NAJWYŻSZA IZBA KONTROLI
Delegatura w Białymstoku

LBI.410.023.03.2017
P/17/062

02252317

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	Beata Palinowska – starszy inspektor kontroli państwowej, upoważnienie do kontroli nr LBI/157/2017 z 3 listopada 2017 r. (dowód: akta kontroli str. 1-2)
Jednostka kontrolowana	Urząd Miasta Wysokie Mazowieckie, ul. Ludowa 15, 18-200 Wysokie Mazowieckie (dalej: „Urząd")
Kierownik jednostki kontrolowanej	Jarosław Siekierko – Burmistrz Miasta Wysokie Mazowieckie[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 odpowiedniego poziomu wykonania zabezpieczeń odpowiadających za autoryzację dostępu do sieci, opracowania dokumentacji dotyczącej przetwarzania danych osobowych (Polityki Bezpieczeństwa i Instrukcji Zarządzania Systemem Informatycznym[4]) oraz ze sposobu przechowywania i zabezpieczenia danych, który odpowiadał przepisom oraz przyjętym procedurom.

Stwierdzono m.in. następujące nieprawidłowości:

- nierzetelnie monitorowano dostęp do informacji,
- nie podjęto niezwłocznych działań celem odebrania dostępu do systemu zawierającego dane osobowe pracownika, z którym rozwiązano stosunek pracy,
- nie monitorowano dostępu do informacji oraz nie przeprowadzano okresowego audytu bezpieczeństwa informacji, mimo wymogów zawartych w § 20 ust 2 pkt 7 i 14 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[5],
- w regulacjach składających się na politykę bezpieczeństwa informacji, o której mowa w § 2 pkt 15 rozporządzenia KRI nie uwzględniono części wymogów określonych w § 20 ust. 1 ww. rozporządzenia, a Instrukcja Zarządzania nie zawierała jednego z ośmiu wymaganych elementów,
- w ośmiu zbiorach danych gromadzono dane w zakresie szerszym niż zgłoszony do Generalnego Inspektora Ochrony Danych Osobowych (dalej: „GIODO"), a w dwóch zbiorach dane, które nie były niezbędne do realizacji przypisanych zadań.

---

1 Funkcję Burmistrza Miasta Wysokie Mazowieckie pełni od 20 listopada 1998 r.

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 Instrukcja zwana dalej: „Instrukcją Zarządzania". Wprowadzona zarządzeniem Burmistrza Miasta Wysokie Mazowieckie z 12 kwietnia 2016 r.

5 Dz. U. z 2016 r. poz. 113, ze zm. Rozporządzenie zwane dalej: „rozporządzeniem KRI".

III. Opis ustalonego stanu faktycznego

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

Opis stanu faktycznego

1.1. W Urzędzie do gromadzenia i przetwarzania danych osobowych były wykorzystywane następujące systemy informatyczne: ŹRÓDŁO, SelWin, FISKUS, SUMPRO, CEiDG, SIO, Płatnik, Płace i SmartDoc. Przyjęto, zgodnie z § 6 ust. 4 rozporządzenia 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 służące do przetwarzania danych osobowych[6] wysoki poziom zabezpieczeń, w związku z tym, że wszystkie stanowiska komputerowe, na których znajdowały się systemy służące do przetwarzania danych osobowych (poza przeznaczonymi do obsługi systemu ŹRÓDŁO) posiadały dostęp do Internetu. (dowód: akta kontroli str. 114-134)

W trakcie oględzin wszystkich 29 stanowisk komputerowych Urzędu stwierdzono, że żaden użytkownik nie posiadał uprawnień administratora systemu operacyjnego. W każdym przypadku dostęp do systemu operacyjnego był zabezpieczony loginem i hasłem. Na 21 stanowiskach konfiguracja komputera umożliwiała uaktywnienie się wygaszacza ekranu po 10 minutach, a powrót do systemu wymagał podania loginu i hasła dostępu. Natomiast na pozostałych ośmiu stanowiskach wygaszacz ekranu nie był aktywny. Na wszystkich stanowiskach program antywirusowy był aktualny. Z kolei na 24 komputerach aktualny był też system operacyjny, na dwóch zainstalowano system Windows XP (użytkownicy nie posiadali dostępu do systemów służących do przetwarzania danych osobowych oraz dostępu do poczty służbowej), a na trzech, które służyły do obsługi systemu ŹRÓDŁO, system operacyjny nie był aktualizowany.

(dowód: akta kontroli str. 114-134)

1.2. W okresie objętym kontrolą w Urzędzie nie były przeprowadzane okresowe analizy ryzyka utraty integralności, dostępności lub poufności informacji, mimo takiego wymogu wynikającego z § 20 ust. 2 pkt. 3 rozporządzenia KRI, co szerzej opisano w dalszej części wystąpienia pokontrolnego, w sekcji „Ustalone nieprawidłowości".

(dowód: akta kontroli str. 170)

1.3. Pracownicy przetwarzający dane osobowe posiadali uprawnienia użytkownika systemu nadane przez Administratora Systemu Informatycznego (dalej: „ASI"), wszyscy posiadali własny login i hasło. Nadane uprawnienia, stosownie do przepisu § 20 ust. 2 pkt 4 rozporządzenia KRI, były adekwatne do realizowanych zadań wynikających z ich zakresów czynności. Hasła dostępu 28 (z 29) użytkowników spełniały wymagania określone w obowiązującej w Urzędzie Instrukcji Zarządzania oraz w załączniku do rozporządzenia w sprawie dokumentacji i warunków technicznych.

Analiza nadawania i odbierania uprawnień pracownikom wykazała, że w 13 (z 14) przypadkach niezwłocznie zmieniono uprawnienia osób zaangażowanych w proces przetwarzania danych w przypadku zmiany zajmowanego stanowiska lub rozwiązania stosunku pracy, zgodnie z § 20 ust. 2 pkt 4 i 5 rozporządzenia KRI.

Nieprawidłowości w zakresie zmiany uprawnień oraz niespełnienia wymogów w zakresie hasła dostępu do systemu operacyjnego szerzej opisano w dalszej części wystąpienia pokontrolnego, w sekcji „Ustalone nieprawidłowości".

(dowód: akta kontroli str. 114-134, 179-181)

1.4. W Urzędzie nie prowadzono zbiorczego rejestru dostępu do systemu w formie papierowej bądź elektronicznej. Informacje o dostępie były gromadzone przez kontroler domeny, a także indywidualnie dla każdego klienta domenowego. Tryb zarządzania logami (ich zawartość i czas przechowywania) był zgodny z ustawieniami domyślnymi przewidzianymi przez producenta systemu. Logi routera, serwera i aplikacji na nim

[6] Dz. U. Nr 100, poz. 1024 ze zm. Rozporządzenie zwane dalej „rozporządzeniem w sprawie dokumentacji i warunków technicznych".

działających były zabezpieczone przed dostępem użytkowników systemu oraz systematycznie – raz w tygodniu – analizowane. Informacje zawarte w logach nie były przetwarzane automatycznie przez ASI, a logi zapisywane na końcówkach klienckich nie były zabezpieczone przed modyfikacją i zniszczeniem. Szerzej nieprawidłowości w zakresie monitorowania dostępu do systemu opisano w dalszej części wystąpienia pokontrolnego, w sekcji „Ustalone nieprawidłowości". (dowód: akta kontroli str. 194-199)

1.5. W Urzędzie, zgodnie z § 20 ust. 2 pkt 7 lit. c rozporządzenia KRI, zapewniono środki uniemożliwiające nieautoryzowany dostęp na poziomie systemów operacyjnych (zastosowano wymuszenie okresowej zmiany hasła), usług sieciowych i urządzeń serwerowni, poprzez zabezpieczenie hasłem. Sieć WI-FI była odseparowana fizycznie od sieci LAN, a dostęp do niej zabezpieczony był hasłem, które było udostępniane wybranym osobom. (dowód: akta kontroli str.158, 194-199)

1.6. W przyjętych regulacjach wewnętrznych dotyczących ochrony danych osobowych nie uregulowano kwestii związanych z wykorzystaniem do pracy sprzętu niebędącego własnością Urzędu. (dowód: akta kontroli str. 25-71)

Konfiguracja sieciowa umożliwiała podłączenie do infrastruktury sprzętu (laptopy, telefony, tablety) niestanowiącego własności pracodawcy, jednak nie było możliwe korzystanie z jej zasobów za pomocą wspomnianego sprzętu. Informacje o podłączeniu do komputerów nośników pamięci były domyślnie zapisywane w logach systemu komputerowego, lecz nie były trwale zabezpieczane (szerzej problem opisano w dalszej części wystąpienia pokontrolnego, w sekcji „Ustalone nieprawidłowości").

Na dwóch komputerach zainstalowano aplikację pulpitu zdalnego TeamViewer, z której korzystali pracownicy firmy ZETO Białystok podczas realizacji prac serwisowych. Dostęp ten nie był objęty kontrolą ASI, co szerzej opisano w dalszej części wystąpienia pokontrolnego, w sekcji „Ustalone nieprawidłowości". (dowód: akta kontroli str. 194-199)

1.7. Od 1 stycznia 2016 r. do 1 grudnia 2017 r. nie wystąpiły przypadki wykrycia nieautoryzowanych działań związanych z przetwarzaniem informacji.
(dowód: akta kontroli str. 170)

1.8. W obowiązującej w Urzędzie dokumentacji zobowiązano pracowników użytkujących komputery przenośne do zachowania szczególnej ostrożności oraz zabezpieczania hasłem plików lub folderów zawierających dane osobowe podczas transportu, przechowywania i użytkowania komputera poza obszarem przetwarzania danych. W Urzędzie użytkowane były dwa komputery przenośnie, które nie miały szyfrowanych dysków, a dostęp do ich systemów operacyjnych był zabezpieczony hasłem. W Urzędzie nie przewidziano zdalnego dostępu pracowników do zasobów sieci lokalnej. (dowód: akta kontroli str. 46-52, 194-199)

1.9. W umowach związanych z serwisem i aktualizacją programów wykorzystywanych do gromadzenia i przetwarzania danych osobowych (system Sumpro, Fiskus, SelWin, Płace) zawarte były zapisy gwarantujące odpowiedni poziom bezpieczeństwa informacji, co było zgodne z § 20 ust. 2 pkt. 10 rozporządzenia KRI. Obejmowały one w szczególności zobowiązanie do: [1] przetwarzania danych osobowych wyłącznie w celu oraz w zakresie związanym z realizacją zawartych umów; [2] zastosowania środków technicznych i organizacyjnych zapewniających ochronę danych, co najmniej w zakresie określonym w art. 36 – 39 a ustawy z dnia 29 sierpnia 1997 r. o ochronie danych osobowych[7]; [3] zachowania w tajemnicy informacji uzyskanych w trakcie realizacji umów.
(dowód: akta kontroli str. 80-93)

1.10. Komputery wchodzące w skład sieci lokalnej były zabezpieczone przed działaniem oprogramowania, którego celem jest uzyskanie nieuprawnionego dostępu do systemu informatycznego, dedykowanym do tego celu oprogramowaniem. Badane komputery posiadały aktualne wersje aplikacji zabezpieczających. Dostęp do sieci lokalnej kontrolowany był przez firewall zainstalowany na routerze CISCO. Było to zgodne z pkt III załącznika do rozporządzenia w sprawie dokumentacji i warunków technicznych.
(dowód: akta kontroli str. 194-199)

---

[7] Dz. U. z 2016 r. poz. 922.

1.11. Urząd wykupił usługę hostingu strony internetowej, domenę internetową oraz pocztę elektroniczną w podmiocie zewnętrznym (Home.pl). Dane poczty przechowywano na serwerze usługodawcy, który był również ich administratorem. Zgodnie z pkt. 7 regulaminu sieci home.pl, podmiot realizujący usługę zapewni przestrzeganie przepisów o ochronie danych osobowych podczas realizacji usług. Ustawienia poczty zapewniały właściwe zabezpieczenie przed wiadomościami typu SPAM oraz przesyłaniem plików zawierających szkodliwe oprogramowanie. (dowód: akta kontroli str. 139-151)

1.12. Sposób wykonywania kopii zbiorów danych, miejsce i czas ich przechowywania został określony w § 9 Instrukcji Zarządzania. Zgodnie z tymi uregulowaniami, kopie pełne zbiorów danych oraz programów i narzędzi służących do ich przetwarzania powinny być wykonywane na koniec dnia, zapisywane na pamięci przenośnej (pendrive) bądź na nośnikach CD/DVD. Nośniki danych natomiast winny być przechowywane w metalowej szafie zamykanej na klucz, przez okres pięciu dni roboczych.

Kopie zapasowe baz danych programów wykorzystywanych w Urzędzie robione były zgodnie z postanowieniami Instrukcji Zarządzania codziennie, następnie były zapisywane na serwerze plików i kopiowane na nośniki optyczne, przechowywane w odosobnionym, bezpiecznym miejscu. (dowód: akta kontroli str. 46-52, 194-199)

1.13. Pracownicy Urzędu dysponowali możliwością ściągania aplikacji i plików wykonalnych, natomiast nie posiadali uprawnień do instalowania ich na stacjach komputerowych, do których mieli dostęp. Uprawnienia do konfiguracji systemów operacyjnych komputerów działających w sieci LAN posiadał tylko administrator. (dowód: akta kontroli str. 194-199)

Na dwóch komputerach, których użytkownicy nie mieli dostępu do systemów służących do przetwarzania danych oraz do służbowej poczty elektronicznej były użytkowane systemy operacyjne Windows XP, dla których producent zakończył wsparcie techniczne.
(dowód: akta kontroli str. 194-199)

ASI prowadził rejestr zasobów informatycznych, który obejmował dane dotyczące systemów operacyjnych zainstalowanych na komputerach. Nie zawierał on pozostałych zainstalowanych programów, co szerzej opisano w pkt. 3.2. wystąpienia pokontrolnego.
(dowód: akta kontroli str. 94-95)

1.14. W Urzędzie, zgodnie z § 20 ust. 2 pkt 12 lit. a rozporządzenia KRI, zadbano o aktualizację systemów operacyjnych oraz aplikacji bezpieczeństwa Były one aktualizowane zgodnie z harmonogramem domyślnie ustawionym przez dostawcę (poza zainstalowanymi na komputerach służących do obsługi systemu ŹRÓDŁO).
(dowód: akta kontroli str. 114-134, 194-199)

1.15. W Urzędzie nie były opracowane regulacje wewnętrzne w zakresie dokonywania płatności drogą elektroniczną. Płatności były realizowane poprzez stronę internetową banku z użyciem technologii VPN. Po sprawdzeniu dokumentu pod względem merytorycznym i formalno-rachunkowym oraz zatwierdzeniu go do wypłaty / przelewu, wyznaczony pracownik sporządzał szablon przelewu, który był zatwierdzany przez jedną z dwóch uprawnionych osób z wykorzystaniem narzędzi uwierzytelniających.
(dowód: akta kontroli str. 215-231)

Ustalone nieprawidłowości

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

1. W Urzędzie nie przeprowadzono udokumentowanych, okresowych analiz ryzyka utraty integralności, dostępności lub poufności informacji, mimo takiego obowiązku określonego w § 20 ust. 2 pkt 3 rozporządzenia KRI, a także w § 4 obowiązującej w Urzędzie Instrukcji Zarządzania.

   ASI wyjaśnił, że: *„Nie były sporządzane formalne, pisemne protokoły, natomiast sytuacje związane z ryzykiem utraty integralności, dostępności lub poufności informacji są analizowane na bieżąco"*. (dowód: akta kontroli str. 46-52, 170, 200-204)

2. Oględziny komputerów wykazały, że hasło dostępu do systemu operacyjnego jednego (z 29) użytkowników nie spełniało wymogów określonych w Instrukcji Zarządzania oraz w załączniku do rozporządzenia w sprawie dokumentacji i warunków technicznych (w odniesieniu do liczby znaków określonej w tych przepisach).

   ASI wyjaśnił, że: *„Przyczyną tego były błędne ustawienia w zakresie wymogów hasła na stacji roboczej. Bezpośrednio po oględzinach dokonałem zmiany ustawień w zakresie hasła dostępu"*.

   W trakcie kontroli nieprawidłowość została usunięta.

   (dowód: akta kontroli str. 127-134, 200-204)

3. W Urzędzie nierzetelnie monitorowano dostęp do informacji, bowiem nie był 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. Także informacje o podłączeniu do komputerów nośników pamięci nie były trwale zabezpieczane.

   Ponadto ASI nie nadzorował korzystania przez pracowników firmy ZETO (podczas realizacji prac serwisowych) z aplikacji pulpitu zdalnego TeamViewer zainstalowanej na dwóch komputerach.

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

   ASI wyjaśnił, że: *„Nie został zastosowany zbiorczy rejestr dostępu do systemu w formie elektronicznej, a logi nie były przetwarzane automatycznie ze względu na ograniczenia finansowe i techniczne. Darmowe oprogramowania dostępne na rynku są zbyt skomplikowane do zastosowania w Urzędzie, mają również większe wymagania sprzętowe. Brak zabezpieczenia logów przed modyfikacją i zniszczeniem również wynika z ograniczeń sprzętowych. Nadzorem nad wykonywanymi czynnościami w ramach serwisu zajmują się pracownicy, na komputerach, na których zainstalowano aplikację TeamViewer"*. (dowód: akta kontroli str. 114-134, 170, 194-199, 203-204)

4. Na ośmiu (z 29) stanowiskach komputerowych nie był aktywny wygaszacz ekranu. Zgodnie z § 8 lit. b Instrukcji zarządzania, system powinien być skonfigurowany w sposób zapewniający uruchomienie wygaszacza ekranu, po 10 minutach bezczynności, natomiast wznowienia pracy wymagać powinno ponownego zalogowania się przy użyciu identyfikatora i hasła dostępu.

   ASI wyjaśnił, że: *„Przyczyną była zmiana konfiguracji systemu. Po przeprowadzonych oględzinach zmieniłem ustawienia wygaszacza ekranu na wszystkich komputerach"*.

   W trakcie kontroli nieprawidłowość została usunięta.

   (dowód: akta kontroli str. 46-52, 114-134, 203-204)

5. W jednym przypadku nie podjęto niezwłocznych działań celem cofnięcia uprawnień dostępu do systemu w związku z ustaniem zatrudnienia. Stosunek pracy wygasł 31 marca 2016 r., natomiast cofnięcie uprawnień w systemie SmartDoc nastąpiło 18 sierpnia 2016 r.

   Było to sprzeczne z § 20 ust. 2 pkt 5 rozporządzenia KRI. Zgodnie z powołanym przepisem, zarządzanie bezpieczeństwem informacji realizowane jest poprzez bezzwłoczną zmianę uprawnień w przypadku zmiany zadań osób zaangażowanych w proce przetwarzania informacji.

   ASI wyjaśnił, że: *„Nie pamiętam, co było przyczyną, prawdopodobnie konto nie było usunięte a dezaktywowane"*. (dowód: akta kontroli str. 179-181, 203-204)

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

Opis stanu faktycznego

2.1. Urząd zgłosił do rejestracji GIODO 51 zbiorów danych osobowych, z których 48 zostało zarejestrowanych. GIODO odmówił rejestracji zbiorów: System kadrowo-płacowy, Płatnik i Rejestr wniosków o ukaranie skierowanych do sądu w związku z wyłączeniem obowiązku rejestracji danych przetwarzanych w tych zbiorach. Zarejestrowane zostały w szczególności następujące zbiory: [1] Ulgi podatkowe; [2] Rejestr wydanych zaświadczeń; [3] Decyzje na zwrot podatku akcyzowego na zakupione paliwo; [4] Rejestr podań o przydział mieszkania; [5] Zbiór decyzji podziałowych nieruchomości; [6] Zbiór decyzji na usunięcie drzew; [7] Wykaz nałożonych mandatów karnych; [8] Wykaz wniosków o dofinansowanie zmiany pokrycia dachowego zawierającego azbest; [9] Akta stanu cywilnego; [10] Licencje na wykonywanie transportu drogowego taksówką; [11] Rejestr skarg i wniosków. W okresie objętym kontrolą Urząd nie występował do GIODO o wykreślenie z rejestru zbiorów danych osobowych. Nie zostało zgłoszonych sześć zbiorów danych przetwarzanych w związku z zatrudnieniem oraz dwa zbiory, których przetwarzanie rozpoczęto po powołaniu Administratora Bezpieczeństwa Informacji (dalej: „ABI").

Wszystkie zgłoszenia zbiorów danych do rejestracji zawierały elementy określone w art. 41 ust 1 ustawy o ochronie danych osobowych. Znajdowały się tam bowiem: wniosek o wpisanie zbioru do rejestru zbiorów danych osobowych, oznaczenie administratora danych i adres jego siedziby lub miejsca zamieszkania, w tym numer identyfikacyjny, podstawa prawna upoważniająca do prowadzenia zbioru, cel przetwarzania danych, opis kategorii osób, których dane dotyczą oraz zakres przetwarzanych danych, sposób zbierania oraz udostępniania danych, informacja o odbiorcach lub kategoriach odbiorców, którym dane mogą być przekazywane, opis środków technicznych i organizacyjnych zastosowanych w celach określonych w art. 36 – 39 powołanej ustawy, a w przypadku zbiorów gromadzonych i przetwarzanych w systemach informatycznych – informacja o sposobie wypełnienia warunków technicznych i organizacyjnych, określonych w przepisach, o których mowa w art. 39a ustawy, a także informacja o ewentualnym przekazywaniu danych do państwa trzeciego. (dowód: akta kontroli str. 96-113, 229-246)

2.2. Burmistrz Miasta, zarządzeniem nr 57/15 z dnia 23 czerwca 2015 r. powołał ABI i w tym samym dniu zgłosił ten fakt GIODO, tj. w terminie zgodnym z określonym w art. 46b ust. 1 ustawy o ochronie danych osobowych. Zgłoszenie powołania ABI nastąpiło na wzorze określonym w załączniku nr 1 do rozporządzenia Ministra Administracji i Cyfryzacji z dnia 10 grudnia 2014 r. w sprawie wzorów zgłoszeń powołania i odwołania administratora bezpieczeństwa informacji[8]. Zawierało ono wszystkie elementy wymienione w art. 46b ust. 2 ustawy o ochronie danych osobowych, tj. oznaczenie administratora danych i adres jego siedziby, numer identyfikacyjny rejestru podmiotów gospodarki narodowej, imię i nazwisko ABI oraz numer PESEL, datę powołania, oświadczenie Administratora Danych Osobowych[9] o spełnianiu przez ABI warunków określonych w art. 36a ust. 5 i 7 ww. ustawy. Od 1 stycznia 2016 r. nie było zmian na stanowisku ABI.

(dowód: akta kontroli str. 4-6)

2.3. ABI realizował zadania określone w art. 36a ust. 2 ustawy o ochronie danych osobowych. W okresie objętym kontrolą dokonał pięciokrotnie sprawdzenia zgodności przetwarzania danych osobowych z przepisami o ich ochronie oraz opracował w tym zakresie sprawozdania dla ADO. Sprawozdania zawierały elementy określone w art. 36c ustawy o ochronie danych osobowych, w szczególności: oznaczenie ADO oraz ABI, wykaz czynności podjętych w toku sprawdzenia, imiona, nazwiska i stanowiska osób biorących udział w tych czynnościach, datę rozpoczęcia i zakończenia sprawdzenia, przedmiot i zakres sprawdzenia, opis stanu faktycznego stwierdzonego w toku sprawdzenia. W okresie objętym kontrolą ABI nie stwierdził przypadków naruszenia przepisów o ochronie danych osobowych w zakresie objętym sprawdzeniem.

---

[8] Dz. U. poz. 1934.
[9] Dalej: „ADO".

ABI nadzorował opracowanie i aktualizowanie dokumentacji opisującej sposób przetwarzania danych osobowych oraz środków technicznych i organizacyjnych zapewniających ich ochronę oraz przestrzeganie zasad w nich określonych.
(dowód: akta kontroli str. 12-23)

Zgodnie z § 5 i § 8 Polityki Bezpieczeństwa Informacji[10], osoby upoważnione do przetwarzania danych osobowych zostały zapoznane z przepisami o ich ochronie. Nowo zatrudnieni pracownicy byli szkoleni z zakresu ochrony danych osobowych. Szkolenia dotyczyły m.in. obowiązków osób upoważnionych do przetwarzania danych osobowych, odpowiedzialności za naruszenie zasad przetwarzania i ochrony danych osobowych, a także zapoznanie z obowiązującą w Urzędzie dokumentacją z tego zakresu.
(dowód: akta kontroli str. 31-36, 160)

ABI prowadził rejestr zbiorów danych przetwarzanych przez ADO, w którym zamieszczano nazwy zbiorów oraz informacje określone w art. 41 ust. 1 pkt 2 – 4a i 7 ustawy o ochronie danych osobowych, w szczególności: oznaczenie ADO, cel i podstawę prawną przetwarzania danych, opis kategorii osób, których dane dotyczą, sposób zbierania i udostępniania danych. Rejestr zawierał 53 zbiory danych, w tym jeden powierzony do prowadzenia Miejskiemu Ośrodkowi Pomocy Społecznej.
(dowód: akta kontroli str. 96-113)

2.4. W Urzędzie prowadzona była ewidencja osób upoważnionych do przetwarzania danych osobowych, która obejmowała wszystkich pracowników jednostki. Zawierała ona elementy określone w art. 39 ust. 1 pkt. 1 i 2 ustawy o ochronie danych osobowych, tj. imię i nazwisko osoby upoważnionej, datę nadania i ustania oraz zakres upoważnienia do przetwarzania danych osobowych. W ewidencji nie odnotowano identyfikatora użytkownika w systemie informatycznym (dla danych przetwarzanych i gromadzonych w systemach informatycznych). Było to sprzeczne z art. 39 ust. 1 pkt. 3 ww. ustawy, co szerzej opisano w dalszej części wystąpienia pokontrolnego, w sekcji „Ustalone nieprawidłowości".
(dowód: akta kontroli str. 7-11)

Burmistrz Miasta posiadał aktualne upoważnienie do przetwarzania danych w Systemie Rejestrów Państwowych, wydane przez Ministra Cyfryzacji. Urząd 5 lipca 2017 r. przekazał do Ministra Cyfryzacji wykaz pracowników upoważnionych do przetwarzania danych gromadzonych w ww. systemie oraz 28 kwietnia 2017 r. poinformował o zmianie uprawnień pracowników[11]. (dowód: akta kontroli str. 171-172)

Zakres upoważnień pracowników Urzędu do przetwarzania danych w systemach informatycznych był zgodny z realizowanymi przez nich zadaniami.
(dowód: akta kontroli str. 173-178)

Kwestie związane z obowiązkiem zapewnienia kontroli nad tym, jakie dane osobowe, kiedy i przez kogo zostały wprowadzone do zbioru oraz komu były przekazywane zostały uregulowane w § 15 Instrukcji Zarządzania. Odnotowywane były w szczególności: data pierwszego wprowadzenia danych do systemu, identyfikator użytkownika wprowadzającego dane osobowe, w przypadku pozyskania danych z innego źródła niż osoba, której dotyczą – informacja o pochodzeniu danych, informacja o odbiorcach.
(dowód: akta kontroli str. 59-79)

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. 170)

2.6. Pracownika Urzędu zatrudnionego na stanowisku informatyka powołano, na podstawie upoważnienia z 18 kwietnia 2016 r., na stanowisko ASI. (dowód: akta kontroli str. 24)

---

[10] Polityka zwana dalej: „PBI".

[11] Wygaśnięcie upoważnienia dla jednego pracownika w związku z ustaniem stosunku pracy oraz nadanie uprawnień nowemu pracownikowi w związku z objęciem stanowiska.

2.7. W okresie objętym kontrolą w Urzędzie, wbrew postanowieniom § 20 ust. 2 pkt **14** rozporządzenia KRI, nie był przeprowadzany coroczny audyt wewnętrzny z zakresu bezpieczeństwa informacji (szerzej opisano to w dalszej części wystąpienia pokontrolnego, w sekcji „Ustalone nieprawidłowości"). (dowód: akta kontroli str. 170)

2.8. W 2017 roku pracownikom Urzędu zaangażowanym w proces przetwarzania informacji zapewniono szkolenie z zakresu sposobu postępowania wobec zagrożeń informatycznych. Było ono przeprowadzone przez pracownika Agencji Bezpieczeństwa Wewnętrznego. Sekretarz Miasta, ABI oraz ASI uczestniczyli w szkoleniach z zakresu ochrony danych osobowych, które obejmowały m.in.: podstawy prawne ochrony danych osobowych, zabezpieczenie danych, dokumentację przetwarzania danych oraz planowane zmiany w zakresie ochrony danych osobowych. (dowód: akta kontroli str. 249)

2.9. W okresie objętym kontrolą w Urzędzie nie były przeprowadzane zewnętrzne kontrole w zakresie bezpieczeństwa danych osobowych. Nie wpływały również skargi związane z nieuprawnionymi przypadkami ujawnienia danych osobowych.
(dowód: akta kontroli str. 170)

2.10. W Urzędzie opracowano i wdrożono dokumentację związaną z przetwarzaniem danych osobowych: zarządzeniem Burmistrza Miasta z 25 maja 2012 r. – Politykę Bezpieczeństwa Danych Osobowych[12], zarządzeniem z 12 kwietnia 2016 r. – PBI i Instrukcję Zarządzania. (dowód: akta kontroli str. 30-53, 59-79)

Polityka Bezpieczeństwa Danych zawierała wszystkie elementy określone w § 4 rozporządzenia w sprawie dokumentacji i 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, [4] sposób przepływu danych pomiędzy poszczególnymi systemami, [5] określenie środków technicznych i organizacyjnych niezbędnych dla zapewnienia poufności, integralności i rozliczalności przetwarzanych danych.
(dowód: akta kontroli str. 59-79)

Instrukcja Zarządzania zawierała siedem (z ośmiu) elementów określonych w § 5 rozporządzenia w sprawie dokumentacji i warunków technicznych, tj.: [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. Nie zawierała natomiast opisu procedury wykonywania przeglądów i konserwacji systemów oraz nośników informacji służących do przetwarzania danych, tj. elementu wymaganego § 5 pkt 8 rozporządzenia w sprawie dokumentacji i warunków technicznych (szerzej problem opisano w dalszej części wystąpienia pokontrolnego, w sekcji „Ustalone nieprawidłowości"). (dowód: akta kontroli str. 59-79)

W Instrukcji Zarządzania wprowadzony został wysoki poziom bezpieczeństwa (wszystkie urządzenia systemów informatycznych związane z przetwarzaniem danych osobowych były połączone z siecią publiczną[13]), co odpowiadało wymaganiom określonym w § 6 rozporządzenia w sprawie dokumentacji i warunków technicznych. Zapisy Instrukcji Zarządzania odpowiadały wymogom wskazanym w załączniku do rozporządzenia w sprawie dokumentacji i warunków technicznych. (dowód: akta kontroli str. 59-79)

---

[12] Dalej: „Polityka Bezpieczeństwa Danych".
[13] Poza stanowiskami wydzielonymi do obsługi Systemu Rejestrów Państwowych.

W Urzędzie nie wprowadzono regulacji składających się na politykę bezpieczeństwa informacji, mimo wymogów określonych w § 2 pkt 15 w związku z § 20 ust. 1 rozporządzenia KRI dotyczącej ochrony wszystkich danych będących w posiadaniu jednostki, co szerzej opisano poniżej, w sekcji „Ustalone nieprawidłowości".

(dowód: akta kontroli str. 170)

Ustalone nieprawidłowości

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

1. Prowadzona w Urzędzie ewidencja osób upoważnionych do przetwarzania danych, wbrew wymogom art. 39 ust. 1 pkt 3 ustawy o ochronie danych osobowych, nie zawierała identyfikatora użytkownika w systemie informatycznym.

   Burmistrz Miasta wyjaśnił, że: *„Ewidencja 30 listopada 2017 r. została uzupełniona o brakujące dane"*. (dowód: akta kontroli str. 7-11, 254-263, 265-267)

2. W Urzędzie nie był przeprowadzany okresowy audyt wewnętrzny w zakresie bezpieczeństwa informacji, co było niezgodne z przepisem § 20 ust. 2 pkt 14 rozporządzenia KRI, w myśl którego bezpieczeństwo informacji realizowane jest poprzez zapewnienie przeprowadzenia audytu nie rzadziej niż raz na rok.

   Burmistrz wyjaśnił, że: *„W Rozporządzeniu Rady Ministrów z dnia 12 kwietnia 2012 r. w sprawie Krajowych Ram Interoperacyjności wskazano jedynie sam obowiązek prowadzenia corocznego audytu wewnętrznego, bez określenia, jakichkolwiek wymogów w zakresie sposobu oraz trybu realizacji czy też formy prowadzonych audytów oraz wymogów stawianych osobom, które miałyby realizować niniejsze zadanie. Pojawiające się oferty firm proponujących przeprowadzenie audytu mówiły o różnym jego zakresie, a w związku z brakiem jednoznacznych wytycznych, nie korzystaliśmy z zewnętrznego audytu. Pracownicy urzędu mają świadomość o bezpieczeństwie informacji w szeroko pojętym znaczeniu i na bieżąco czuwają przy wykonywaniu czynności, aby były zachowane wszelkie możliwe zasady bezpieczeństwa informacji"*.

   (dowód: akta kontroli str. 170, 265-267)

3. Instrukcja Zarządzania nie zawierała opisu procedury wykonywania przeglądów i konserwacji systemów oraz nośników informacji służących do przetwarzania danych, tj. elementu wymaganego § 5 pkt 8 rozporządzenia w sprawie dokumentacji i warunków technicznych.

   ABI wyjaśnił, że: *„Brak tego elementu Instrukcji Zarządzania Systemem Informatycznym wynika z przeoczenia"*. (dowód: akta kontroli str. 46-52, 205)

4. W regulacjach składających się na politykę bezpieczeństwa informacji, o której mowa w § 2 pkt 15 rozporządzenia KRI, nie uwzględniono części wymogów określonych w § 20 ust. 1 ww. rozporządzenia. Rozwiązania przyjęte w Instrukcji zarządzania i w politykach bezpieczeństwa dotyczyły jedynie ochrony danych osobowych, nie regulowały natomiast całościowych procedur związanych z bezpieczeństwem informacji.

   Burmistrz wyjaśnił, że: *„Brak całościowej polityki bezpieczeństwa informacji wynika z przekonania, że przyjęte w urzędzie przepisy wewnętrzne w przedmiocie zabezpieczenia danych osobowych i bezpieczeństwa informacji są wystarczające i kompletne"*.

   Polityka bezpieczeństwa obejmuje zbiór przepisów, reguł i praktyk, które regulują sposób zarządzania, ochrony i dystrybucji zasobów przez jednostkę dążącą do osiągnięcia określonych celów bezpieczeństwa.

   (dowód: akta kontroli str. 25-70, 170, 265-267)

Ocena cząstkowa

Najwyższa Izba Kontroli ocenia pozytywnie mimo stwierdzonych nieprawidłowości działalność Urzędu dotyczącą opracowania i wdrożenia dokumentacji oraz procedur ochrony danych i zgłaszania rejestracji zbiorów do GIODO, a także realizację ustawowych zadań przez ABI.

3. Sposób przechowywania oraz zabezpieczenia danych

Opis stanu faktycznego

3.1. W załączniku do PBI „Wykaz pomieszczeń, w których przetwarzane są dane osobowe" określony został sposób ich zabezpieczenia: [1] alarm przeciwwłamaniowy, [2] gaśnice, [3] czujnik oddymienia, [4] szafki i pomieszczenia zamykane na klucz. W wyniku oględzin stwierdzono, że zastosowane zabezpieczenia były zgodne z założonymi. W PBI nie były określone dodatkowe wymagania dla pomieszczeń przeznaczonych na archiwum. W wyniku przeprowadzonych oględzin stwierdzono, że pomieszczenie archiwum zostało wyposażone w czujnik ruchu i wilgoci, a na korytarzu, bezpośrednio przy archiwum, znajdowała się gaśnica.

W Urzędzie nie była wprowadzona polityka kluczy, natomiast wyznaczone było pomieszczenie do ich przechowywania. Kopie zapasowe zbiorów danych oraz elektroniczne nośniki informacji zawierające dane osobowe były przechowywane w sposób zgodny z określonym w § 9 i § 10 Instrukcji zarządzania. (dowód: akta kontroli str. 46-52, 135-138)

3.2. ASI w myśl przepisu § 20 ust. 2 pkt. 2 rozporządzenia KRI prowadził rejestr zasobów informatycznych, który obejmował typ i model sprzętu, numer seryjny, zainstalowany system operacyjny wraz z datą aktualizacji, nazwę użytkownika oraz miejsce lokalizacji. Nie obejmował on zaś informacji o zainstalowanych programach i aplikacjach oraz posiadanych licencjach, co szerzej opisano w dalszej części wystąpienia pokontrolnego, w sekcji „Ustalone nieprawidłowości". (dowód: akta kontroli str. 94-95)

3.3. W okresie objętym kontrolą w Urzędzie nie dokonywano likwidacji / naprawy sprzętu będącego nośnikiem danych. (dowód: akta kontroli str. 170)

3.4. Niszczenie dokumentów w Urzędzie, zgodnie z § 13 PBI, odbywało się za pomocą niszczarek. Do tego celu Urząd wyposażono w trzy niszczarki.
(dowód: akta kontroli str. 31-36, 135-138)

3.5. W Urzędzie z komputerów przenośnych korzystał Burmistrz Miasta i Sekretarz. W PBI pracowników użytkujących komputery przenośne zobowiązano do zachowania szczególnej ostrożności podczas jego transportu, przechowywania i użytkowania poza obszarem przetwarzania danych oraz do zabezpieczenia hasłem plików lub folderów zawierających dane osobowe. Pracownikom nie umożliwiono zdalnego dostępu do zasobów sieci lokalnej Urzędu. (dowód: akta kontroli str. 46-53)

3.6. Sprzątanie pomieszczeń, w których przetwarzano dane osobowe odbywało się od 14^{00} do 22^{00}, tj. poza godzinami pracy Urzędu. Osoby sprzątające uzyskały zgodę ADO na przebywanie w obszarze przetwarzania danych poza godzinami pracy Urzędu, stosownie do przepisu rozdz. A ust. 1 pkt 1 załącznika do rozporządzenia w sprawie dokumentacji i warunków technicznych. Natomiast sprzątanie pomieszczenia serwerowni odbywało się pod nadzorem ASI.

Zgodnie z przyjętymi w Urzędzie uregulowaniami, dokumenty zawierające dane osobowe powinny być przechowywane w szafach zamykanych na klucz, a za prawidłowe zabezpieczenie danych osobowych oraz miejsc ich przechowywania w trakcie i po zakończeniu pracy odpowiedzialni byli kierownicy referatów.
(dowód: akta kontroli str. 161-168)

3.7. W Urzędzie nie opracowano procedur wykonywania przeglądów i konserwacji systemów oraz nośników informacji służących do przetwarzania danych, co szerzej opisano w obszarze nr 2 wystąpienia pokontrolnego, w sekcji „Ustalone nieprawidłowości".
(dowód: akta kontroli str. 46-52)

3.8. W Urzędzie nie były przygotowane rozwiązania na wypadek wystąpienia sytuacji nadzwyczajnych, np. awarii, długotrwałego braku zasilania. Nie opracowano również procedur dotyczących przywracania systemów po awarii oraz planu ciągłości działania umożliwiającego kontynuację wykonywania zadań publicznych (co szerzej opisano w dalszej części wystąpienia pokontrolnego, w sekcji „Uwagi dotyczące badanej działalności"). Jeden komputer został zabezpieczony przed utratą zasilania, za pomocą zasilacza awaryjnego UPS, na pozostałych zastosowano listwy przepięciowe. Serwerownię Urzędu wyposażono w UPS. Opracowano natomiast sposób tworzenia i przywracania kopii

zapasowych. Urząd nie posiadał dodatkowego źródła zasilania na wypadek długotrwałych przerw w dostawie prądu.

ASI wyjaśnił, że: *„Stanowiska komputerowe nie zostały wyposażone w zasilacze UPS, ponieważ przerwy w dostawach prądu zdarzają się bardzo rzadko (raz w roku), komputery nie przechowują danych ważnych dla urzędu, a bazy danych są umieszczone na serwerach zasilanych z UPSów. Ponadto zakup i utrzymanie około 30 UPS-ów jest nieopłacalny ekonomicznie (w urzędzie brak wydzielonej sieci zasilającej dla UPS-a centralnego)".*

(dowód: akta kontroli str. 46-52, 200-204)

3.9. W Urzędzie od 1 stycznia 2016 r. do 1 grudnia 2017 r. nie wystąpiły przypadki fizycznej utraty danych. (dowód: akta kontroli str. 170)

Ustalone nieprawidłowości

W działalności jednostki w przedstawionym wyżej zakresie stwierdzono nieprawidłowość, polegającą na nieujęciu w rejestrze zasobów informatycznych, wbrew wymogom § 20 ust. 2 pkt 2 rozporządzenia KRI, informacji o oprogramowaniu służącym do przetwarzania danych, obejmującej jego rodzaj i konfigurację. Zgodnie z przywołanym przepisem, zarządzanie bezpieczeństwem informacji realizowane jest w szczególności przez zapewnienie przez kierownictwo podmiotu publicznego warunków umożliwiających realizację i egzekwowanie działań utrzymywania aktualności inwentaryzacji sprzętu i oprogramowania służącego do przetwarzania informacji, obejmującej ich rodzaj i konfigurację.

ASI wyjaśnił, że: *„Prowadzony rejestr jest wykonywany automatycznie przez aplikację GLPI. Aplikacja ta gromadziła zbyt dużo danych, przez co rejestr stawał się nieczytelny".*

(dowód: akta kontroli str. 94-95, 200-204)

Uwagi dotyczące badanej działalności

Najwyższa Izba Kontroli zwraca uwagę na potrzebę opracowania wewnętrznych regulacji dotyczących rozwiązań na wypadek wystąpienia sytuacji nadzwyczajnych, np. długotrwałego braku zasilania bądź przywracania systemów po awarii, a także planu ciągłości działania umożliwiającego kontynuację wykonywania zadań jednostki. Plan ten powinien określić systemy i aplikacje o znaczeniu krytycznym oraz wszystkie podporządkowane lub powiązane plany. Istotne jest, aby plany te były jasno udokumentowane, przekazane pracownikom i aktualizowane w celu odzwierciedlenia bieżącej działalności Urzędu. Ponadto obowiązek zabezpieczenia systemu informatycznego służącego do przetwarzania danych osobowych przed utratą danych spowodowaną awarią zasilania lub zakłóceniami w sieci zasilającej wynika z regulacji rozdz. A pkt. III załącznika do rozporządzenia w sprawie dokumentacji i warunków technicznych.

(dowód: akta kontroli str. 170)

Ocena cząstkowa

Najwyższa Izba Kontroli ocenia pozytywnie mimo stwierdzonej nieprawidłowości działania Urzędu dotyczące przestrzegania przyjętych procedur w zakresie przechowywania i zabezpieczania danych, które zapewniały ich właściwą ochronę.

4. Przetwarzanie zasobów informacyjnych zgodnych z zakresem działalności jednostki kontrolowanej

Opis stanu faktycznego

4.1. W Urzędzie prowadzono 58 zbiorów danych[14], w tym 44 w formie papierowej i 14 w formie elektronicznej. Do gromadzenia i przetwarzania danych wykorzystywano systemy: [1] Fiskus, w którym prowadzono: *Decyzje na zwrot podatku akcyzowego na zakupione paliwo, Ulgi podatkowe, Podatki lokalne, Deklaracje o wysokości opłaty za gospodarowanie odpadami komunalnymi*; [2] SUMPRO – *Ewidencja mandatów karnych*; [3] ZRÓDŁO i SelWin: *Rejestr mieszkańców, Rejestr zamieszkania cudzoziemców, Dowody osobiste, Akta stanu cywilnego, Rejestr wyborców*; [4] SmartDoc: *Dziennik korespondencji*; [5] System Informacji Oświatowej; [6] CEiDG: *Działalność gospodarcza*; [7] *System kadrowo-płacowy*; [8] *Płatnik*. (dowód: akta kontroli str. 96-113)

4.2. W okresie objętym kontrolą nie aktualizowano zbiorów danych zgłoszonych do GIODO. Na podstawie analizy 10 zbiorów stwierdzono, że w dwóch zakres przetwarzanych danych był zgodny z danymi wskazanymi w zgłoszeniach do GIODO, a w pozostałych ośmiu

[14] Jeden zbiór *Karta dużej rodziny* powierzono do prowadzenia Miejskiemu Ośrodkowi Pomocy Rodzinie.

przetwarzano dane w szerszym zakresie niż zgłoszono, co szerzej opisano w dalszej części wystąpienia pokontrolnego, w sekcji „Ustalone nieprawidłowości".

(dowód: akta kontroli str. 182-193)

4.2. W ośmiu (z 10) objętych analizą zbiorach danych zakres gromadzonych i przetwarzanych danych osobowych był niezbędny do realizacji zadań, które zostały przypisane Urzędowi, a w dwóch zbiorach zakres gromadzonych danych był większy niż wymagany do realizacji zadań (szerzej problem opisano poniżej, w sekcji „Ustalone nieprawidłowości"). (dowód: akta kontroli str. 184-193)

Urząd wywiązał się z obowiązku poinformowania kandydatów do pracy o konieczności zawarcia w dokumentach aplikacyjnych klauzuli dotyczącej zgody na przetwarzanie danych osobowych do celów realizacji procesu rekrutacji, tj. zgodnie z ustawą o ochronie danych osobowych. (dowód: akta kontroli str. 247-248)

4.4. Urząd posiadał dostęp do zewnętrznych zbiorów danych osobowych: ŹRÓDŁO i CEiDG. Dostęp do systemu ŹRÓDŁO uzyskał na podstawie upoważnienia z 4 stycznia 2016 r. nadanego przez Ministra Spraw Wewnętrznych. Urząd spełnił wymogi związane z dostępem do tego systemu: trzy stanowiska komputerowe do obsługi systemu nie posiadały dostępu do Internetu, a pracownicy uzyskali stosowne upoważnienia. Dostęp do systemu CEiDG posiadał jeden pracownik Urzędu, który uzyskał go na podstawie zgłoszenia do Ministerstwa Rozwoju. (dowód: akta kontroli str. 171-172, 180-181)

Ustalone nieprawidłowości

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

1. Zakres danych w ośmiu (z 10) zbiorów danych był szerszy niż wskazany w zgłoszeniach do GIODO. Przetwarzane dane obejmowały dodatkowo numer telefonu, adres poczty elektronicznej, datę urodzenia, nr rachunku bankowego.

   Burmistrz Miasta wyjaśnił, że: *„(...) dane osobowe typu nr telefonu, adres e-mail były podawane przez petentów dobrowolnie w celu usprawnienia załatwienia sprawy i szybszego kontaktu z klientem urzędu. (...) zakres danych przetwarzanych w zbiorach zostanie rozszerzony o dane faktycznie gromadzone."*

   (dowód: akta kontroli str. 182-193, 265-267)

2. W Urzędzie gromadzono i przetwarzano dane w dwóch (z 10 objętych analizą) zbiorach, które nie były wykorzystywane (niezbędne) do realizacji zadań, dla których zbiory te były prowadzone. W zbiorze danych „Rejestr podań o przydział mieszkania" gromadzono i przetwarzano dane wynikające z dokumentacji medycznej (otrzymanej od wnioskodawców, Urząd nie wymagał przedkładania takich dokumentów). Natomiast zgodnie z zasadami wynajmowania lokali wchodzących w skład mieszkaniowego zasobu miasta Wysokie Mazowieckie[15] jedynym kryterium przydziału mieszkań był dochód. W zbiorze danych „Zbiór decyzji na usunięcie drzew" gromadzono i przetwarzano dane (pobrane z wypisu z rejestru gruntów) takie jak: imiona rodziców, numer NIP, numer Pesel, mimo że przepisy art. 83b ust. 1 ustawy z dnia 16 kwietnia 2004 r. o ochronie przyrody[16] nie wymagają podania tych danych we wniosku o wydanie zezwolenia na usunięcie drzewa lub krzewu.

   Przetwarzanie ww. danych było sprzeczne z art. 23 ust. 1 pkt 2 ustawy o ochronie danych osobowych. Zgodnie z tym przepisem przetwarzanie danych jest dopuszczalne tylko wtedy, gdy jest to niezbędne dla zrealizowania uprawnienia lub spełnienia obowiązku wynikającego z przepisu prawa.

   Burmistrz Miasta wyjaśnił, że dane zostaną zanonimizowane.

   (dowód: akta kontroli str. 182-183, 187-188, 265-267)

Ocena cząstkowa

Najwyższa Izba Kontroli ocenia pozytywnie mimo stwierdzonych nieprawidłowości sposób przetwarzania zasobów informacyjnych, który był zgodny z zakresem działalności Urzędu, a w odniesieniu do zbiorów zewnętrznych – spełniał wymogi związane z dostępem do tych zbiorów.

---

[15] Zasady przyjęte uchwałą nr XLII/190/02 Rady Miasta Wysokie Mazowieckie z 22 marca 2002 r.
[16] Dz. U. z 2018 poz. 2134 ze zm.

IV. Wnioski

Wnioski pokontrolne

Przedstawiając powyższe oceny 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[17] wnosi o:

1. Przeprowadzanie okresowych analiz ryzyka utraty integralności, dostępności lub poufności informacji, a także przeglądów i konserwacji systemów informatycznych.
2. Podejmowanie niezwłocznych działań celem cofnięcia uprawnień dostępu do systemu w związku z ustaniem zatrudnienia.
3. Prowadzenie rejestru zasobów informatycznych zgodnie z wymogami określonymi w § 20 ust. 2 pkt 2 rozporządzenia KRI.
4. Monitorowanie dostępu do zasobów informacyjnych Urzędu.
5. Przeprowadzanie, nie rzadziej niż raz w roku, okresowego audytu bezpieczeństwa informacji.
6. Dostosowanie zapisów Instrukcji Zarządzania do wymogów § 5 rozporządzenia w sprawie dokumentacji i warunków technicznych oraz wprowadzenie regulacji stanowiących politykę bezpieczeństwa informacji, zgodnie z § 2 pkt 15 w związku z § 20 ust. 1 rozporządzenia KRI.
7. Aktualizowanie zbiorów danych zgłoszonych do GIODO.
8. Gromadzenie danych w zbiorach w zakresie niezbędnym do realizowania przypisanych zadań.

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 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.

Białystok, dnia 15 stycznia 2018 r.

Kontroler
Beata Palinowska
starszy inspektor kontroli państwowej

Palinowska Beata
podpis

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

podpis

[17] Dz. U. z 2017 r. poz. 524. Ustawa zwana dalej „ustawą o NIK".