NAJWYŻSZA IZBA KONTROLI
Delegatura w Białymstoku

LBI.410.023.14.2017
P/17/062

00361618

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	Adrian Gosk – specjalista kontroli państwowej, upoważnienie do kontroli nr LBI/167/2017 z 28 listopada 2017 r. (dowód: akta kontroli str. 1-2)
Jednostka kontrolowana	Urząd Gminy w Klukowie, ul. Mazowiecka 14, 18-214 Klukowo[1]
Kierownik jednostki kontrolowanej	Piotr Uszyński – Wójt Gminy[2] (dowód: akta kontroli str. 3)

II. Ocena kontrolowanej działalności[3]

Ocena ogólna

Najwyższa Izba Kontroli ocenia negatywnie zapewnienie przez Urząd właściwej ochrony elektronicznych zasobów informacyjnych przed nieuprawnionym dostępem, przejęciem lub zniszczeniem[4].

Uzasadnienie oceny ogólnej

Stwierdzono bowiem nieprawidłowości, polegające w szczególności na:

- nadaniu wszystkim użytkownikom komputerów uprawnień administratora systemu operacyjnego tych urządzeń, wbrew przepisom § 20 ust. 2 pkt 4 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],
- nierzetelnym prowadzeniu ewidencji osób upoważnionych do przetwarzania danych osobowych, wymaganej art. 39 ustawy z dnia 29 sierpnia 1997 r. o ochronie danych osobowych[6] oraz odebraniu z ponad 10-miesięcznym opóźnieniem byłemu pracownikowi upoważnienia do przetwarzania tych danych, co było niezgodne z § 20 ust. 2 pkt 4 i 5 rozporządzenia KRI,
- niemonitorowaniu dostępu do informacji, niewykonywaniu okresowych analiz zarządzania bezpieczeństwem, a także nieprzeprowadzaniu corocznych audytów wewnętrznych z zakresu bezpieczeństwa informacji, mimo wymogów zawartych w § 20 ust. 2 pkt 3 i 7 lit a oraz pkt 14 rozporządzenia KRI,
- niezarejestrowaniu u Generalnego Inspektora Ochrony Danych Osobowych (dalej: „GIODO") trzech (z 10) zbiorów danych osobowych prowadzonych z wykorzystaniem systemów informatycznych, a także niezgłoszeniu GIODO nieposiadania w latach 2016 – 2017 pięciu takich zbiorów, czym naruszono dyspozycję art. 41 ust. 2 ustawy o ochronie danych osobowych,
- przetwarzaniu danych, które nie były niezbędne do realizacji zadań, wbrew art. 23 ust. 1 pkt 2 tej ustawy.

---

1 Dalej: „Urząd".
2 Piotr Uszyński jest Wójtem Klukowa od 27 listopada 2014 r.
3 Najwyższa Izba Kontroli stosuje 3-stopniową skalę ocen: pozytywna, pozytywna mimo stwierdzonych nieprawidłowości, negatywna.
4 Kontrolą objęto okres od 1 stycznia 2016 r. do dnia zakończenia czynności kontrolnych.
5 Dz. U. 2017 r. poz.2247. Rozporządzenie zwane dalej: „rozporządzeniem KRI".
6 Dz. U. 2016 poz. 922.

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 okresie objętym kontrolą do gromadzenia i przetwarzania danych wykorzystywano dziewięć systemów informatycznych (we wszystkich programach przetwarzano dane osobowe), które funkcjonowały na 19 komputerach (17 stacjonarnych oraz dwóch laptopach[7]). Spośród tych urządzeń, dwa nie posiadały dostępu do Internetu, a na pozostałych stworzono taką możliwość. Oględziny wszystkich 19 użytkowanych komputerów wykazały m.in., że: we wszystkich przypadkach dostęp do systemu zabezpieczony został loginem i odpowiedniej złożoności hasłem, a na dwóch komputerach logowanie następowało z wykorzystaniem indywidualnej karty z certyfikatem, a także podaniem PIN-u. Jednak na żadnym z 19 użytkowanych w Urzędzie komputerów nie wprowadzono mechanizmu obowiązkowej okresowej zmiany hasła, co szerzej opisano w dalszej części wystąpienia pokontrolnego, w sekcji „Ustalone nieprawidłowości". Wszyscy użytkownicy posiadali dostęp do niezbędnego w ich pracy oprogramowania, jednak nadane im uprawnienia nie były adekwatne do sprawowanych funkcji. Posiadali oni bowiem uprawnienia administratora systemu operacyjnego, co szerzej opisano w dalszej części wystąpienia pokontrolnego, w sekcji „Ustalone nieprawidłowości". Korzystano wyłącznie z aktualnych i dopuszczalnych aplikacji, w tym oprogramowania antywirusowego. Baza antywirusowa była aktualna na 17 komputerach, zaś na dwóch była nieaktualna, co szerzej opisano w pkt 1.10. niniejszego wystąpienia pokontrolnego. Dane nie były na bieżąco i automatycznie archiwizowane, co przedstawiono w dalszej części wystąpienia pokontrolnego, w sekcji „Ustalone nieprawidłowości". (dowód: akta kontroli str. 312-323)

1.2. W okresie objętym kontrolą w Urzędzie nie przeprowadzano okresowych analiz zarządzania bezpieczeństwem, wymaganych § 20 ust. 2 pkt 3 rozporządzenia KRI, co szerzej opisano w dalszej części wystąpienia pokontrolnego, w sekcji „Ustalone nieprawidłowości". (dowód: akta kontroli str. 303-310)

1.3. Analiza wszystkich 17 kont użytkowników korzystających z systemów informatycznych, w których przetwarzano dane wykazała, że posiadali oni indywidualne loginy i hasła do systemów operacyjnych, a także imienne upoważnienia Wójta do przetwarzania danych w poszczególnych systemach / programach, a zakres tych upoważnień odpowiadał ich zakresom czynności służbowych.

Jedynemu pracownikowi (dopuszczonemu do przetwarzania danych osobowych), z którym rozwiązano stosunek pracy w okresie objętym kontrolą, ze znacznym, ponad 10-miesięcznym opóźnieniem (dopiero po rozpoczęciu niniejszej kontroli NIK) odebrano uprawnienia dostępu do systemu informatycznego, co szerzej opisano w dalszej części wystąpienia pokontrolnego, w sekcji „Ustalone nieprawidłowości".
(dowód: akta kontroli str. 167, 171, 312-323)

1.4. Na każdej z 19 poddanych oględzinom stacji roboczych istniała możliwość weryfikacji dostępu poszczególnych użytkowników poprzez elektroniczny dziennik systemowy. Nie monitorowano jednak logów poszczególnych aplikacji, ruchu sieciowego, a także danych wychodzących z sieci lokalnej Urzędu do sieci publicznej, co szerzej opisano w dalszej części wystąpienia pokontrolnego, w sekcji „Ustalone nieprawidłowości".
(dowód: akta kontroli str. 286-292, 312-323)

1.5. Oględziny 19 komputerów wykazały też, że na każdym urządzeniu hasła dostępowe do systemu operacyjnego spełniały wymagania przewidziane dla środków bezpieczeństwa na poziomie wysokim, tj. każdorazowe uwierzytelnienie użytkownika w systemie następowało po podaniu identyfikatora oraz odpowiedniej złożoności hasła. Nie wprowadzono jednak mechanizmu obowiązkowej okresowej zmiany hasła, co szerzej opisano w pkt 1.1. niniejszego wystąpienia.

---

[7] Urząd nie posiadało służbowych tabletów i innych urządzeń mobilnych skonfigurowanych z siecią lokalną.

Zabezpieczenia na poziomie wysokim (odpowiednio złożone hasło wraz z okresową modyfikacją bądź zabezpieczenia zindywidualizowane) funkcjonowały także w siedmiu (z dziewięciu) programach służących do przetwarzania danych osobowych. W pozostałych dwóch programach (Infosystem i Fiskus) stosowano słabsze zabezpieczenia, w postaci haseł o niższej złożoności oraz bez wymuszenia ich zmiany. Informatyk Urzędu (świadczący usługi informatyczne jako podmiot zewnętrzny) wyjaśnił, iż dokumentacja bezpieczeństwa Urzędu nie przewidywała obostrzeń związanych z dwustopniowym logowaniem się. W praktyce wykorzystywano zabezpieczenia ustalone przez autorów poszczególnych programów, a użytkownicy mogli mieć identyczne hasła zarówno do systemu operacyjnego, jak i programów branżowych. Według informatyka, nikt nie zgłaszał wystąpienia problemów związanych z niedostatecznymi zabezpieczeniami dostępu do programów branżowych, a sam również nie miał w tym zakresie żadnych uwag.
(dowód: akta kontroli str. 303-323)

Urząd nie posiadał sieci bezprzewodowych. Wydzielone zostało pomieszczenie dla urządzeń serwerowych, które zabezpieczono przed nieautoryzowanym dostępem, poprzez zastosowanie odpowiednio złożonych i cyklicznie zmienianych haseł. Oględziny tego pomieszczenia wykazały jednak, że nie spełniało ono wymogów bezpieczeństwa fizycznego, co opisano szerzej w dalszej części wystąpienia pokontrolnego, w sekcji „Ustalone nieprawidłowości". (dowód: akta kontroli str. 286-292, 312-323)

W opinii powołanego w trakcie niniejszej kontroli biegłego z zakresu teleinformatyki, zabezpieczenie usług sieciowych, serwerowni, a także stacji roboczych w Urzędzie nie było zadawalające. (dowód: akta kontroli str. 286-292)

1.6. W regulacjach wewnętrznych Urzędu nie przewidziano możliwości wykorzystywania do realizacji obowiązków służbowych sprzętu prywatnego, czego powodem – jak wyjaśnił informatyk Urzędu – było wyposażenie wszystkich pracowników w odpowiednie urządzenia służbowe i korzystanie przez nich tylko z takiego sprzętu. Ponadto, jego zdaniem, nigdy nie było zgłoszeń jakichkolwiek incydentów w tym zakresie. Konfiguracja sieciowa umożliwiała jednak podłączenie do infrastruktury sprzętu (laptopy, telefony, tablety, pendrivy itp.) niestanowiącego własności Urzędu, a na pięciu komputerach zainstalowano również aplikację pulpitu zdalnego TeamViewer, z której korzystali pracownicy firmy serwisującej. Dostęp ten nie był objęty kontrolą informatyka Urzędu, co szerzej opisano w dalszej części wystąpienia pokontrolnego, w sekcji „Ustalone nieprawidłowości".
(dowód: akta kontroli str. 107-152, 286-292, 303-310, 312-323)

1.7. W okresie objętym kontrolą nie odnotowano w Urzędzie przypadków wykrycia nieautoryzowanych działań związanych z przetwarzaniem informacji, fizycznej utraty danych oraz konieczności odtwarzania zbioru danych z kopii bezpieczeństwa.
(dowód: akta kontroli str. 303-311)

1.8. W Urzędzie dopuszczono możliwość użytkowania służbowych urządzeń przenośnych (dwóch posiadanych laptopów) poza siedzibą Urzędu i na żadnym z tych urządzeń nie zastosowano szyfrowania danych. Informatyk Urzędu wyjaśnił, iż nigdy żaden z laptopów nie był wynoszony poza siedzibę. Ponadto umowa zawarta z informatykiem Urzędu dopuszczała również możliwość zdalnego łączenia się z serwerami i poszczególnymi stacjami roboczymi. Według informatyka, w praktyce nie korzystał on z tego narzędzia, natomiast kilkukrotnie udzielał niektórym użytkownikom telefonicznych wskazówek dotyczących występującego u nich problemu. Żeby takie rozwiązanie było skuteczne użytkownicy musieli mieć pozostawione uprawnienia administracyjne.
(dowód: akta kontroli str. 107-152, 204-209, 303-310)

1.9. Urząd w latach 2016 – 2017 posiadał umowy serwisowe: z firmą zajmującą się obsługą urządzenia serwerowego, na którym posadowiono dwa programy branżowe oraz z informatykiem Urzędu (od 4 stycznia 2018 r. usługi informatyczne na rzecz Urzędu świadczył inny podmiot zewnętrzny, co omówiono szerzej w pkt 2.2. niniejszego wystąpienia). W obu umowach podmioty zewnętrzne w związku z realizacją usług zobowiązały się do przestrzegania przepisów o ochronie danych osobowych. W okresie objętym kontrolą nie obowiązywały umowy z podmiotami zewnętrznymi dotyczące naprawy urządzeń komputerowych. Urząd nie korzystał z usług naprawy komputerów, gdyż –

jak wyjaśnił informatyk – obecnie użytkowany sprzęt, po kompleksowej jego wymianie w 2015 roku, jest stosunkowo nowy i nie wymagał w dwóch ostatnich latach napraw. Drobne usterki programowe eliminował osobiście.

(dowód: akta kontroli str. 204-209, 261-273, 303-310)

1.10. Wszystkie komputery Urzędu wyposażono w lokalnie instalowane oprogramowanie antywirusowe, którego aktualizacja odbywała się automatycznie. Siedemnaście zbadanych komputerów posiadało aktualne wersje aplikacji zabezpieczających, natomiast na obu komputerach do obsługi systemu zewnętrznego (Źródło) baza antywirusowa była nieaktualna. Informatyk Urzędu wyjaśnił, iż zgodnie z zapisami umowy z MSWiA (podmiot przekazujący ww. komputery), nie ingerowano w sprzęt i w otrzymane oprogramowanie oraz nie miał on wpływu na nieaktualność bazy antywirusowej na tych komputerach. W opinii powołanego w trakcie niniejszej kontroli biegłego z zakresu teleinformatyki, zastosowanie aplikacji bezpieczeństwa z centralnym modułem zarządzania rozszerzyłoby kontrolę administratora nad działaniami użytkowników. Dostęp do sieci lokalnej kontrolowany był przez firewall zainstalowany na routerze CISCO, co było zgodne z pkt III załącznika do 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[8].

(dowód: akta kontroli str. 286-292, 303-326)

1.11. Urząd wykupił w podmiocie zewnętrznym usługę hostingu strony www oraz poczty elektronicznej. Dane przechowywano na serwerze usługodawcy. Zgodnie § 20 ust. 2 pkt 10 rozporządzenia KRI i pkt. 7 regulaminu świadczenia tych usług, podmiot ten zobowiązał się do przestrzegania obowiązujących przepisów prawnych, w tym dotyczących ochrony danych osobowych. Według informatyka Urzędu ustawienia poczty elektronicznej zapewniały właściwe zabezpieczenie przed wiadomościami typu SPAM oraz przesyłaniem plików zawierających szkodliwe oprogramowanie.

(dowód: akta kontroli str. 274-281, 303-310)

1.12. W regulacjach wewnętrznych Urzędu przewidziano szereg zapisów przewidujących tworzenie kopii bezpieczeństwa danych, jednak w okresie objętym kontrolą – poza wykonywanymi w cyklu miesięcznym kopiami zapasowymi z programu Płatnik – nie wykonywano innych kopii bezpieczeństwa, co szerzej opisano w dalszej części wystąpienia pokontrolnego, w sekcji „Ustalone nieprawidłowości". W latach 2016 – 2017 nie wystąpiła w Urzędzie konieczność odtwarzania zbioru danych ze sporządzonych kopii.

(dowód: akta kontroli str. 4-102, 107-152, 174-201, 286-292, 303-311)

1.13. Na każdej z 19 poddanych oględzinom stacji roboczych zainstalowane było wyłącznie dopuszczone oprogramowanie służbowe i nie było oprogramowania pozostającego bez wsparcia producentów. Jednak – według biegłego z zakresu teleinformatyki – pracownicy (wyposażeni w system autoryzacji oparty na profilach z uprawnieniami administratora) posiadali również techniczną możliwość instalowania danych do tego nieprzeznaczonych i zainfekowania komputerów złośliwym oprogramowaniem.

(dowód: akta kontroli str. 286-292, 312-323)

1.14. W Urzędzie, zgodnie z § 20 ust. 2 pkt 12 lit. a rozporządzenia KRI, zadbano o aktualizację systemów operacyjnych i aplikacji bezpieczeństwa (poza zainstalowanymi na dwóch komputerach służących do obsługi systemu Źródło), które były wykonywane zgodnie z harmonogramami ustalonymi przez ich producentów.

(dowód: akta kontroli str. 286-292, 298-300, 312-323)

1.15. Urząd nie posiadał regulacji wewnętrznych odnoszących się do dokonywania płatności drogą elektroniczną. Według informatyka Urzędu nie było też takiej potrzeby i nie wymagał tego obsługujący bank. W praktyce pięciu pracowników Urzędu, odpowiedzialnych za ustalenie parametrów przelewu elektronicznego (w tym numeru konta odbiorcy), wyposażono w urządzenia kryptograficzne ładowane do portu USB komputera.

---

[8] Dz. U. Nr 100 poz. 1024. Rozporządzenie zwane dalej: „rozporządzeniem w sprawie dokumentacji przetwarzania danych osobowych".

Zatwierdzenie zweryfikowanego przelewu następowało przez Wójta bądź w razie jego nieobecności Sekretarza Urzędu (również z wykorzystaniem odpowiednich elektronicznych narzędzi identyfikacyjnych). (dowód: akta kontroli str. 259-260, 303-310)

Ustalone nieprawidłowości

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

1. Wbrew § 20 ust. 2 pkt 4 rozporządzenia KRI, wszystkim użytkownikom komputerów wykorzystywanych w Urzędzie nadano uprawnienia administratora systemu operacyjnego tych urządzeń, mimo że – zgodnie z ich zakresem obowiązków – nie realizowali oni zadań związanych z administrowaniem systemami. Według informatyka Urzędu, należy wziąć pod uwagę, iż w Urzędzie z reguły zatrudnieni byli urzędnicy z wieloletnim doświadczeniem, ale bez specjalistycznej wiedzy i umiejętności informatycznych. Dotychczas nie wystąpiły incydenty związane z bezpieczeństwem elektronicznych zasobów informacyjnych, a ewentualna awaria mogła nastąpić pod nieobecność informatyka. Dlatego po otrzymaniu obecnego sprzętu, w 2015 roku zdecydowano się nie ograniczać uprawnień i wyposażyć wszystkich użytkowników w możliwość korzystania z narzędzi administracyjnych. Informatyk zaznaczył, że nie zmienił tej opcji i uważał, że rozwiązanie to będzie optymalne. Nikt nie nadużył tych uprawnień.

   Ponadto – wbrew § 20 ust. 2 pkt 4-5 rozporządzenia KRI – do dnia rozpoczęcia kontroli NIK aktywne konto użytkownika w dwóch systemach informatycznych posiadała osoba, która przestała być pracownikiem Urzędu w lutym 2017 roku. Informatyk wyjaśnił, iż powodem było jego przeoczenie, ale fakt ten nie stanowił zagrożenia, ponieważ od momentu rozwiązania stosunku pracy nie przebywał on fizycznie w siedzibie Urzędu, a jego komputer przejął inny pracownik.
   (dowód: akta kontroli str. 139-141, 167, 171, 286-292, 303-318)

2. W Urzędzie nie zabezpieczano należycie danych przetwarzanych w systemach informatycznych, mimo wprowadzenia wysokiego poziomu bezpieczeństwa przetwarzania danych, wymaganego cz. C pkt XII załącznika do rozporządzenia w sprawie dokumentacji przetwarzania danych osobowych oraz postanowieniami § 2 Instrukcji Zarządzania Systemem Informatycznym[9]. Na żadnym z 19 użytkowanych w Urzędzie komputerów nie wprowadzono mechanizmu obowiązkowej okresowej zmiany hasła. Było to niezgodne z cz. A pkt IV powołanego załącznika do rozporządzenia, wymagającego zmiany hasła nie rzadziej niż co 30 dni oraz z § 2 Instrukcji Zarządzania przewidującym odpowiednią złożoność hasła oraz jego okresową zmianę. Według informatyka Urzędu, nie wprowadził on mechanizmu wymuszenia zmiany hasła, ponieważ użytkownicy posiadali uprawnienia administracyjne i w razie takiej potrzeby mogliby (przynajmniej niektórzy) takie wymuszenie zdjąć. Dodał, iż nie dokonywał weryfikacji przestrzegania tego obowiązku i w dużej mierze opierał się na zaufaniu. Uważa, iż brak sytuacji kryzysowych i incydentów potwierdził, że przyjęta do tej pory praktyka sprawdziła się.

   Ponadto do dnia rozpoczęcia niniejszej kontroli nie nadano hasła na elektronicznym nośniku służącym do archiwizacji danych z programu Płatnik. Z wyjaśnień informatyka wynika, że w trakcie kontroli dokonał zabezpieczenia nośnika odpowiednio złożonym hasłem. (dowód: akta kontroli str. 107-152, 286-292, 303-323)

3. W okresie objętym kontrolą w Urzędzie nie przeprowadzano okresowych analiz ryzyka utraty integralności, dostępności lub poufności informacji, ani nie podejmowano działań minimalizujących to ryzyko, wymaganych § 20 ust. 2 pkt 3 rozporządzenia KRI (od 31 maja 2012 r.). Informatyk Urzędu wyjaśnił, że on i kierownictwo doskonale orientowali się w słabościach obszaru informatyki i znali podstawowe zagrożenia (przede wszystkim niewłaściwe zabezpieczenie pomieszczenia z serwerami), stąd zdecydowano się nie przeprowadzać takich analiz do momentu uzupełnienia podstawowych braków. Powołany przepis nie określa częstotliwości ww. okresowych

[9] Wprowadzona została zarządzeniem Nr 37/2016 Wójta Gminy Klukowo z dnia 6 grudnia 2016 r. w sprawie wprowadzenia Polityki Bezpieczeństwa Informacji w Urzędzie Gminy Klukowo (ze zm.), zawierającym Politykę Bezpieczeństwa oraz Instrukcję Zarządzania Systemem Informatycznym (dalej „Instrukcja Zarządzania).

analiz, ale – zdaniem NIK – wskazuje na obowiązek podejmowania działań minimalizujących ryzyko utraty integralności, dostępności lub poufności informacji, a zabezpieczenie pomieszczenia z serwerami nastąpiło dopiero w trakcie niniejszej kontroli. (dowód: akta kontroli str. 286-292, 303-323)

4. W latach 2016 – 2017 w Urzędzie nie monitorowano dostępu do informacji, mimo takiego wymogu zawartego w § 20 ust. 2 pkt 7 lit a rozporządzenia KRI. Nie analizowano bowiem logów poszczególnych aplikacji, ruchu sieciowego, a także danych wychodzących z sieci lokalnej Urzędu do sieci publicznej, co w przypadku ewentualnych nadużyć mogło utrudnić identyfikację źródła problemu. Według informatyka Urzędu, czynności tych nie wykonywano, ponieważ nie było możliwości technicznych (brakowało odpowiednich urządzeń i oprogramowania) i finansowych (wysokość zaplanowanych wydatków nie pozwalała chociażby na zabezpieczenie pomieszczenia z serwerami).

   Informatyk Urzędu nie nadzorował też prac serwisowych realizowanych z wykorzystaniem, zainstalowanej na pięciu komputerach, aplikacji pulpitu zdalnego TeamViewer. Wyjaśnił on, że nigdy nie stwierdzono nieprawidłowości związanych z wykorzystywaniem tej aplikacji oraz że rozwiązanie to miało pozytywny wpływ na obniżenie kosztów. (dowód: akta kontroli str. 286-292, 303-323)

   W opinii powołanego w trakcie niniejszej kontroli biegłego z zakresu teleinformatyki serwisant łączący się za pośrednictwem aplikacji pulpitu zdalnego TeamViewer miał dostęp do wszystkich zasobów, do których dostęp w momencie połączenia posiadał dany użytkownik, a przy tego typu rozwiązaniu nie było pewności, kto faktycznie znajdował się po drugiej stronie połączenia (weryfikacja odbywała się wyłącznie na podstawie rozmowy telefonicznej), a po przeprowadzonych pracach i ewentualnych błędach serwisanta nie pozostawał ślad w ewidencji. (dowód: akta kontroli str. 286-292)

5. Wbrew § 20 ust. 2 pkt 9 rozporządzenia KRI, w okresie objętym kontrolą Urząd nie zapewnił fizycznego bezpieczeństwa urządzeń serwerowych. Zostały one bowiem umieszczone w pomieszczeniu dostępnym pracownikom, bez zastosowania jakichkolwiek zabezpieczeń (kontroli dostępu, szafy serwerowej, klimatyzacji itp.). Jak wyjaśnił informatyk Urzędu, brak odpowiednich zabezpieczeń tego pomieszczenia był od lat „największą bolączką". Powodem takiego stanu był niedobór środków finansowych. Pracownicy musieli posiadać swobodny dostęp do pomieszczenia z serwerem, ze względu na umieszczoną w nim kserokopiarkę, a serwer przed przypadkową ingerencją osób trzecich został zasłonięty. W trakcie niniejszej kontroli przeprowadzono modernizację przedmiotowego pomieszczenia – zainstalowano monitoring, a wszystkie urządzenia serwerowe zostały umieszczone w szafie zabezpieczającej przed ich fizycznym zniszczeniem bądź uszkodzeniem. Ponadto Wójt w trakcie przeprowadzonych oględzin oświadczył, iż: „w miarę wygospodarowania kolejnych środków budżetowych planuje dalszą modernizację tego pomieszczenia pod kątem zwiększenia poziomu bezpieczeństwa, w szczególności jego doposażenie w klimatyzację". (dowód: akta kontroli str. 286-292, 303-323, 327-331)

6. W okresie objętym kontrolą dane, poza wykonywanymi w cyklu miesięcznym kopiami zapasowymi z programu Płatnik, nie były na bieżąco i automatycznie archiwizowane – nie wykonywano kopii bezpieczeństwa (zapasowych) danych ani kopii archiwalnych. Tymczasem, zgodnie z § 2 pkt IV Instrukcji Zarządzania oraz wewnętrzną procedurą „Postępowanie w zakresie wykonywania i obsługi kopii zapasowych oraz okresowego badania nośników służących do przechowywania informacji", kopie wszystkich danych osobowych powinny być tworzone raz na tydzień, a kopie archiwalne – nie rzadziej niż raz w miesiącu. Jak wyjaśnił informatyk Urzędu, zapis większości programów ze względu na ich charakter odbywał się na bieżąco na serwerach (dotyczyło to programów: SmartDoc, Infosystem, Źródło, CEIDG, Fiskus, nowe SIO i programu bankowego), stąd uznano, że nie ma potrzeby dodatkowej rejestracji (tworzenia kopii zapasowych) tych danych. Dodał, że: „nam w zasadzie pozostała archiwizacja danych z Płatnika, jednak ze względu na zasilanie tego systemu danymi w cyklach miesięcznych nie było sensu wykonywać kopii częściej. Jeśli chodzi o programy Selwin i SIO (starszą wersję), to nikt nie zgłaszał mi potrzeby archiwizacji danych z tych

aplikacji, niemniej w latach 2016 – 2017 oba programy były już programami tylko z danymi historycznymi. Zdaniem informatyka, wymiar czasu pracy przewidziany podpisaną z nim umową, nie pozwalał na prowadzenie archiwizacji danych zgodnie z wymogami Instrukcji oraz ww. procedury.

(dowód: akta kontroli str. 149-152, 174-201, 286-292, 303-323)

W opinii powołanego w trakcie niniejszej kontroli biegłego z zakresu teleinformatyki brak kopii bezpieczeństwa poza zagrożeniem utratą danych i zaburzeniem ciągłości pracy systemu skutkuje nieutrwaleniem ewentualnych nadużyć w zakresie bezpieczeństwa informacji. (dowód: akta kontroli str. 286-292)

Ocena cząstkowa

Najwyższa Izba Kontroli ocenia negatywnie 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 latach 2016 – 2017 przetwarzano dane osobowe w 32 zbiorach danych, w tym w 10 z wykorzystaniem systemów informatycznych. Do dnia rozpoczęcia niniejszej kontroli Urząd zarejestrował w GIODO 24 zbiory danych osobowych (wszystkie zgłoszenia nastąpiły przed 1 stycznia 2016 r.), jednak pięć z nich faktycznie nie było prowadzonych w Urzędzie (nie występowano do GIODO o wykreślenie tych zbiorów), a kolejnych 12 zbiorów (w tym trzy prowadzone z wykorzystaniem systemów informatycznych) nie zgłoszono, co szerzej omówiono w dalszej części wystąpienia pokontrolnego, w sekcji „Ustalone nieprawidłowości". Ostatni ze zbiorów zgłoszono w październiku 2017 roku (zgłoszenie zawierało wszystkie elementy wymagane art. 41 ust. 1 ustawy o ochronie danych osobowych), ale do dnia zakończenia niniejszej kontroli nie został on zamieszczony w rejestrze dostępnym na stronie internetowej GIODO.

(dowód: akta kontroli str. 202, 211-216, 303-323)

2.2. Zgodnie ze zgłoszeniem do GIODO (z 19 listopada 2015 r.), w latach 2016 – 2017 funkcję administratora bezpieczeństwa informacji („ABI") sprawował informatyk Urzędu (upoważniony podmiot zewnętrzny), a w związku z wygaśnięciem (31 grudnia 2017 r.) jego umowy, 15 stycznia 2018 r. powołano jednego z pracowników na tą funkcję. W obu przypadkach Urząd dopełnił obowiązków wynikających z art. 46b ust. 1 ustawy o ochronie danych osobowych, związanych ze zgłoszeniem odwołania ABI i powołaniem nowego.

W dniu 4 stycznia 2018 r. Wójt podpisał umowę serwisu sprzętu oraz oprogramowania komputerowego z kolejnym podmiotem zewnętrznym. Wykonawca zobowiązał się w niej m.in. do wykonywania zleconych prac z zachowaniem należytej staranności oraz zgodnie z obowiązującymi przepisami (w tym o ochronie danych osobowych) i normami technicznymi, a także do zachowania w tajemnicy wszelkich pozyskanych informacji. Jak wyjaśnił Wójt, w dalszej perspektywie planowane są dalsze zmiany organizacyjne w obszarze informatyki i ochrony danych osobowych, wynikające z zapowiadanej istotnej zmiany przepisów w tym zakresie.

(dowód: akta kontroli str. 103-106, 126, 203-209, 232-235, 330-340)

2.3. ABI, stosownie do przepisu art. 36a ustawy o ochronie danych osobowych, w latach 2016 – 2017 zapewnił zapoznanie się pracowników przetwarzających dane z wymaganymi przepisami, co wykazała analiza dokumentacji wszystkich 15 pracowników Urzędu. Ponadto ABI prowadził rejestr zbiorów przetwarzanych danych, w którym nie zamieszczono jednak kompletu prowadzonych w Urzędzie zbiorów, co szerzej opisano w dalszej części wystąpienia pokontrolnego, w sekcji „Ustalone nieprawidłowości". ABI nie przeprowadzał również kontroli zgodności przetwarzania danych osobowych z przepisami o ochronie danych osobowych i nie sporządzał dla ADO wymaganych sprawozdań w tym zakresie, co szerzej opisano w dalszej części wystąpienia pokontrolnego, w sekcji „Ustalone nieprawidłowości". ABI nie zadbał też o bieżącą aktualizację dokumentacji opisującej przetwarzanie danych osobowych, co omówiono szerzej w pkt 2.10. niniejszego wystąpienia pokontrolnego. (dowód: akta kontroli str. 107-152, 293-297, 303-323)

2.4. W Urzędzie prowadzono ewidencję osób upoważnionych do przewarzania danych osobowych, obejmującą elementy określone w art. 39 ust. 1 ustawy o ochronie danych osobowych. Nie była ona jednak prowadzona rzetelnie, gdyż nie ujęto w niej jednego pracownika przetwarzającego takie dane oraz nie odnotowano identyfikatorów z systemów informatycznych 11 z 15 pracowników, co szerzej opisano w dalszej części wystąpienia pokontrolnego, w sekcji „Ustalone nieprawidłowości". Wójt posiadał aktualne upoważnienie do przetwarzania danych w Systemie Rejestrów Państwowych, wydane przez Ministra Cyfryzacji. W 2015 roku Urząd przekazał do Ministra Spraw Wewnętrznych wykaz pracowników upoważnionych do przetwarzania danych gromadzonych w ww. systemie. Zakres upoważnień pracowników Urzędu do przetwarzania danych osobowych był zgodny z realizowanymi zadaniami. (dowód: akta kontroli str. 139-141, 251-258, 303-323)

2.5. W okresie objętym kontrolą wystąpiły zmiany organizacyjne uzasadniające potrzebę aktualizacji regulacji wewnętrznych dotyczących gromadzenia i przetwarzania posiadanych zasobów informacyjnych. Nie wszystkie zmiany skutkowały zaktualizowaniem dokumentacji opisującej przetwarzanie danych osobowych, co omówiono szerzej w pkt 2.10. niniejszego wystąpienia pokontrolnego. (dowód: akta kontroli str. 107-152, 303-323)

2.6. W latach 2016 – 2017 regulacje wewnętrzne dotyczące bezpieczeństwa informacji powierzały obowiązki związane z administrowaniem systemami, w których gromadzono i przetwarzano dane osobowe, informatykowi Urzędu, który pełnił również funkcję ABI. Do jego zadań należało m.in. zabezpieczenie zbiorów danych prowadzonych w systemach informatycznych oraz przeciwdziałanie dostępowi osób niepowołanych. Informatyk posiadał stosowne upoważnienie, zobowiązał się do przestrzegania przepisów bezpieczeństwa, a także do zachowania w poufności wszelkich pozyskanych informacji. Poza obsługą za pośrednictwem środków teleinformatycznych, zobowiązany został do realizacji powierzonych zadań w wymiarze co najmniej dwóch wizyt miesięcznie, a usuwanie awarii systemu (uniemożliwiającej pracę) powinno rozpocząć się w ciągu 24 godzin od zgłoszenia. Wójt Gminy zapytany o sposób sprawowania nadzoru nad informatykiem w latach 2016 – 2017 wyjaśnił, iż dysponował określonym budżetem i środki na zadania związane z obsługą informatyczną oraz ochroną danych osobowych nie pozwalały na zatrudnienie osoby w pełnym wymiarze czasu pracy. W jego ocenie, biorąc pod uwagę skalę działalności oraz stosunkowo nieskomplikowane rozwiązania informatyczne nie było również takiej potrzeby. Według Wójta, wymiar czasu pracy określony w umowach był optymalny i odpowiadał obu stronom, a informatykowi stworzono możliwość dużej elastyczności w podziale czasu pracy, gdyż w latach 2016 – 2017 obsługiwał również jednostkę podległą (GOPS). Brak jakichkolwiek wypowiedzeń (skrócenia czasu obowiązywania zawartych umów) świadczył, według Wójta, że obie strony były zadowolone ze współpracy.
(dowód: akta kontroli str. 107-152, 204-209, 330-331)

2.7. W Urzędzie w latach 2016 – 2017 nie przeprowadzano corocznych 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. 303-323)

2.8. W okresie objętym kontrolą pracownicy Urzędu uczestniczyli w szkoleniach z zakresu bezpieczeństwa przetwarzania danych / informacji: w kwietniu 2017 roku ABI przeszkolił 13 pracowników Urzędu z zakresu ochrony danych osobowych (w ramach szkolenia omówiono m.in. politykę haseł, zasady bezpiecznego użytkowania sprzętu IT, zagrożenia bezpieczeństwa informacji i ich konsekwencje, a także problematykę odpowiedzialności karnej, cywilnej i dyscyplinarnej), a Sekretarz Urzędu w listopadzie 2017 roku dodatkowo uczestniczyła w dwudniowym szkoleniu pn. „Ochrona danych osobowych w praktyce jednostek samorządu terytorialnego". ABI odnosząc się do braku innych szkoleń wyjaśnił, że 2016 rok przeznaczył przede wszystkim na opracowywanie nowej dokumentacji bezpieczeństwa, której projekt przedłożył pod koniec roku i została zatwierdzona przez Wójta, stąd nie miał możliwości prowadzenia szkoleń, zaś w 2017 roku przeszkolił tych, którzy byli obecni w dniu szkolenia w pracy. Dla dwóch pozostałych osób wstępnie zaplanował przeszkolenie w 2018 roku (osoby te były przeszkolone w 2015 roku).
(dowód: akta kontroli str. 222-224, 230-231, 303-323)

2.9. W okresie objętym kontrolą Urząd nie był kontrolowany przez podmioty zewnętrzne w zakresie bezpieczeństwa danych. W latach 2016 – 2017 nie wpływały do Urzędu skargi związane z przypadkami ujawnienia danych osobowych. (dowód: akta kontroli str. 311)

2.10. Do 6 grudnia 2016 r. w Urzędzie obowiązywała dokumentacja bezpieczeństwa zawierająca szereg nieaktualnych regulacji (w zakresie m.in. listy osób upoważnionych do przetwarzania danych, wykorzystywanego oprogramowania, wykazu przetwarzanych zbiorów danych oraz „podstawowego" poziomu bezpieczeństwa systemu informatycznego). ABI wyjaśnił, że taki stan zastał w momencie objęcia obowiązków i wiedząc o tych brakach zdecydował się na opracowanie nowej dokumentacji, uwzględniającej specyfikę Urzędu, którą wprowadzono w życie pod koniec 2016 roku – zarządzeniem Nr 37/2016 Wójta z dnia 6 grudnia 2016 r. wprowadzono Politykę Bezpieczeństwa i Instrukcję Zarządzania, które odpowiadały wymogom §§ 4 – 5 rozporządzenia w sprawie dokumentacji przetwarzania danych osobowych. Wg stanu na dzień kontroli NIK, dokumenty te zawierały m.in. nieaktualny wykaz 22 zbiorów przetwarzanych danych osobowych oraz nieaktualny zakres danych przetwarzanych w poszczególnych zbiorach, co szerzej opisano poniżej, w sekcji „Ustalone nieprawidłowości". (dowód: akta kontroli str. 4-102,107-152, 303-323)

Ustalone nieprawidłowości

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

1. W latach 2016 – 2017 Urząd nie zgłaszał GIODO zmian dotyczących pięciu zarejestrowanych (w 1999 roku) zbiorów danych osobowych („czytelnicy biblioteki publicznej", „czytelnicy biblioteki publicznej filia w Kuczynie", „czytelnicy biblioteki publicznej filia w Wyszonkach Kościelnych", „ewidencja pojazdów" oraz „ewidencja kierowców"), których w Urzędzie nie prowadzono w okresie objętym kontrolą. Pierwsze trzy znajdowały się bowiem w bibliotece, a pozostałe dwa zostały przed 1 stycznia 2016 r. przekazane do Starostwa Wysokomazowieckiego. Naruszało to art. 41 ust. 2 ustawy o ochronie danych osobowych, wymagający zgłoszenia GIODO zmiany dotyczącej zbioru w ciągu 30 dni od jej wystąpienia.

   Ponadto do dnia rozpoczęcia kontroli NIK nie zgłoszono do rejestracji trzech zabiorów danych osobowych („dziennik korespondencji", „system informacji oświatowej" i „rejestr wniosków o udzielenie informacji publicznej"), założonych w bliżej nieokreślonym czasie, przed 1 stycznia 2016 r. i prowadzonych w Urzędzie z wykorzystaniem systemów informatycznych. Naruszono w ten sposób wymogi art. 40 ustawy o ochronie danych osobowych. Odpowiedzialny za rejestrację w GIODO informatyk wyjaśnił, że nie jest w stanie określić kiedy niezgłoszone do GIODO zbiory danych osobowych zostały założone i że nie posiadał czasu, aby doprowadzić do zgodności informacje między faktycznie prowadzonymi zbiorami danych osobowych a zarejestrowanymi w GIODO.
   (dowód: akta kontroli str. 202, 303-323)

2. Prowadzony przez ABI rejestr zbiorów przetwarzanych danych nie zawierał siedmiu prowadzonych w Urzędzie zbiorów, w tym trzech prowadzonych z wykorzystaniem systemów informatycznych, co było sprzeczne z przepisem art. 36a ust. 2 pkt 2 ustawy o ochronie danych osobowych. ABI przyznał, że nieujęcie w rejestrze tych zbiorów danych spowodowane było jego błędem. (dowód: akta kontroli str. 293-297, 303-323)

3. ABI w okresie objętym kontrolą nie przeprowadzał kontroli zgodności przetwarzania danych osobowych z przepisami o ochronie danych osobowych i nie sporządzał dla Wójta wymaganych sprawozdań w tym zakresie, mimo takiego obowiązku wynikającego z art. 36a ust. 2 pkt 1 lit a ustawy o ochronie danych osobowych. ABI wyjaśnił, że powodem nieprzeprowadzania ww. czynności był zbyt mały wymiar czasu przewidziany w zawartej z nim umowie. Z kolei Wójt zapytany o sprawowanie nadzoru nad ABI wyjaśnił, że kilka lat wcześniej sam pełnił obowiązki ABI i codziennie przebywał w Urzędzie, a zatem znakomicie orientował się o niewystępowaniu kradzieży, utraty, a także dopuszczenia do danych osobowych osób niepowołanych. Jego zdaniem realizacja przez ABI kontroli (sprawdzeń) wewnętrznych oraz sporządzanie sprawozdań potwierdzających ww. stan byłaby jedynie dopełnieniem obowiązków formalnych, natomiast nie przyniosłaby Urzędowi wymiernych korzyści, stąd nie naciskał na dostarczenie ww. dokumentów. (dowód: akta kontroli str. 303-323, 330-331)

4. Były pracownik Urzędu, który do końca stycznia 2017 roku był zatrudniony i przetwarzał dane osobowe z wykorzystaniem dwóch systemów informatycznych, do dnia rozpoczęcia kontroli NIK nadal posiadał imienne upoważnienie Wójta do przetwarzania takich danych, co było niezgodne z § 20 ust. 2 pkt 5 rozporządzenia KRI. W trakcie niniejszej kontroli ABI (z upoważnienia Wójta) cofnął ww. upoważnienie i wyjaśnił, że doszło do tego z powodu niedopatrzenia. Dodał, że pracownik ten od momentu rozwiązania stosunku pracy nie miał możliwości przetwarzania tych danych, ponieważ nie było go fizycznie w Urzędzie, a jego komputer przejął inny pracownik.
(dowód: akta kontroli str. 139-141, 167,171, 303-323)

   W ewidencji osób upoważnionych do przewarzania danych osobowych nie odnotowano identyfikatorów z systemów informatycznych 11 (z 15) pracowników, co naruszało przepis art. 39 ust. 1 pkt 3 ustawy o ochronie danych osobowych. ABI wyjaśnił, że wynikało to z jego nieuwagi i przeoczenia.
(dowód: akta kontroli str. 139-141, 303-323)

5. W Urzędzie nie przeprowadzano corocznych audytów wewnętrznych z zakresu bezpieczeństwa informacji, mimo obowiązku wynikającego z § 20 ust. 2 pkt 14 rozporządzenia KRI. Informatyk wyjaśnił, że on i kierownictwo Urzędu doskonale orientowali się w słabościach obszaru informatyki i znane im były podstawowe zagrożenia (przede wszystkim niewłaściwe zabezpieczenie pomieszczenia z serwerami), stąd nie przeprowadzano takich audytów do momentu uzupełnienia ww. braków. (dowód: akta kontroli str. 303-323)

6. W okresie objętym kontrolą, mimo wymogu określonego w § 20 ust. 2 pkt 1 rozporządzenia KRI, nie dokonano zmian w Polityce Bezpieczeństwa, chociaż zawierała ona nieaktualne: [1] wykaz 22 zbiorów danych osobowych oraz służące do tego celu oprogramowania (wraz z określeniem przepływu danych między systemami); [2] zakres przetwarzania danych osobowych w 15 zbiorach danych. Odpowiedzialny za to zadanie ABI, przyczyny ww. zaniechania wyjaśnił brakiem czasu.
(dowód: akta kontroli str. 107-152, 303-323)

Ocena cząstkowa

Najwyższa Izba Kontroli ocenia negatywnie wdrożenie dokumentacji i procedur ochrony danych osobowych.

3. Sposób przechowywania oraz zabezpieczenia danych

Opis stanu faktycznego

3.1. W Urzędzie nie wprowadzono systemu kontroli dostępu, monitoringu, systemu alarmowego i systemu przeciwpożarowego. Nie stosowano również zabezpieczeń okien (krat, rolet lub folii antywłamaniowej), a w obowiązującej dokumentacji bezpieczeństwa nie były określone wprost jakiekolwiek wymagania dla pomieszczeń, w których przetwarzane były dane osobowe. ABI zobowiązany został jedynie do: „zapewnienia środków technicznych i organizacyjnych odpowiednich do zagrożeń oraz objętych ochroną danych". ABI wyjaśnił, że był to zabieg świadomy, aby nie określać wymagań, na które brakowało środków finansowych. Według Wójta, ABI zobowiązany został do zapewnienia środków technicznych i organizacyjnych odpowiednich do zagrożeń oraz objęcia ochroną danych i takie zostały zapewnione – w zakresie właściwego oprogramowania oraz jego skonfigurowania i wyposażenia (m.in. zamki w pomieszczeniach i w szafkach na dokumenty, niszczarki, gaśnice, a ostatnio także kamera w pomieszczeniu z serwerami). Z wyjaśnień Wójta wynika, że cały budynek, w którym mieści się siedziba Urzędu, poza wyznaczonymi godzinami pracy jest zamykany (dodatkowo kolejne drzwi oddzielają Urząd od innych instytucji zlokalizowanych w tym budynku), a zastosowane i wdrożone mechanizmy zabezpieczające stanowiły kompromis między stroną kosztową a potrzebami wynikającymi z doświadczeń i miejscowych realiów, skłaniających do obligatoryjnego zastosowania ww. zabezpieczeń. W Urzędzie nie opracowano tzw. „polityki kluczy". W praktyce klucze umieszczano w przeznaczonej do tego skrzynce.
(dowód: akta kontroli str. 303-326, 330-331)

3.2. Informatyk Urzędu na bieżąco gromadził dane, o których mowa w § 20 ust. 2 pkt 2 rozporządzenia KRI, tj. prowadził w formie elektronicznej ewidencję obejmującą aktualne dane dotyczące całości służbowego sprzętu informatycznego (rodzaj sprzętu wraz

z konfiguracją) i oprogramowania (systemy operacyjne, programy i aplikacje branżowe, posiadane licencje itp.). (dowód: akta kontroli str. 303-323)

3.3. W okresie objętym kontrolą Urząd pozbył się dziewięciu zbędnych komputerów (wraz ze sformatowanymi twardymi dyskami), z których co najmniej jeden przekazano do dalszego użytkowania, co szerzej opisano w dalszej części wystąpienia pokontrolnego, w sekcji „Ustalone nieprawidłowości". (dowód: akta kontroli str. 236-241, 286-292, 303-310)

3.4. Do niszczenia bieżących wydruków oraz dokumentów niewymagających archiwizacji wykorzystywano w Urzędzie pięć niszczarek (w tym jedną ogólnodostępną w sekretariacie Urzędu). Nie opracowano w tym zakresie żadnych wytycznych lub procedur. Według oświadczenia ABI, „nie było konieczności przy niszczeniu dokumentacji korzystania do tej pory z usług firm zewnętrznych ze względu na niewielką skalę".
(dowód: akta kontroli str. 312-326)

3.5. Wykorzystywanie w latach 2016 – 2017 urządzeń przenośnych w Urzędzie omówione zostało w pkt 1.8. niniejszego wystąpienia pokontrolnego.
(dowód: akta kontroli str. 107-152, 204-209, 303-310)

3.6. ABI zapoznał pracownika dopowiadającego za sprzątanie pomieszczeń z przepisami dotyczącymi ochrony danych osobowych oraz obowiązującymi w tym zakresie regulacjami wewnętrznymi, a także odebrał pisemne oświadczenie od tej osoby o zachowaniu tajemnicy zarówno w trakcie trwania stosunku pracy, jak i po ustaniu zatrudnienia. Według posiadanego zakresu czynności, osoba sprzątająca realizowała te usługi również poza godzinami pracy Urzędu (od 6.00 do 8.00 oraz od 15.00 do 21.00) i nie została w okresie objętym kontrolą objęta szkoleniem z zakresu ochrony danych osobowych (omówionym szerzej w pkt 2.8. niniejszego wystąpienia). Zdaniem ABI, nastąpiło to w wyniku przeoczenia. Dodał, że osoba ta nie przetwarzała dotąd danych osobowych, a więc ewentualne szkolenie w jej przypadku „miałoby znacznie okrojony charakter".
(dowód: akta kontroli. str. 223-229, 303-311)

3.7. W okresie objętym kontrolą Urząd nie przeprowadzał przeglądów i konserwacji oraz nie korzystał z usług firm zewnętrznych w tym zakresie, mimo że od 6 grudnia 2016 r. Wójt wprowadził wewnętrzną procedurę pn. „Przeglądy i konserwacje systemów", przewidującą m.in. przeprowadzanie przeglądu głównych usług autoryzacyjnych oraz systemu ochrony styku z siecią publiczną. Zdaniem ABI w 2017 roku nie przeprowadził ww. czynności ze względu na zbyt mały wymiar czasu przewidziany w zawartej z nim umowie.
(dowód: akta kontroli str. 189-193, 303-311)

3.8. Urząd od 6 grudnia 2016 r. posiadał procedury na wypadek wystąpienia sytuacji nadzwyczajnych, w tym zdarzeń losowych. Nie określały one jednak szczegółowych rozwiązań na wypadek długotrwałej utraty zasilania i przywracania systemów po awarii oraz planu ciągłości działania, umożliwiającego kontynuację wykonywania zadań publicznych. Serwer Urzędu wyposażono w urządzenie UPS, umożliwiające podtrzymanie pracy serwera. Oględziny 19 komputerów wykazały, że 17 z nich posiadało zasilacze awaryjne UPS bądź akumulatory podtrzymujące zasilanie. Brakowało takiego wyposażenia na dwóch komputerach stacjonarnych, co szerzej opisano w dalszej części wystąpienia, w sekcji „Uwagi dotyczące badanej działalności". (dowód: akta kontroli str. 174-199, 303-327)

3.9. W okresie objętym kontrolą nie było w Urzędzie przypadków fizycznej utraty danych i konieczności odtwarzania ich z kopii bezpieczeństwa. (dowód: akta kontroli str. 311)

Ustalone nieprawidłowości

W działalności kontrolowanej jednostki w przedstawionym wyżej zakresie stwierdzono nieprawidłowość, polegającą na niepozbawieniu przez informatyka w sposób trwały zawartości dysków twardych komputerów, które jako zbędne przekazano do dalszego użytkowania (np. Ochotniczej Straży Pożarnej w Klukowie). Dokonano jedynie sformatowania dysków twardych, co nie odpowiadało wymogom zawartym w załączniku do rozporządzenia w sprawie dokumentacji przetwarzania danych osobowych. Informatyk wyjaśnił, że na przełomie kwietnia i maja 2016 roku nastąpiło jedyne przekazanie służbowego sprzętu komputerowego i większość komputerów (osiem) po komisyjnej ocenie ich zużycia została przekazana do likwidacji, z kolei jeden przekazano do OSP w Klukowie. Z jego wyjaśnień wynikało również, iż w przypadku wszystkich komputerów, przed

przekazaniem dokonał sformatowania dysku i ponownej instalacji systemu operacyjnego. Uważał bowiem, że jest to rozwiązanie wystarczające. Zdaniem biegłego z zakresu teleinformatyki, formatowanie dysku nie powoduje fizycznego wykasowania informacji na nim zapisanych, a dane te są możliwe do otworzenia w stosunkowo nieskomplikowany sposób. Aby działanie było skuteczne, przy likwidacji sprzętu najprościej jest fizycznie uszkodzić strukturę nośnika, a w przypadku dalszego użytkowania dysku – należy zapisać cały dysk binarnymi zerami – poprzez wykorzystanie dedykowanego do tego oprogramowania. (dowód: akta kontroli str. 236-241, 286-292, 303-310)

Uwagi dotyczące badanej działalności

Najwyższa Izba Kontroli zwraca uwagę, na potrzebę uszczegółowienia w Urzędzie wewnętrznych regulacji dotyczących rozwiązań na wypadek wystąpienia sytuacji nadzwyczajnych, np. długotrwałego braku zasilania lub przywracania systemów po awarii oraz planu ciągłości działania, umożliwiającego kontynuację wykonywania zadań w sytuacjach nadzwyczajnych. Dokument ten powinien określić systemy i aplikacje o znaczeniu krytycznym oraz wszystkie podporządkowane lub powiązane plany. Istotne jest, aby były one jasno udokumentowane, przekazane pracownikom i aktualizowane w celu odzwierciedlenia bieżącej działalności jednostki. Urząd nie był też w pełni przygotowany do wykonywania zadań w sytuacji długotrwałej utraty zasilania. Nie posiadał bowiem agregatu prądotwórczego, a dwa (z 19 analizowanych) komputerów nie posiadały zasilaczy awaryjnych UPS bądź urządzeń o podobnej funkcjonalności. Informatyk wyjaśnił, że Urząd nie posiadał środków na pilniejsze potrzeby, stąd nie był również zabezpieczony na wypadek długotrwałej utraty zasilania. Zaznaczył, iż w razie wystąpienia takiej sytuacji posiadanie agregatu nie zapewniłoby ciągłości działania, ponieważ większość systemów zewnętrznych nie funkcjonowałaby na skutek braku połączenia internetowego, również ściśle uzależnionego od podtrzymywania zasilania. Dodał, że nie wie dlaczego nie było dwóch UPS-ów – jego zdaniem nigdy nie było z tym problemów i nikt nie zwrócił uwagi na ten fakt. 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 przetwarzania danych osobowych.
(dowód: akta kontroli str. 174-199, 303-326)

Ocena cząstkowa

Najwyższa Izba Kontroli ocenia negatywnie działania Urzędu dotyczące przestrzegania przyjętych procedur w zakresie przechowywania i zabezpieczania danych oraz zapewnienia ich właściwej ochrony.

4. Przetwarzanie zasobów informacyjnych zgodnych z zakresem działalności jednostki

Opis stanu faktycznego

4.1. W okresie objętym kontrolą w Urzędzie przetwarzano dane w 32 zbiorach danych, z których 10 prowadzono z wykorzystaniem systemów informatycznych, a pozostałe 22 w formie tradycyjnej (papierowej). Z kolei w wykazie zbiorów danych zawartych w Polityce Bezpieczeństwa ujęto 22 zbiory (co szerzej omówiono w pkt 2.10. niniejszego wystąpienia), a do GIODO zgłoszono 25 zbiorów, ale pięciu z nich faktycznie w tym okresie nie prowadzono (co szerzej omówiono w pkt 2.1. niniejszego wystąpienia).
(dowód: akta kontroli str. 128-138, 303-323)

4.2. W okresie objętym kontrolą Urząd nie aktualizował zakresu przetwarzanych danych w zbiorach zarejestrowanych w GIODO, z uwagi na prowadzenie przez ABI rejestru, o którym mowa w art. 36a ust. 2 pkt 2 ustawy o ochronie danych osobowych (rejestr ten nie zawierał jednak wszystkich zbiorów prowadzonych w Urzędzie, co omówiono szerzej w pkt 2.3. niniejszego wystąpienia). (dowód: akta kontroli str. 293-297, 303-323)

4.3. Analiza 10 z 32 zbiorów danych prowadzonych w Urzędzie wykazała, że w siedmiu zakres przetwarzanych danych był niezbędny do realizacji przypisanych zadań, a w trzech przetwarzano także inne dane, co szerzej opisano w dalszej części wystąpienia, w sekcji „Ustalone nieprawidłowości". (dowód: akta kontroli str. 128-138, 303-323)

W latach 2016 – 2017 Urząd w ogłoszeniach w sprawie konkursów na kierowników jednostek podległych informował kandydatów o uprawnieniach wynikających z art. 24 ust. 1 ustawy o ochronie danych osobowych (wzmiankowano m.in. o obowiązku składnia

oświadczeń o wyrażeniu zgody na przetwarzanie danych osobowych oraz o podstawie prawnej takiego żądania). (dowód: akta kontroli str. 301-302, 311)

4.4. Urząd uzyskał dostęp do zewnętrznego zbiorów danych przetwarzanych z wykorzystaniem systemów informatycznych (Źródło) na podstawie umowy zawartej z MSWiA i spełnił wymogi techniczno-organizacyjne dostępu do tego zbioru danych. (dowód: akta kontroli str. 242-250, 303-323)

Ustalone nieprawidłowości

W działalności kontrolowanej jednostki w przedstawionym wyżej zakresie stwierdzono nieprawidłowość, polegającą na gromadzeniu i przetwarzaniu w trzech (z 10 objętych analizą) zbiorach danych, które nie były niezbędne do realizacji zadań, dla których zbiory te były prowadzone. W zbiorze danych:

a) „Zbiór wniosków o nadanie numeru nieruchomości" przetwarzano m.in. imiona rodziców, PESEL, nr i serię dowodu osobistego, stan cywilny oraz płeć, mimo że z treści załącznika nr 1 do rozporządzenia Ministra Administracji i Cyfryzacji z dnia 9 stycznia 2012 r. w sprawie ewidencji miejscowości, ulic i adresów[10] nie wynikało, aby dane te były wymagane,

b) „Zbiór decyzji związany z wycinką drzew" w Urzędzie przetwarzano m.in. imiona rodziców, NIP, PESEL, nr i serię dowodu osobistego oraz stan cywilny, chociaż z treści art. 83b ustawy z dnia 16 kwietnia 2004 r. o ochronie przyrody[11] nie wynikało, aby takie dane były wymagane we wniosku o wydanie zezwolenia na usunięcie drzewa lub krzewu,

c) „Decyzje na zajęcie pasa drogowego" przetwarzano m.in.: imiona rodziców, serię i nr dowodu osobistego, PESEL, NIP i stan cywilny, mimo że z treści § 1 rozporządzenia Rady Ministrów z dnia 1 czerwca 2004 r. w sprawie określenia warunków udzielania zezwoleń na zajęcie pasa drogowego[12] nie wynikało, aby takie dane były wymagane w tym postępowaniu.

Przetwarzanie ww. danych było zatem sprzeczne z art. 23 ust. 1 pkt 2 ustawy o ochronie danych osobowych. Zgodnie z tym przepisem, przetwarzanie danych jest bowiem dopuszczalne tylko wtedy, gdy jest to niezbędne dla zrealizowania uprawnienia lub spełnienia obowiązku wynikającego z przepisu prawa. Według ABI, wszyscy urzędnicy zadeklarowali, że przetwarzają jedynie dane niezbędne w ich pracy, ale przyznał, że opierał się w tym zakresie jedynie na ich doświadczeniu i zaufaniu do nich. Nie był w stanie tego zweryfikować, biorąc pod uwagę inne powierzone obowiązki. Odnosząc się do bezpośrednich przyczyn, ABI wskazał, iż do wniosków wnioskodawcy sami załączali kopie dokumentów (np. aktów notarialnych), z treści których wynikały ww. dane. (dowód: akta kontroli str. 303-323)

Ocena cząstkowa

Najwyższa Izba Kontroli ocenia negatywnie sposób przetwarzania zasobów informacyjnych.

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[13], wnosi o:

1. Nadanie użytkownikom systemów informatycznych uprawnień adekwatnych do sprawowanych funkcji, stosownie do przepisów § 20 ust. 2 pkt 4 rozporządzenia KRI.
2. Należyte zabezpieczenie danych przetwarzanych w systemach informatycznych, a w szczególności wykonywanie kopii bezpieczeństwa, wprowadzenie mechanizmu obowiązkowej okresowej zmiany haseł użytkowników, a także trwałe usuwanie zawartości dysków przy przekazywaniu sprzętu do likwidacji bądź dalszego użytkowania.

---

[10] Dz. U. z 2012 r. poz. 125.
[11] Dz. U. z 2016 r. poz. 2134, ze zm.
[12] Dz. U. z 2016 poz. 1264.
[13] Dz. U. z 2017 r. poz. 524. Ustawa zwana dalej „ustawą o NIK".

3. Realizację obowiązków wynikających z § 20 ust. 2 rozporządzenia KRI w zakresie: aktualizacji przyjętych regulacji wewnętrznych dotyczących bezpieczeństwa informacji, przeprowadzania okresowych analiz zarządzania bezpieczeństwem, monitorowania dostępu do informacji i zapewnienia audytów wewnętrznych z zakresu bezpieczeństwa informacji.
4. Wykonywanie obowiązków wynikających z art. 36a ust. 2 ustawy o ochronie danych osobowych, w tym przeprowadzanie okresowych kontroli zgodności przetwarzania danych osobowych z przepisami o ochronie danych osobowych i rzetelne prowadzenie rejestru zbiorów danych.
5. Uzupełnienie ewidencji osób upoważnionych do przewarzania danych osobowych o identyfikatory pracowników przetwarzających dane z wykorzystaniem systemów informatycznych, stosownie do dyspozycji art. 39 ust. 1 pkt 3 ustawy o ochronie danych osobowych.
6. Zarejestrowanie w GIODO brakujących trzech zbiorów danych osobowych prowadzonych z wykorzystaniem systemów informatycznych oraz zgłoszenie wszelkich zmian dotyczących zarejestrowanych zbiorów danych, zgodnie z wymogami art. 41 ust. 2 ustawy o ochronie danych osobowych.
7. Gromadzenie danych osobowych w zbiorach w zakresie niezbędnym do realizacji zadań przypisanych Urzędowi, stosownie do art. 23 ust. 1 pkt 2 powołanej ustawy.

V. Pozostałe informacje i pouczenia

Prawo zgłoszenia zastrzeżeń

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

Zgodnie z art. 54 ustawy o NIK, kierownikowi jednostki kontrolowanej przysługuje prawo zgłoszenia na piśmie umotywowanych zastrzeżeń do wystąpienia pokontrolnego, w terminie 21 dni od dnia jego przekazania. Zastrzeżenia zgłasza się do dyrektora 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 31 stycznia 2018 r.

Kontroler
Adrian Gosk
specjalista kontroli państwowej

.....
podpis

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

.....
podpis