NAJWYŻSZA IZBA KONTROLI
Delegatura w Białymstoku

LBI.410.023.02.2017
P/17/062

02263817

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, upoważnienia do kontroli nr LBI/152/2017 z 3 listopada 2017 r. i nr LBI/3/2018 z 2 stycznia 2018 r. (dowód: akta kontroli str. 1-4)
Jednostka kontrolowana	Urząd Miejski w Nowogrodzie, ul. Łomżyńska 41, 18-414 Nowogród (zwany dalej: „Urzędem")
Kierownik jednostki kontrolowanej	Grzegorz Andrzej Palka – Burmistrz Nowogrodu[1] (dowód: akta kontroli str. 5, 198-199)

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, która odpowiadała przepisom oraz przyjętym procedurom.

Stwierdzone nieprawidłowości polegały 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 Generalnemu Inspektorowi Ochrony Danych Osobowych (dalej: „GIODO") do zarejestrowania pięciu z 18 przetwarzanych w Urzędzie zbiorów danych osobowych,
- przetwarzaniu danych w zbiorach danych osobowych przez trzech (z 19) pracowników merytorycznych Urzędu, bez upoważnienia Burmistrza,
- 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[4],
- nieuwzględnieniu w regulacjach składających się na politykę bezpieczeństwa informacji, o której mowa w § 2 pkt 15 rozporządzenia KRI, wszystkich wymogów określonych w § 20 ust. 1 ww. rozporządzenia.

---

1 Od 4 września 2017 r. Od 1 grudnia 2014 r. do 5 czerwca 2017 r. burmistrzem był Józef Piątek. W związku z jego śmiercią, do pełnienia tej funkcji wyznaczono Krzysztofa Tomasza Niewiadomskiego (od 13 lipca do 3 września 2017 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 Dz. U. z 2017 r. poz. 2247. 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. System informatyczny Urzędu zbudowany był w architekturze klient – serwer. Sieć nie była zarządzana przez domenę Windows. Centralną jednostką sieci był serwer pracujący na Microsoft Windows Serwer 2003, pełniący funkcję serwera aplikacji. Drugi serwer, posadowiony na Microsoft Windows Serwer 2008, działał jako serwer bazy danych. Był on niezbędny do pracy specjalistycznych programów wspomagających pracę Urzędu. Odrębnym urządzeniem był serwer plików, zrealizowany na Windows Serwer 2012. Równolegle, bez podłączenia do sieci LAN Urzędu, działały dwa serwery – serwer Dziennika Elektronicznego i serwer elektronicznego obiegu dokumentów. Wymienione urządzenia, wraz z urządzeniami sieciowymi, zostały umieszczone w wydzielonej, dostępnej uprawnionemu personelowi, klimatyzowanej serwerowni.

Sieć komputerowa w Urzędzie oparta został na routerze firmy CISCO, który administrowany był przez Urząd Marszałkowski Województwa Podlaskiego („UMWP"). Administrator systemu informatycznego Urzędu nie posiadał do niego danych dostępowych. Monitorowanie pracy wspomnianego urządzenia leżało po stronie Urzędu Marszałkowskiego. Do tego celu zestawiono VPN do UMWP (jedyny VPN do sieci Urzędu).

Dostęp do Internetu realizowany był poprzez łącze DSL. Sieć odseparowana była od Internetu firewallem, stanowiącym integralną część routera CISCO, odpowiedzialnego za zarządzanie siecią. Sieć oparta została na protokole DHCP, bez filtracji MAC adresów, ze stałą adresacją IP zasobów sieci. (dowód: akta kontroli str. 39-45)

Do prowadzenia zbiorów danych osobowych w wersji elektronicznej wykorzystywanych było 11 systemów informatycznych, tj.: SRP ŹRÓDŁO, SELWIN, EMUiA, SIO, CEIDG, SmartDoc, Fiskus (Gospodarka odpadami), Podatki (Pakiet), Besti@, QNT (Pakiet), Internet Banking oraz oprogramowanie biurowe – arkusze programu MS-Word i MS-Excel.
(dowód: akta kontroli str. 46-57, 150-172)

W budynku Urzędu pracowały 22 komputery, z których 16 wchodziło w skład sieci LAN, cztery komputery (trzy stacje robocze i laptop) służyły do obsługi aplikacji ŹRÓDŁO (aplikacja do obsługi Systemu Rejestrów Państwowych), zaś dwa (stacja robocza i laptop) pełniły funkcję „maszyn do pisania". Na trzech zainstalowano system Windows 7, na jednym – Windows Vista, a na pozostałych 18 – Windows 10.

Oględziny wszystkich 15 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[5],
- 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. 46-57)

1.2. W latach 2016 – 2017 (do 6 grudnia) 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. 107)

---

[5] 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). Rozporządzenie zwane dalej: „rozporządzeniem w sprawie dokumentacji oraz warunków technicznych".

1.3. Według stanu na 6 grudnia 2017 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 na nich konta administratora i użytkownika (z ograniczonymi uprawnieniami), które zostały zabezpieczone hasłem. Zastosowano okresowe wymuszenie zmiany hasła. Użytkownicy komputerów nie posiadali uprawnień do instalacji oprogramowania, zmiany uprawnień czy usuwania plików systemowych. Wszystkie aktualizacje oprogramowania komputerów, w tym specjalistycznego oprogramowania, aktualizacji systemowych i aplikacji antywirusowych, odbywały się automatycznie, zgodnie z harmonogramem domyślnie ustawionym przez producenta. Wszystkie zbadane komputery posiadały aktualne systemy operacyjne, bazy zagrożeń aplikacji bezpieczeństwa i oprogramowanie specjalistyczne.
(dowód: akta kontroli str. 39-57, 113-116, 134)

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 – nie znany był zakres ustawień routera, gdyż był on administrowany poza Urzędem. Informacje zawarte w logach nie były przetwarzane automatycznie przez administratora sytemu. Logi zapisane na końcówkach klienckich nie były zabezpieczone przed modyfikacją i zniszczeniem. Logi routera, serwera i aplikacji na nim działających były zabezpieczone 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. 39-45)

1.5. Ustalenia biegłego wskazują, że wszystkie komputery posiadały założone konto administratora i użytkownika. Każde z nich zabezpieczono hasłem. Wdrożona była procedura okresowej zmiany hasła. Urządzenia sieciowe chroniono przed nieautoryzowanym fizycznym dostępem poprzez umieszczenie ich w zamkniętej serwerowni. Urządzenia pracujące w serwerowni były zabezpieczone hasłem, co wykluczało nieautoryzowany dostęp do nich. Na terenie Urzędu nie działała sieć Wi-Fi.
(dowód: akta kontroli str. 39-45)

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. Po podłączeniu takiego sprzętu nie było możliwości korzystania z zasobów sieciowych jednostki. 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. 39-45)

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. 107)

1.8. Biegły stwierdził, że w Urzędzie nie przewidziano zdalnego dostępu do zasobów sieci lokalnej przez pracowników. Na routerze CISCO zestawiony był VPN z siecią UMWP. Był on wykorzystywany do zarządzania routerem. 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 korzystali pracownicy ZETO Białystok przy realizacji prac serwisowych. (dowód: akta kontroli str. 39-45)

1.9. Urząd, na dzień kontroli, z podmiotami zewnętrznymi zawarte miał dwie umowy serwisu oprogramowania. Tylko w jednej z nich zawarto regulacje zobowiązujące wykonawcę do zachowania w tajemnicy i nieudostępniania danych osobowych przekazanych przez Urząd. Ponadto wykonawca zobowiązał się w szczególności do: [1] zastosowania środków technicznych i organizacyjnych zapewniających ochronę przetwarzania danych osobowych, a w szczególności zabezpieczenia danych przed ich 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 drugiej umowie szerzej opisano w dalszej części wystąpienia pokontrolnego, w sekcji „Ustalone nieprawidłowości". (dowód: akta kontroli str. 58-66)

1.10. Wszystkie komputery (16) wchodzące w skład sieci lokalnej były zabezpieczone dedykowanym do tego oprogramowaniem. Posiadały one aktualne wersje aplikacji zabezpieczających. Dostęp do sieci lokalnej kontrolowany był przez firewall zainstalowany na routerze CISCO. Biegły stwierdził, że zastosowanie aplikacji bezpieczeństwa, która posiadałaby moduł centralnego zarządzania oprogramowaniem pozwoliło by na znacznie większą kontrolę nad działaniem systemu. (dowód: akta kontroli str. 39-45)

1.11. Serwer poczty Urzędu znajdował się na platformie regionalnej Wrota Podlasia, utworzonej w wyniku realizacji projektu pn. „Wdrażanie elektronicznych usług dla ludności województwa podlaskiego – część II, administracja samorządowa". Ustawienia poczty pozwalały na zabezpieczenie przed wiadomościami typu SPAM, a programy antywirusowe chroniły przed przesyłaniem plików zawierających szkodliwe oprogramowanie.
(dowód: akta kontroli str. 67-87)

1.12. Backupy baz danych programów wykorzystywanych w Urzędzie robione były codziennie. Zapisywano je na dysku zewnętrznym i przechowywano przez 30 dni. Raz w tygodniu backup był wgrywany na nośnik optyczny, który przechowywano w odosobnionym, bezpiecznym miejscu (szafa metalowa). Pliki użytkowników z poszczególnych komputerów backupowano w razie zaistnienia takiej konieczności.
(dowód: akta kontroli str. 39-45, 131)

1.13. Biegły stwierdził, że pracownicy Urzędu dysponowali możliwością ściągania aplikacji i plików wykonalnych, ale nie posiadali uprawnień pozwalających na instalowanie ich na stacjach komputerowych, do których mieli dostęp. Uprawnienia do konfiguracji systemów komputerów działających w Urzędzie posiadał wyłącznie administrator. Oględziny wszystkich komputerów Urzędu wykazały, że zainstalowane na nich systemy operacyjne były aktualne i objęte wsparciem technicznym producenta. W Urzędzie prowadzono też książkę inwentarzową wartości niematerialnych i prawnych, w której ewidencjonowano programy zainstalowane na stacjach komputerowych. (dowód: akta kontroli str. 39-57, 131)

1.14. Biegły stwierdził, że wszystkie zbadane komputery posiadały aktualne wersje systemów operacyjnych (poza komputerami służącymi do aplikacji Źródło) i aplikacji bezpieczeństwa. Aktualizacje były wykonywane zgodnie z harmonogramem domyślnie ustawionym przez dostawcę systemu operacyjnego. Aktualne były również wersje specjalistycznego oprogramowania zainstalowanego na komputerach i na serwerze.
(dowód: akta kontroli str. 39-45)

1.15. W Urzędzie nie opracowano procedur związanych z płatnościami realizowanymi drogą elektroniczną. Były one realizowane za pośrednictwem elektronicznego systemu zdalnej obsługi bankowej. Dane przekazywane między Urzędem a bankiem były przesyłane łączem szyfrowanym. Realizacja zleconych przez Urząd przelewów była wykonywana przez upoważnionych pracowników, którzy posiadali klucze autoryzujące, zabezpieczone kodami PIN. (dowód: akta kontroli str. 88-90)

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. Burmistrz wyjaśnił, że: *„nie przeprowadzono takich analiz ze względu na ograniczone możliwości finansowe. Nadmieniam, iż aktualnie trwają prace nad dostosowaniem obecnych struktur do nowych przepisów GDPR[6] w celu wypełnienia ustawowych obowiązków".* (dowód: akta kontroli str. 107, 215-217)

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 referenta ds. obsługi informatycznej, a logi zapisywane na końcówkach klienckich nie były zabezpieczone przed modyfikacją i zniszczeniem. Ponadto referent ds. obsługi informatycznej nie nadzorował korzystania przez pracowników firmy ZETO (podczas realizacji prac serwisowych) z zainstalowanej na trzech komputerach aplikacji pulpitu zdalnego TeamViewer.

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

   Referent ds. obsługi informatycznej 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. 39-45, 108-110)

3. W okresie objętym kontrolą w jednej (z dwóch) zawartych przez Urząd umów dotyczących świadczenia usługi serwisu eksploatacyjnego oprogramowania komputerowego nie ujęto regulacji zobowiązujących wykonawcę do przestrzegania ustawy z dnia 29 sierpnia 1997 r. o ochronie danych osobowych[7] oraz przepisów o ochronie informacji niejawnych. 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: *„umowa była przygotowana przez firmę serwisową. Została skonsultowana przez naszego radcę prawnego, który nie wniósł do niej uwag. Umowa ta obowiązuje do końca 2017 r. Obecnie jesteśmy na etapie konsultacji nowej umowy, która będzie już zawierała zapisy gwarantujące odpowiedni poziom bezpieczeństwa informacji".* (dowód: akta kontroli str. 64-66, 111-112)

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

Opis stanu faktycznego

2.1. W Urzędzie dane były przetwarzane w 18 zbiorach, z których dziewięć prowadzono wyłącznie w wersji elektronicznej, osiem w wersji papierowej, a jeden w wersji elektronicznej i papierowej. Do GIODO zgłoszono 13 z nich, pozostałe pięć nie zostało zarejestrowane, co szerzej opisano w dalszej części wystąpienia pokontrolnego, w sekcji „Ustalone nieprawidłowości". Zakres danych we wszystkich zarejestrowanych zbiorach odpowiadał

---

[6] General Data Protection Regulation – rozporządzenie Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (Dz.U.UE.L.2016.119.1.).

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

zakresowi, w jakim były one przetwarzane. W okresie objętym kontrolą Urząd nie aktualizował danych rejestracyjnych zbiorów zgłoszonych do GIODO.

GIODO odmówił rejestracji zbioru „Kadry", który w jego opinii jest zwolniony z tego obowiązku, zgodnie z art. 43 ust. 1 pkt 4 ustawy o ochronie danych osobowych.

(dowód: akta kontroli str. 94-106)

2.2. W Urzędzie do 12 grudnia 2017 r. nie skorzystano z możliwości powołania Administratora Bezpieczeństwa Informacji (dalej: „ABI"), o której mowa w art. 36a ust. 1 ustawy o ochronie danych osobowych. Burmistrz wyjaśnił, że pełni tę funkcję dopiero od września 2017 roku i był przekonany, że wyznaczony w 2013 roku przez poprzedniego Burmistrza ABI (tj. referent ds. obsługi informatycznej Urzędu) sprawuje tę funkcję nadal. Nie miał świadomości, że w związku ze zmianą przepisów o ochronie danych osobowych w 2015 roku należało ponownie powołać ABI oraz zgłosić do rejestracji GIODO fakt jego powołania. Tak więc nie wiedział, że w przypadku niewyznaczenia ponownego ABI, realizacja zadań określonych w art. 36a ust 2 pkt 1 ustawy o ochronie danych osobowych, należy do niego. (dowód: akta kontroli str. 7-29, 117-118, 215-217)

2.3. W Polityce bezpieczeństwa (rozdział I pkt 3) zobowiązano ABI do realizacji zadań w zakresie ochrony danych, a w szczególności do: [1] ochrony i bezpieczeństwa danych osobowych zawartych w zbiorach systemów informatycznych w Urzędzie; [2] podejmowania stosownych działań zgodnie z „Polityką bezpieczeństwa" w przypadku wykrycia nieuprawnionego dostępu do bazy danych lub naruszenia zabezpieczenia danych znajdujących się w systemie informatycznym; [3] niezwłocznego informowania Administratora Danych Osobowych („ADO") lub osoby przez niego upoważnionej o przypadkach naruszenia przepisów o ochronie danych osobowych; [4] nadzoru i kontroli systemów informatycznych służących do przetwarzania danych osobowych oraz osób przy nim zatrudnionych; [5] prowadzenia ewidencji osób upoważnionych do przetwarzania danych osobowych oraz ewidencji wszystkich zbiorów danych osobowych; [6] rejestracji użytkowników w systemach informatycznych; [7] opracowania i wdrożenia programu szkolenia w zakresie zabezpieczenia systemu informatycznego.

W myśl przepisu art. 36b ustawy o ochronie danych osobowych, w przypadku niewyznaczenia ABI, zadania określone w art. 36a ust 2 pkt 1 tej ustawy, z wyłączeniem obowiązku sporządzania sprawozdania, realizuje ADO. Pomimo to wywiązano się jedynie z dokonania sprawdzeń zgodności przetwarzania danych osobowych z przepisami o ich ochronie oraz zapoznania osób upoważnionych do przetwarzania danych osobowych z przepisami o ich ochronie. Nie realizowano natomiast pozostałych zadań, określonych w art. 36a ust 2 pkt 1 ustawy o ochronie danych osobowych, co szerzej opisano w dalszej części wystąpienia pokontrolnego, w sekcji „Ustalone nieprawidłowości".

(dowód: akta kontroli str. 6-38, 107-110, 119-120)

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 – 2 ww. ustawy, tj.: imię i nazwisko osoby upoważnionej, datę nadania i ustania upoważnienia. W ewidencji nie zawarto natomiast zakresu upoważnienia oraz identyfikatora, co szerzej opisano w dalszej części wystąpienia pokontrolnego, w sekcji „Ustalone nieprawidłowości".

Analiza zakresów obowiązków wszystkich 19 pracowników merytorycznych Urzędu i wydanych upoważnień Burmistrza do przetwarzania danych osobowych wykazała, że:

- 14 było upoważnionych do przetwarzania danych we wszystkich zbiorach, do których mieli dostęp,
- dwóch zostało upoważnionych do przetwarzania danych, bez wskazania zbioru danych (tj. zakresu upoważnienia),
- trzech przetwarzało dane osobowe w zbiorach danych bez stosownego upoważnienia Burmistrza, co szerzej opisano w dalszej części wystąpienia pokontrolnego, w sekcji „Ustalone nieprawidłowości". (dowód: akta kontroli str. 113-116, 200-214)

2.5. W Urzędzie do 11 grudnia 2017 r. nie wydawano innych wewnętrznych aktów prawnych, procedur, instrukcji lub poleceń dotyczących sposobu gromadzenia i przetwarzania zasobów informacyjnych, niż dokumenty przyjęte 2 października 2007 r., tj.: Polityka bezpieczeństwa oraz Instrukcja zarządzania systemem informatycznym.
(dowód: akta kontroli str. 6-38, 107)

2.6. Obowiązki związane z administrowaniem systemami, w których gromadzono i przetwarzano dane osobowe powierzono (zakresem czynności) referentowi ds. obsługi informatycznej Urzędu[8]. Do jego zadań należało m.in.: [1] ustalanie dla poszczególnych stanowisk warunków, jakie musi spełniać program komputerowy, by usprawnił pracę tego stanowiska i ułatwił niezbędny obieg informacji, [2] nadzór nad instalacją sprzętu i programów komputerowych, [3] ustalanie sposobów zabezpieczania danych, kodowania informacji bazy danych, listy i wartości parametrów niezbędnych do uruchomienia i obsługi stanowisk, sposobu oraz częstości archiwizacji i rekonstrukcji danych, [4] okresowe przeglądy sprzętu, nośników pamięci oraz warunków pracy na stanowiskach komputerowych, [5] konserwacja sprzętu i usuwanie usterek, zgłaszanie awarii sprzętu i programów firmom zobowiązanym do dokonywania napraw w ramach umów.
(dowód: akta kontroli str. 6-38, 121-122)

2.7. Od 1 stycznia 2016 r. do 31 grudnia 2017 r. w Urzędzie nie przeprowadzano okresowych (co najmniej raz w roku) 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. 107, 129-130)

2.8. W okresie objętym kontrolą pracownicy Urzędu nie uczestniczyli w szkoleniach z zakresu bezpieczeństwa przetwarzania informacji, co szerzej opisano w dalszej części wystąpienia pokontrolnego, w sekcji „Ustalone nieprawidłowości". W wyjaśnieniu referent ds. obsługi informatycznej podał, że: *„każdy pracownik upoważniony do przetwarzania danych osobowych został indywidualnie przeszkolony, otrzymał niezbędną dokumentację oraz został pouczony w kwestii odpowiedzialności za naruszenie bezpieczeństwa tych danych. Wszyscy pracownicy podpisali również oświadczenia o zapoznaniu się z przepisami prawa dotyczącymi ochrony danych osobowych jak również Polityką bezpieczeństwa i Instrukcją zarządzania systemami informatycznymi".*
(dowód: akta kontroli str. 41, 107-110)

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. 107)

2.10. W Urzędzie, zarządzeniem Nr 45/07 Burmistrza z 2 października 2007 r., wprowadzono: *„Politykę Bezpieczeństwa systemów informatycznych służących do przetwarzania danych osobowych w Urzędzie Miejskim w Nowogrodzie"* i *„Instrukcję określającą sposób zarządzania systemem informatycznym, służącym do przetwarzania danych osobowych, ze szczególnym uwzględnieniem bezpieczeństwa informacji".* Dokumenty te nie były aktualizowane, co szerzej opisano w dalszej części wystąpienia pokontrolnego, w sekcji „Ustalone nieprawidłowości". (dowód: akta kontroli str. 6-38)

Polityka bezpieczeństwa zawierała elementy określone w § 4 rozporządzenia w sprawie dokumentacji oraz warunków technicznych, za wyjątkiem sposobu przepływu danych[9] pomiędzy wewnętrznymi systemami Urzędu oraz zewnętrznymi, chociaż korzystano z informacji pobieranych np. za pośrednictwem aplikacji Płatnik ZUS.

---

[8] Polityka bezpieczeństwa nie przewidywała powierzenia zadań administratorowi systemów informatycznych.

[9] Przepływ danych jest to sposób współpracy pomiędzy różnymi systemami informatycznymi oraz relacje, jakie istnieją pomiędzy danymi zgromadzonymi w zbiorach, do przetwarzania których systemy te są wykorzystywane. Sposób przepływu wskazuje na zakres przesyłanych danych, podmiotu lub kategorii podmiotów, do których są one przekazywane oraz ogólnych informacji na temat sposobów ich przesyłania (Internet, poczta elektroniczna, inne rozwiązania).

Ponadto nie zaktualizowano: *Wykazu budynków, pomieszczeń lub części pomieszczeń, tworzących obszar, w którym przetwarzane są dane osobowe*, *Wykazu zbiorów danych osobowych* oraz *Opisu struktury zbiorów danych* (stanowiących odpowiednio załączniki Nr 4, 5 i 6 do Polityki bezpieczeństwa), co szerzej opisano w dalszej części wystąpienia pokontrolnego, w sekcji „Ustalone nieprawidłowości".

Instrukcja zarządzania spełniała wszystkie wymogi § 5 rozporządzenia w sprawie dokumentacji oraz warunków technicznych. Zawierała bowiem m.in.: [1] procedury nadawania uprawnień do przetwarzania danych i rejestrowania tych uprawnień w systemach informatycznych oraz wskazanie osoby odpowiedzialnej (ABI) 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 wirusów komputerowych, nieuprawnionym dostępem oraz awariami zasilania, [7] procedury wykonywania przeglądów i konserwacji systemów oraz nośników informacji służących do przetwarzania danych. (dowód: akta kontroli str. 6-38, 123-128)

W Urzędzie poza ww. dokumentami nie wydawano innych regulacji, procedur, instrukcji dotyczących gromadzenia i przetwarzania zasobów informatycznych oraz danych osobowych. (dowód: akta kontroli str. 107)

Ustalone nieprawidłowości

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

1. Do dnia kontroli nie zgłoszono GIODO do rejestracji pięciu[10] z 18 zbiorów danych prowadzonych w Urzędzie, co naruszało wymogi art. 40 ustawy o ochronie danych osobowych. Burmistrz wyjaśnił, że: *„powodem niezgłoszenia były problemy w identyfikacji zakresów przetwarzanych zbiorów danych i ich określeniem"*.

   W trakcie kontroli (12 grudnia 2017 r.) zgłoszono GIODO do rejestracji pięć zbiorów danych. (dowód: akta kontroli str. 94-96, 111-112, 173-194)

2. ADO 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. Burmistrz wyjaśnił, iż: *„był przekonany, że prowadzony w Urzędzie wykaz (jako załącznik do Polityki bezpieczeństwa) spełnia ustawowe wymogi dotyczące rejestru zbioru danych. Natomiast w Urzędzie zastosowano środki techniczne i organizacyjne, aby chronić dane osobowe przed ich udostępnieniem osobom nieupoważnionym, zabraniem przez osoby nieuprawnione, przetwarzaniem z naruszeniem ustawy, uszkodzeniem, utratą lub zniszczeniem"*.

   Ponadto ADO nie opracował i nie wdrożył programu szkolenia w zakresie zabezpieczenia systemu informatycznego, wymaganego w rozdziale I pkt 3 tiret 7 Polityki bezpieczeństwa. W wyjaśnieniu Burmistrz podał, że: *„opracowanie programu szkolenia w zakresie zabezpieczenia systemu informatycznego wynika z indywidualności systemów przetwarzania danych (każdy odrębny system ma indywidualną strukturę z zakresu obsługiwanych danych osobowych) i nie może być uogólnione. Każdy pracownik został przeszkolony pod kątem bezpieczeństwa korzystania i obsługi systemu (oprogramowania), przez podmiot realizujący uruchomienie tego systemu (oprogramowania). Ze strony Urzędu natomiast przeprowadziłem indywidualne (na stanowisku pracy) szkolenie z zakresu ochrony danych osobowych"*. (dowód: akta kontroli str. 107, 119-120, 215-217)

[10] Prowadzonych w Urzędzie: od 1999 roku „Rejestru skarg i wniosków", od 2004 roku „Zbioru spraw dotyczących wycinki drzew i krzewów", od 2005 roku zbioru pn. „Stypendia", od 2008 roku zbioru dotyczącego „ilości i miejsc występowania odpadów zawierających azbest" oraz od 2016 roku „Elektronicznego Zarządzania Dokumentami".

3. W ewidencji osób upoważnionych do przetwarzania danych osobowych, wbrew wymogom określonym w art. 39 ust. 1 pkt 2 i 3 ustawy o ochronie danych osobowych, nie wskazano zakresu upoważnienia oraz identyfikatora w systemie informatycznym. Burmistrz wyjaśnił, że: *„głównym tego powodem było nieaktualizowanie Polityki bezpieczeństwa, bowiem w pierwszych udzielonych upoważnieniach do przetwarzania danych osobowych nie zawsze wskazywano ich zakres. Dlatego w ewidencji ujmowano, iż upoważnienie wydano w pełnym zakresie. Natomiast w ewidencji nie ujmowano identyfikatora, gdyż w przypadku ewentualnej zmiany zakresu obowiązków lub innych okoliczności identyfikator użytkownika może ulec zmianie lub zdezaktywowaniu. Ponadto w naszej jednostce każdy pracownik ma przydzielony indywidualny zestaw komputerowy, którego nie użytkuje inny pracownik. Systemy logują odpowiednie operacje użytkownika przypisanego w rejestrach do imienia i nazwiska*". (dowód: akta kontroli str. 126-128, 215-217)

4. Trzech (z 19) pracowników merytorycznych Urzędu przetwarzało dane w zbiorach danych osobowych bez upoważnienia Burmistrza, tj.: [1] skarbnik gminy przetwarzała od 16 sierpnia 2016 r. dane osobowe w systemie QNT (Quorum moduł: F-K, Płace, środki trwałe; Program QJPK; Program Qdeklaracje) oraz od 27 lipca 2016 r. w Internet Banking, [2] podinspektor ds. obsługi rady[11] przetwarzała od 1 stycznia 2017 r. dane osobowe w systemie FISKUS (gospodarka odpadami, księgowość), [3] podinspektor ds. organizacyjnych przetwarzała od 21 września 2017 r. dane osobowe w SmartDoc.

   Stanowiło to naruszenie przepisu art. 37 ustawy o ochronie danych osobowych, w myśl którego do przetwarzania danych mogą być dopuszczone wyłącznie osoby posiadające upoważnienie nadane przez administratora danych. Burmistrz wyjaśnił, że: *„wszyscy pracownicy Urzędu podpisali oświadczenia, iż zapoznali się z przepisami dotyczącymi ochrony danych osobowych, Polityki bezpieczeństwa systemów informatycznych i instrukcji przetwarzania danych osobowych oraz że dane osobowe będą przetwarzane przez pracownika zgodnie z prawem. Natomiast brak tych pięciu upoważnień wynikał z niedopatrzenia*". W trakcie kontroli (24 listopada 2017 r.) trzem pracownikom wydano brakujące upoważnienia. (dowód: akta kontroli str. 113-116, 129-130, 200-214)

5. 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: *„nie przeprowadzono audytów wewnętrznych w zakresie bezpieczeństwa informacji, ponieważ nie ma w Urzędzie pracowników posiadających odpowiednie doświadczenie i niezbędną wiedzę do przeprowadzenia takiego audytu. Natomiast wykonanie profesjonalnych audytów przez rzetelną firmę z odpowiednimi uprawnieniami wiąże się ze sporym wydatkiem finansowym dla naszej Gminy, sięgającym nawet kilku tysięcy złotych za wykonanie pojedynczego audytu. Dopiero taki audyt byłby rzetelny i wiarygodny. Na razie budżet nie pozwala na wydatkowanie aż takich środków kosztem zmniejszenia wydatków na zapewnienie bezpieczeństwa systemu ochrony danych. Staramy się we własnym zakresie, w miarę istniejących możliwości wykonać niezbędne cele i zadania, związane z systemem bezpieczeństwa informacji, przy czynnej współpracy wewnętrznej kierownictwa i pracowników Urzędu. Ponadto trwają rozmowy z kierownictwem innych jednostek w celu nawiązania współpracy, aby znacząco zredukować koszty wykonania tych audytów*". (dowód: akta kontroli str. 107, 129-130)

6. W latach 2016 – 2017 (do 20 listopada) pracownicy Urzędu nie uczestniczyli w szkoleniach dotyczących zagadnień związanych z ochroną danych osobowych oraz bezpieczeństwem informacji. 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.

---

[11] Zgodnie z aneksem Nr 1 do zakresu czynności, osoba ta w czasie nieobecności pracownika zatrudnionego na stanowisku ds. gospodarki odpadami komunalnymi dodatkowo prowadzi system odbierania odpadów komunalnych na terenie Gminy, aktualizuje bazę danych rejestru gminnego wszystkich właścicieli nieruchomości objętych systemem gospodarki odpadami komunalnymi, prowadzi ewidencję opłat przy pomocy oprogramowania komputerowego, współpracuje z Referatem Finansowym w zakresie egzekucji opłat.

W wyjaśnieniu Burmistrz podał, że: *„pracownicy nie byli szkoleni w ww. zakresie, gdyż Urząd posiadał ograniczone środki na ten cel. Należy wskazać, iż 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. 107, 111-112)

7. Od przyjęcia w 2007 roku do 11 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* (załącznik Nr 4 do Polityki bezpieczeństwa), który zawierał siedem z dziewięciu pomieszczeń, w których te dane przetwarzano lub archiwizowano; nie ujęto też systemu alarmowego jako rodzaju zastosowanego zabezpieczenia,
   - *Wykaz zbiorów w których przetwarzane są dane osobowe* (załącznik Nr 5 do Polityki bezpieczeństwa), który zawierał 12 z 18 prowadzonych przez Urząd zbiorów danych,
   - *Opis struktury zbiorów danych* (załącznik Nr 6 do Polityki bezpieczeństwa), który zawierał osiem z 18 prowadzonych przez Urząd zbiorów danych.

   Było to sprzeczne z przepisem § 20 ust. 2 pkt 1 rozporządzenia KRI, zgodnie z którym zapewnia się aktualizację regulacji wewnętrznych w zakresie zmieniającego się otoczenia. Burmistrz wyjaśnił, że pełni tę funkcję dopiero od września 2017 roku. *„Byłem przekonany, że wykazy te są aktualizowane na bieżąco przez referenta ds. obsługi informatycznej Urzędu, który został przez poprzedniego Burmistrza wyznaczony w 2013 r. na ABI. Nie miałem świadomości, że w związku ze zmianą przepisów o ochronie danych osobowych w 2015 r. należało ponownie powołać ABI oraz zgłosić do rejestracji GIODO fakt jego powołania. Tak więc nie wiedziałem, że realizacja tych zadań należy do mnie"*. Natomiast referent ds. obsługi informatycznej Urzędu wyjaśnił, że: *„brak aktualizacji wykazów wynikał z obciążenia pracą i obowiązkami. W Urzędzie pełnię funkcję informatyka i administratora systemów i sieci teleinformatycznej. Wszystkie obowiązki są realizowane niezwłocznie, z zachowaniem odpowiednich priorytetów zadań, a opóźnienia wynikają z obszernego zakresu zadań bieżących"*.

   Ponadto Polityka bezpieczeństwa, mimo wymogu określonego w § 4 pkt 4 rozporządzenia w sprawie dokumentacji oraz warunków technicznych, nie zawierała sposobu przepływu danych pomiędzy poszczególnymi systemami. Tak więc regulacje składające się na politykę bezpieczeństwa informacji, określoną w § 2 pkt 15 rozporządzenia KRI, nie odpowiadały wymogom § 20 ust. 1 ww. rozporządzenia.

   Burmistrz wyjaśnił, że: *„obecnie trwają przygotowania do aktualizacji bieżącej polityki bezpieczeństwa i zapewnienia zgodności z nowymi wytycznymi RODO. W 2016 r. weszły w życie, a od maja 2018 r. zaczną obowiązywać przepisy europejskiego rozporządzenia o ochronie danych osobowych. Aktualnie planowane są środki finansowe na rozwiązania techniczne i merytoryczne służące poprawie bezpieczeństwa wewnętrznej sieci teleinformatycznej oraz poszerzenie kompetencji i wiedzy pracowników"*. (dowód: akta kontroli str. 119-120, 123-130, 195-196, 215-217)

Ocena cząstkowa

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

3. Sposób przechowywania oraz zabezpieczenia danych

Opis stanu faktycznego

3.1. W Instrukcji zarządzania określono środki zabezpieczające służące poufności i integralności przetwarzanych danych. Przyjęte rozwiązania określały fizyczne, organizacyjne i techniczne środki zabezpieczeń, wskazując m.in., że: [1] dostęp do danych osobowych mogą mieć wyłącznie pracownicy posiadający upoważnienia podpisane przez ADO; [2] każdy z pracowników powinien zachować szczególną ostrożność przy przetwarzaniu, przenoszeniu danych osobowych; [3] należy chronić dane przed dostępem do nich osób nieupoważnionych; [4] pomieszczenia, w których są przetwarzane dane osobowe muszą być zamykane na klucz; [5] dostęp do kluczy powinni posiadać tylko

upoważnieni pracownicy; [6] dostęp do pomieszczeń możliwy jest wyłącznie w godzinach pracy Urzędu, a w przypadku, gdy jest wymagany poza godzinami pracy – możliwy jest za zgodą ADO; [7] dostęp do pomieszczeń, w których przetwarzane są dane osobowe mogą mieć tylko upoważnieni pracownicy; [8] w przypadku pomieszczeń, do których dostęp mają również osoby nieupoważnione, mogą przebywać w tych pomieszczeniach tylko w obecności osób upoważnionych i tylko w czasie wymaganym na wykonanie niezbędnych czynności; [9] szafy, w których przechowywane są dane osobowe muszą być zamykane na klucz (klucze mogą posiadać upoważnieni pracownicy); [10] dane osobowe w formie papierowej mogą znajdować się na biurkach tylko na czas niezbędny do dokonania czynności służbowych, a następnie muszą być chowane do szaf; [11] stacje komputerowe, na których przetwarzane są dane osobowe powinny mieć ustawione monitory w sposób uniemożliwiający wgląd osobom nieupoważnionym. (dowód: akta kontroli str. 6-38)

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; [6] klucze do wejścia głównego Urzędu były w posiadaniu Burmistrza oraz wyznaczonego pracownika [7] papierowa część wszystkich dziewięciu zbiorów danych osobowych przechowywana była w szafach zamykanych na klucz; [8] jeden pokój, w którym przetwarzane były dane osobowe, znajdował się na parterze budynku i posiadał wzmocnione blachą drzwi, kraty w oknach i system alarmowy (z czujnikiem w pomieszczeniu). Pozostałe pomieszczenia znajdowały się na pierwszym piętrze budynku, a okna nie posiadały zabezpieczeń antywłamaniowych i krat metalowych. Pomieszczenie archiwum znajdowało się w podpiwniczeniu budynku Urzędu i nie posiadało systemu przeciwpożarowego oraz zabezpieczania przed zalaniem, a akta składowano na drewnianych półkach, co szerzej opisano w dalszej części wystąpienia, w sekcji „Ustalone nieprawidłowości". (dowód: akta kontroli str. 131-133)

3.2. Urząd posiadał bieżące informacje z zakresu inwentaryzacji sprzętu i oprogramowania służącego do przetwarzania informacji, obejmującej ich rodzaj i konfigurację. Dane te ujmowane były w Księgach inwentarzowych środków trwałych i pozostałych środków trwałych, które obejmowały określenie lokalizacji sprzętu / oprogramowania, przynależność, rodzaj – bieżącą konfigurację, datę przyjęcia na stan, oznaczenie fabryczne i ewidencyjne oraz wartość. Znajdowały się w nich dane o wszystkich urządzeniach w Urzędzie. Było to zgodne z § 20 ust. 2 pkt 2 rozporządzenia KRI.

(dowód: akta kontroli str. 131-132)

3.3. W latach 2016 – 2017 (do 31 grudnia) w Urzędzie nie likwidowano sprzętu komputerowego, będącego nośnikiem danych oraz nie wystąpiły przypadki, w których sprzęt komputerowy naprawiany był przez podmioty zewnętrzne. Referent ds. obsługi informatycznej Urzędu wyjaśnił, że: *„w przypadku zaistnienia takich sytuacji przekazujemy sprzęt z zdemontowanymi nośnikami danych. Jeżeli nie jesteśmy w stanie samodzielnie wykonać naprawy nośnika danych, wymieniamy go na nowy, a niesprawny przechowujemy bezpiecznie do momentu specjalistycznego zniszczenia i utylizacji. Jeżeli przekazujemy / odsprzedajemy sprawny sprzęt komputerowy pozbawiamy go nośników danych, przechowując je bezpiecznie do momentu specjalistycznego zniszczenia i utylizacji*". (dowód: akta kontroli str. 91-93)

3.4. Niszczenie dokumentów w Urzędzie, zgodnie z pkt 5 c Instrukcji zarządzania systemem informatycznym, odbywało się za pomocą niszczarek. Do tego celu Urząd wyposażono w pięć niszczarek. (dowód: akta kontroli str. 91-93)

3.5. W Instrukcji zarządzania systemem informatycznym określono zasady dotyczące użytkowania komputerów przenośnych. Przyjęto w nich, że: [1] w przypadku przetwarzania danych na komputerach przenośnych (notebook) należy zachować szczególną ostrożność przy ich przewożeniu; [2] po zakończeniu pracy komputery takie powinny być zabezpieczone w zamykanych na klucz szafach; [3] niezabezpieczonych danych nie należy przesyłać drogą elektroniczną.

W okresie objętym kontrolą na terenie Urzędu wykorzystywano dwa komputery przenośne, z których jeden służył do obsługi aplikacji ŹRÓDŁO (wykorzystywany przez Sekretarza do nadawania ról użytkownikom), drugi zaś wykorzystywano jako „maszynę do pisania". Burmistrz wyjaśnił, że: *„nie korzystano ze służbowych komputerów przenośnych poza siedzibą jednostki"*. (dowód: akta kontroli str. 6-38, 111-112, 131-132)

3.6. Sprzątanie pomieszczeń Urzędu, w których przetwarzano dane osobowe odbywało się w godzinach pracy, w obecności pracowników upoważnionych do przetwarzania danych. W Urzędzie nie wprowadzono regulacji wewnętrznych w tym zakresie.

Sprzątaniem pomieszczenia serwerowni zajmował się referent ds. obsługi informatycznej Urzędu, a dostęp do tego pomieszczenia miały jeszcze dwie osoby: Burmistrz i Sekretarz. (dowód: akta kontroli str. 91-93)

3.7. Procedury dotyczące przeglądów i konserwacji systemów oraz nośników informacji służących do przetwarzania danych osobowych zostały określone w pkt 8 Instrukcji zarządzania systemem informatycznym. Ustalono w nich, że przeglądu i konserwacji dokonuje się przynajmniej dwa razy w roku, poprzez: badanie spójności bazy danych, uruchamianie zapytań do bazy danych w celu analizy danych, przegląd wydruków po wyznaczonych procesach, sprawdzanie zgodności danych z dokumentami, analiza zgłaszanych uwag użytkowników. Fakt oraz wymagana częstotliwość przeprowadzenia takich przeglądów i konserwacji nie została udokumentowana przez referenta ds. obsługi informatycznej Urzędu. W wyjaśnieniu podał on, że: *„przeprowadza regularne przeglądy i konserwacje na każdym ze stanowisk pracy. Rejestruje się ewentualne incydenty i problemy krytyczne, które do chwili obecnej nie miały miejsca. Jeżeli wszystko funkcjonuje prawidłowo i poziom bezpieczeństwa jest odpowiednio zachowany nie dokumentujemy takich czynności"*. (dowód: akta kontroli str. 6-38, 108-110)

3.8. Urząd nie posiadał wewnętrznych regulacji dotyczących rozwiązań na wypadek wystąpienia sytuacji nadzwyczajnych, np. długotrwałego braku zasilania, co szerzej opisano w dalszej części wystąpienia, w sekcji „Uwagi dotyczące badanej działalności". W instrukcji zarządzania systemem informatycznym określono natomiast zabezpieczenia przed utratą danych. Dotyczy to głównie: [1] stosowania zasilaczy UPS, które powinny zapewnić automatyczne zakończenie pracy i wyłączenie serwerów przy zaniku lub nadmiernym wahaniu napięcia – minimalny czas podtrzymania pracy wynosi pięć minut; [2] ochrony przed utratą zgromadzonych danych przez robienie kopii zapasowych na dodatkowych partycjach dysku, z których w przypadku awarii odtwarzane są dane i system operacyjny. Burmistrz wyjaśnił, że: *„Urząd jest przygotowany na wypadek wystąpienia sytuacji nadzwyczajnych, np. awarii, długotrwałego braku zasilania przez zastosowanie agregatów prądotwórczych dających możliwość zachowania ciągłości pracy w ww. sytuacjach. Jednostki przechowujące, i / lub przetwarzające dane osobowe wyposażone są w UPS-y, które zabezpieczają je przed skokami napięcia lub jego krótkotrwałym zanikiem. W przypadku utraty zasilania lub awarii praca pozostaje zapisana w systemach dzięki wykorzystanej funkcji autozapisu"*. (dowód: akta kontroli str. 6-38, 215-217)

3.9. Jak wyjaśnił referent ds. obsługi informatycznej Urzędu w okresie objętym kontrolą nie wystąpiły przypadki fizycznej utraty danych. (dowód: akta kontroli str. 91-93, 107)

Ustalone nieprawidłowości

W działalności kontrolowanej jednostki w przedstawionym wyżej zakresie stwierdzono nieprawidłowość, polegającą na niewyposażeniu pomieszczenia archiwum w system przeciwpożarowy, niezabezpieczeniu go przed zalaniem oraz składowaniu akt na drewnianych półkach. Przyjęcie takich rozwiązań nie zapewnia właściwej ochrony zbiorów danych przed działaniem czynników fizycznych i zdarzeń losowych (pożar, zalanie) i stanowi naruszenie wymogów § 6 i § 8 ust. 1 pkt 1 załącznika nr 6 do rozporządzenia

w sprawie działania archiwów zakładowych[12]. W wyjaśnieniu Burmistrz podał, że: *„w najbliższych latach planowana jest przeprowadzka do nowej siedziby przy ul. Rynek 20, która będzie wyposażona w system przeciwpożarowy. W nowym budynku archiwum planowane jest na pierwszym piętrze. W związku z tym odpadnie ryzyko i pożaru, i zalania. Obecnie akta przechowywane są w zamkniętym pomieszczeniu, na wyposażeniu którego znajduje się gaśnica proszkowa (6 kg). Druga gaśnica proszkowa znajduje się przy drzwiach prowadzących do archiwum"*. (dowód: akta kontroli str. 111-112, 131-132)

Uwagi dotyczące badanej działalności

Najwyższa Izba Kontroli zwraca uwagę na potrzebę opracowania w Urzędzie, 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.

Ocena cząstkowa

Najwyższa Izba Kontroli ocenia pozytywnie przestrzeganie przyjętych procedur w zakresie przechowywania i zabezpieczania danych w Urzędzie, które zapewniały ich właściwą ochronę. Stwierdzona nieprawidłowość nie miała wpływu na tę ocenę.

4. Przetwarzanie zasobów informacyjnych zgodnych z zakresem działalności jednostki kontrolowanej

Opis stanu faktycznego

4.1. Dane w Urzędzie przetwarzane były w 18 zbiorach danych, z których dziewięć prowadzono wyłącznie w wersji elektronicznej, osiem w wersji papierowej, zaś jeden w wersji elektronicznej i papierowej. Do GIODO zgłoszono 13 zbiorów danych, w tym siedem prowadzonych w wersji elektronicznej i sześć w wersji papierowej. Nie zgłoszono do zarejestrowania pięciu zbiorów danych prowadzonych w Urzędzie (dwóch prowadzonych wyłącznie w wersji elektronicznej, dwóch w wersji papierowej oraz jednego w wersji elektronicznej i papierowej), co szczegółowo omówiono w pkt 2.1 niniejszego wystąpienia.

Wykaz zbiorów danych osobowych (stanowiący załącznik Nr 5 do Polityki bezpieczeństwa) zawierał jedynie 12 (wszystkie zgłoszone do GIODO) zbiorów danych, co szczegółowo omówiono w pkt 2.10 wystąpienia. (dowód: akta kontroli str. 94-96, 195-196)

4.2. W okresie objętym kontrolą Urząd nie aktualizował (nie zachodziła taka konieczność) danych w rejestrze prowadzonym przez GIODO w odniesieniu do zbiorów, które były zarejestrowane. (dowód: akta kontroli str. 94-96)

4.3. We wszystkich 13 zbiorach zgłoszonych do GIODO i prowadzonych przez Urząd zakres przetwarzanych danych był zgodny ze zgłoszeniem.

Analiza wszystkich 18 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. 94-96)

4.4. Burmistrz był ADO zbiorów danych (do których dostęp posiadali pracownicy Urzędu), z wyjątkiem SRP ŹRÓDŁO, serwis CEIDG, serwis EMUiA[13], w rozumieniu art. 7 pkt 4 ustawy o ochronie danych osobowych. Urząd uzyskał dostęp do zbioru danych SRP ŹRÓDŁO z dniem 1 marca 2015 r., na podstawie upoważnienia Ministra Spraw Wewnętrznych z 7 listopada 2014 r. Urząd spełnił wymogi dostępu do tego zbioru danych, tj. m.in. uniemożliwił dostęp do „otwartego" Internetu, na stanowiskach komputerowych, z których obsługiwano ten system, pracownicy otrzymali upoważnienia do przetwarzania danych osobowych w tym systemie (informacja o upoważnieniu pracowników została

[12] 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.).

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

przekazana do Ministerstwa). Dostęp do serwisu CEIDG Urząd uzyskał natomiast na podstawie zgłoszenia z 4 października 2011 r. oraz zapewnił certyfikowany podpis elektroniczny dwóm pracownikom obsługującym ten serwis. Możliwość przetwarzania danych w serwisie EMUiA została udostępniona na podstawie porozumienia zawartego 23 kwietnia 2012 r. z Głównym Geodetą Kraju. Urząd wywiązał się z obowiązków zapewnienia odpowiedniej infrastruktury technicznej niezbędnej do użytkowania aplikacji oraz wskazania jej administratora i użytkowników. (dowód: akta kontroli str. 135-149)

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.

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[14], 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. Wskazanie w ewidencji osób upoważnionych do przetwarzania danych osobowych elementów określonych w art. 39 ust. 1 pkt 2 i 3 ustawy o ochronie danych osobowych.
4. Upoważnianie pracowników do przetwarzania danych osobowych we wszystkich zbiorach, w których dane są przez nich przetwarzane i w zakresie niezbędnym do realizowanych zadań.
5. Zapewnienie szkoleń osobom zaangażowanym w proces przetwarzania informacji, z uwzględnieniem zagrożenia jej bezpieczeństwa, skutków naruszenia zasad bezpieczeństwa, konsekwencji prawnych i środków zapewniających jej bezpieczeństwo, stosownie do postanowień § 20 ust. 2 pkt 6 rozporządzenia KRI.
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 papierowej wersji posiadanych zbiorów danych właściwej ochrony przed działaniem czynników fizycznych i zdarzeń losowych (pożar, zalanie).

V. Pozostałe informacje i pouczenia

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

Prawo zgłoszenia zastrzeżeń

Zgodnie z art. 54 ustawy o NIK, kierownikowi jednostki kontrolowanej przysługuje prawo zgłoszenia na piśmie umotywowanych zastrzeżeń do wystąpienia pokontrolnego, w terminie 21 dni od dnia jego przekazania. Zastrzeżenia zgłasza się do dyrektora Delegatury NIK w Białymstoku.

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

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 22 stycznia 2018 r.

Kontroler
Tomasz Pomian
główny specjalista kontroli państwowej

.....
podpis

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

.....
podpis