do przetwarzania danych wyposażone były w zabezpieczenia na wypadek zaniku napięcia (UPS); [4] kopie zapasowe tworzone były przez ABI; [5] w Urzędzie zainstalowano system alarmowy, którego kod dezaktywacyjny był znany Burmistrzowi, Sekretarzowi, pracownikowi sekretariatu oraz pracownikowi obsługi wykonującemu prace związane ze sprzątaniem obiektu, [6] klucze do wejścia głównego Urzędu były w posiadaniu wymienionych czterech osób; [7] papierowa część wszystkich 36 zbiorów danych osobowych przechowywana była w szafach zamykanych na klucz; [8] dwa pokoje, w których przetwarzane były dane osobowe, znajdowały się na parterze budynku. Jedno pomieszczenie (informatyka – ABI) zabezpieczone zostało oknem antywłamaniowym, zaś drugie (Referat Komunalny, Planowania Przestrzennego i Działalności Gospodarczej) takich zabezpieczeń nie posiadało. Oba pomieszczenia zabezpieczono natomiast alarmowymi czujkami ruchu. Pozostałe pomieszczenia znajdowały się na pierwszym i na drugim piętrze budynku, a okna (poza pokojem USC, które wyposażone było w okno antywłamaniowe) nie posiadały zabezpieczeń antywłamaniowych i krat metalowych [9] pomieszczenie archiwum znajdowało się na parterze budynku Urzędu i nie posiadało systemu przeciwpożarowego, a akta składowano w drewnianych zamykanych szafach. Na wyposażeniu archiwum znajdowały się dwie gaśnice proszkowe (12 i 6 kg). Kolejna gaśnica proszkowa była przy drzwiach prowadzących do archiwum (6 kg). W archiwum oraz na korytarzu prowadzącym do archiwum znajdowały się alarmowe czujniki ruchu. Ponadto w kierunku drzwi archiwum skierowana była kamera monitoringu wizyjnego (rejestracja odbywa się w cyklu ciągłym, z możliwością odtworzenia nagrania do 30 dni wstecz; rejestrator znajdował się w pomieszczeniu serwerowni). (dowód: akta kontroli str. 202-206)

3.2. Urząd posiadał informacje z zakresu inwentaryzacji sprzętu i oprogramowania służącego do przetwarzania informacji, obejmującej ich rodzaj i konfigurację. Dane te ujmowane były w tabeli *„Sprzęt i oprogramowanie służące do przetwarzania danych osobowych"*. Znajdowały się w nich dane o wszystkich urządzeniach w Urzędzie. Było to zgodne z § 20 ust. 2 pkt 2 rozporządzenia w sprawie KRI. (dowód: akta kontroli str. 207)

3.3. W latach 2016 – 2017 (do 31 grudnia) w Urzędzie, jak wyjaśnił ABI, nie likwidowano sprzętu komputerowego, będącego nośnikiem danych oraz nie wystąpiły przypadki, w których sprzęt komputerowy naprawiany był przez podmioty zewnętrzne.
(dowód: akta kontroli str. 57-60)

3.4. Niszczenie dokumentów w Urzędzie zawierających dane osobowe odbywało się za pomocą niszczarek. Do tego celu Urząd wyposażono w dziesięć niszczarek. W Urzędzie nie opracowano regulacji wewnętrznych w tym zakresie. (dowód: akta kontroli str. 202-203)

3.5. W Instrukcji zarządzania systemem informatycznym określono zasady dotyczące użytkowania komputerów przenośnych. Przyjęto w nich, że osoba użytkująca komputer przenośny zawierający dane osobowe zachowuje szczególną ostrożność podczas jego transportu, przechowywania i użytkowania poza obszarem przetwarzania danych osobowych, w tym stosuje hasła dostępu do komputera przenośnego oraz do plików, w których przechowywane są dane osobowe.

W okresie objętym kontrolą na terenie Urzędu wykorzystywano jeden komputer przenośny, który pełnił funkcję urządzenia umożliwiającego wyświetlanie prezentacji w sali konferencyjnej. (dowód: akta kontroli str. 99-103, 202-203)

3.6. Sprzątanie pomieszczeń, w których przetwarzano dane osobowe odbywało się od 13^{00} do 19^{00}, tj. poza godzinami pracy Urzędu. Osoby sprzątające uzyskały zgodę ADO na przebywania w obszarze przetwarzania danych poza godzinami pracy Urzędu.

Natomiast sprzątanie pomieszczenia serwerowni odbywało się w godzinach pracy Urzędu i pod nadzorem ABI. Dostęp do serwerowni posiadał tylko ABI i ADO (Burmistrz).
(dowód: akta kontroli str. 57-60, 202-203)

3.7. Procedury dotyczące przeglądów i konserwacji systemów oraz nośników informacji służących do przetwarzania danych osobowych zostały określone w § 5 Instrukcji zarządzania systemem informatycznym. Określono w nich, że ABI dokonuje przeglądów technicznych sprzętu informatycznego oraz dba o ich dobry stan techniczny (co 30 dni wykonuje przeglądy okresowe i raz na rok przegląd generalny). W przypadku stwierdzenia usterek, ABI ma obowiązek niezwłocznie powiadomić o tym fakcie ADO. Fakt oraz wymagana częstotliwość przeprowadzenia takich przeglądów i konserwacji nie została przez ABI udokumentowana. W wyjaśnieniu ABI podał, że: *„przeglądy techniczne sprzętu informatycznego dokonywane były w okresach miesięcznych a przegląd generalny dokonywany jest raz w roku. Ze względu na brak poważnych usterek w sprzęcie informatycznym z przeglądów nie sporządzano pisemnych notatek*".
(dowód: akta kontroli str. 99-103, 189-191)

3.8. Do 22 grudnia 2017 r. Urząd nie posiadał wewnętrznych regulacji dotyczących rozwiązań na wypadek wystąpienia sytuacji nadzwyczajnych, np. długotrwałego braku zasilania. Burmistrz w dniu 22 grudnia 2017 r. zatwierdził *„Plan ciągłości działania na wypadek awarii systemu informatycznego w Urzędzie Miejskim w Szczuczynie*". Plan ten m.in. określał: warunki uruchomienia planu, osoby i zasoby wymagane do realizacji planu oraz działania zapewniające przywrócenie zdolności realizacji działalności statutowej (funkcja, opis działań, potrzebne zasoby, osoby odpowiedzialne).
(dowód: akta kontroli str. 208-212)

3.9. Jak wyjaśnił ABI, w okresie objętym kontrolą nie wystąpiły przypadki fizycznej utraty danych. (dowód: akta kontroli str. 56)

Ustalone nieprawidłowości

W działalności kontrolowanej jednostki w przedstawionym wyżej zakresie stwierdzono nieprawidłowość dotyczącą pomieszczenia archiwum, które – wbrew wymogom § 6 i § 8 ust. 1 pkt 1 załącznika nr 6 do rozporządzenia w sprawie organizacji i zakresu działania archiwów zakładowych[16] – nie posiadało systemu przeciwpożarowego oraz zabezpieczenia przed zalaniem, a akta składowano w drewnianych szafach. Przyjęcie takich rozwiązań nie zapewniało właściwej ochrony zbiorów danych przed działaniem czynników fizycznych

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

i zdarzeń losowych (pożar, zalanie). W wyjaśnieniu Burmistrz podał, że: *„mieścimy się w zabytkowym budynku. W pomieszczeniu archiwum nie znajduje się żadna infrastruktura wodna czy kanalizacyjna. Planując remont, musieliśmy sprostać wielu ograniczeniom stawianym przez Konserwatora Zabytków co do struktury obiektu. Traktujemy to pomieszczenie jako zastępcze i tymczasowe. W związku z toczącym się wygaszaniem Publicznego Gimnazjum planowane jest przygotowanie profesjonalnego pomieszczenia archiwum w budynku Publicznego Gimnazjum. Pomieszczenie to będzie spełniało wszelkie wymogi*". (dowód: akta kontroli str. 61-62, 202-203)

Ocena cząstkowa

Najwyższa Izba Kontroli ocenia pozytywnie przestrzeganie przez Urząd przyjętych procedur dotyczących przechowywania i zabezpieczenia danych oraz zapewnienia im właściwej ochrony. Stwierdzona nieprawidłowość nie miała wpływu na tę ocenę.

4. Przetwarzanie zasobów informacyjnych zgodnych z zakresem działalności jednostki kontrolowanej

4.1. Dane w Urzędzie przetwarzane były w 35 zbiorach danych, z których osiem prowadzono wyłącznie w wersji papierowej, zaś 27 w wersji elektronicznej i papierowej. Do GIODO zgłoszono siedem zbiorów danych – wszystkie prowadzone w wersji papierowej. Nie zgłoszono do zarejestrowania pięciu zbiorów danych prowadzonych w Urzędzie (czterech prowadzonych w wersji elektronicznej i papierowej oraz jednego tylko w wersji papierowej), co szczegółowo omówiono w pkt 2.1 niniejszego wystąpienia.
(dowód: akta kontroli str. 77-78)

4.2. W okresie objętym kontrolą Urząd nie aktualizował danych w rejestrze prowadzonym przez GIODO w odniesieniu do zbiorów, które były zarejestrowane, co szczegółowo omówiono w pkt 2.1 niniejszego wystąpienia. (dowód: akta kontroli str. 63-64)

4.3. We wszystkich siedmiu zbiorach zgłoszonych do GIODO i prowadzonych przez Urząd zakres przetwarzanych danych był zgodny ze zgłoszeniem.

Analiza wszystkich 36 zbiorów danych prowadzonych w Urzędzie wykazała, że dane w nich gromadzone były wykorzystywane (niezbędne) do realizacji zadań, dla których zbiory były prowadzone. (dowód: akta kontroli str. 77-78, 134-139)

4.4. Burmistrz był ADO zbiorów danych (do których dostęp posiadali pracownicy Urzędu), z wyjątkiem SRP ŹRÓDŁO, serwis CEIDEG, serwis EMUiA[17], w rozumieniu art. 7 pkt 4 ustawy o ochronie danych osobowych. Urząd uzyskał dostęp do zbioru danych SRP ŹRÓDŁO z dniem 4 stycznia 2016 r., na podstawie upoważnienia Ministra Spraw Wewnętrznych z 20 czerwca 2016 r. Urząd spełnił wymogi dostępu do tego zbioru danych, tj. m.in. uniemożliwił dostęp do „otwartego" Internetu na stanowisku komputerowym z którego obsługiwano ten system, pracownik otrzymał upoważnienie do przetwarzania danych osobowych w tym systemie (informacja o udzielonym pracownikowi upoważnieniu została przekazana do Ministerstwa). Dostęp do serwisu CEIDG Urząd uzyskał na podstawie zgłoszenia z lipca 2011 roku oraz zapewnił podpis elektroniczny trzem pracownikom obsługującym ten serwis. Możliwość przetwarzania danych w serwisie EMUiA została udostępniona na podstawie porozumienia zawartego 11 kwietnia 2012 r. z Głównym Geodetą Kraju. Urząd wywiązał się z obowiązków zapewnienia odpowiedniej infrastruktury technicznej niezbędnej do użytkowania aplikacji oraz wskazania administratora i użytkowników tej aplikacji. (dowód: akta kontroli str. 217-228)

Ustalone nieprawidłowości

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

Ocena cząstkowa

Najwyższa Izba Kontroli ocenia pozytywnie sposób przetwarzania zasobów informacyjnych, który był zgodny z zakresem działalności Urzędu, a w odniesieniu do zbiorów zewnętrznych spełniał wymogi związane z uzyskaniem do nich dostępu.

[17] System Rejestrów Państwowych aplikacja ŹRÓDŁO, Centralna Ewidencja i Informacja o Działalności Gospodarczej, Ewidencja Miejscowości Ulic i Adresów.

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[18], wnosi o:

1. Wywiązywanie się z obowiązków określonych w art. 36a ust. 2 ustawy o ochronie danych osobowych.
2. Analizowanie i zabezpieczenie przed modyfikacją lub zniszczeniem logów systemów operacyjnych komputerów wykorzystywanych w Urzędzie.
3. Umożliwianie zdalnego dostępu firmie serwisującej składniki systemu Urzędu, po uzyskaniu odpowiedniej autoryzacji, która pozwoli na zidentyfikowanie działań podejmowanych przez ten podmiot w serwisowanych systemach.
4. Zawarcie w umowie na świadczenie usług serwisowych zapisów gwarantujących odpowiedni poziom bezpieczeństw informacji oraz ich zabezpieczenia w sposób uniemożliwiający ujawnienie osobom nieuprawnionym.
5. Zapewnienie szkoleń, o których mowa w § 20 ust. 2 pkt 6 rozporządzenia KRI, wszystkim pracownikom zaangażowanym w proces przetwarzania informacji.
6. Wywiązywanie się z obowiązków, wynikających z § 20 ust. 1 i ust. 2 pkt. 1, 3 i 14 rozporządzenia KRI, w zakresie aktualizacji przyjętych regulacji wewnętrznych, prowadzenia okresowych analiz ryzyka utraty integralności, dostępności lub poufności informacji oraz audytów wewnętrznych z zakresu bezpieczeństwa informacji.
7. Zapewnienie właściwej ochrony papierowej wersji posiadanych zbiorów danych przed działaniem czynników fizycznych i zdarzeń losowych (pożar, zalanie).

V. Pozostałe informacje i pouczenia

Prawo zgłoszenia zastrzeżeń

Wystąpienie pokontrolne zostało sporządzone w dwóch egzemplarzach; jeden kierownikowi 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 Delegatury NIK w Białymstoku.

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 uwagi 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.

Białystok, dnia 25 stycznia 2018 r.

Kontroler
Tomasz Pomian
główny specjalista kontroli państwowej

podpis

DYREKTOR DELEGATURY
Najwyższej Izby Kontroli w Białymstoku
z up. WICEDYREKTOR
Robert Skwarko

podpis

[18] Dz. U. z 2017 r. poz. 524, dalej: Ustawa o NIK.