NAJWYŻSZA IZBA KONTROLI
Delegatura w Białymstoku

LBI.410.023.09.2017
P/17/062

02260817

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
Kontroler	Jerzy Chwiedosik – główny specjalista kontroli państwowej, upoważnienie do kontroli nr LBI/160/2017 z 21 listopada 2017 r. (dowód: akta kontroli str. 1-2)
Jednostka kontrolowana	Urząd Gminy Sidra (zwany dalej „Urzędem"), Rynek 5, 16-124 Sidra
Kierownik jednostki kontrolowanej	Jan Hrynkiewicz, Wójt Gminy Sidra od 1998 roku (dowód: akta kontroli str. 4)

II. Ocena kontrolowanej działalności[1]

Ocena ogólna

Najwyższa Izba Kontroli ocenia negatywnie zapewnienie przez Urząd[2] właściwej ochrony elektronicznych zasobów informacyjnych przed nieuprawnionym dostępem, przejęciem lub zniszczeniem.

Uzasadnienie oceny ogólnej

Stwierdzono bowiem szereg nieprawidłowości, polegających w szczególności na:

- niezgłoszeniu Generalnemu Inspektorowi Ochrony Danych Osobowych (dalej „GIODO") do zarejestrowania dwóch z 15 prowadzonych zbiorów danych osobowych oraz wyrejestrowania zbioru, który nie był już prowadzony,
- nieprzeprowadzaniu okresowych analiz ryzyka utraty integralności, dostępności lub poufności informacji, co stanowiło naruszenie wymogów § 20 ust. 2 pkt 3 rozporządzenia Rady Ministrów z dnia 12 kwietnia 2012 r. w sprawie Krajowych Ram Interoperacyjności, minimalnych wymagań dla rejestrów publicznych i wymiany informacji w postaci elektronicznej oraz minimalnych wymagań dla systemów teleinformatycznych[3] (zwanego dalej „rozporządzeniem KRI"),
- niemonitorowaniu dostępu do informacji,
- archiwizowaniu baz danych w sposób niezgodny z ustalonymi zasadami,
- nierealizowaniu przez Wójta Gminy Sidra[4] zadań określonych w art. 36a ust. 2 pkt 1 lit. a, b w związku z art. 36b ustawy z dnia 29 sierpnia 1997 r. o ochronie danych osobowych[5],
- przeprowadzaniu audytów w zakresie bezpieczeństwa informacji rzadziej niż raz na rok,
- umożliwieniu Administratorowi Systemów Informatycznych (dalej „ASI") dostępu do wszystkich systemów, w których przetwarzano dane bez upoważnienia ADO,
- sprzątaniu po godzinach pracy Urzędu pomieszczeń, w których przetwarzano dane osobowe bez obecności upoważnionego pracownika i bez zgody Wójta na dostęp do tych pomieszczeń po godzinach pracy,
- niezapewnieniu właściwej ochrony urządzeń znajdujących się w serwerowni.

---

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

[2] Kontrolą objęty został okres od 1 stycznia 2016 r. do rozpoczęcia czynności kontrolnych – 23 listopada 2017 r.

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

[4] Zwanego dalej „Wójtem" lub Administratorem Danych Osobowych – „ADO".

[5] Dz. U. z 2016 r. 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 Urzędzie do gromadzenia i przetwarzania danych osobowych były wykorzystywane następujące systemy informatyczne: ŹRODŁO, SELwin, USCwin, CEiDG, Fiskus, Podatki lokalne, Płace, Płatnik. Przyjęto wysoki poziom zabezpieczeń w związku z tym, że wszystkie stanowiska komputerowe, na których znajdowały się systemy służące do przetwarzania danych osobowych, poza przeznaczonymi do obsługi systemu ŹRÓDŁO, posiadały dostęp do Internetu.

W trakcie oględzin wszystkich 17 komputerów, w tym 16 wchodzących w skład sieci LAN Urzędu ustalono, że żaden użytkownik nie posiadał uprawnień administratora systemu operacyjnego – były one przypisane do wydzielonego konta administratora, w każdym przypadku dostęp do systemu operacyjnego był zabezpieczony loginem i hasłem, na wszystkich stanowiskach konfiguracja komputera umożliwiała uaktywnienie się wygaszacza ekranu po 10 minutach, a powrót do systemu wymagał podania loginu i hasła dostępu. Na stanowiskach (z wyjątkiem komputera, na którym znajdowały się systemy ŹRÓDŁO, SELwin i USCwin) zainstalowany był aktualny program antywirusowy. Cztery komputery z zainstalowanym systemem operacyjnym Windows XP nie były wykorzystywane do przetwarzania danych. Nieaktualny system operacyjny był też na komputerze z systemem ŹRÓDŁO. W większości przypadków ekran monitora uniemożliwiał wgląd osobom postronnym. (dowód: akta kontroli str. 112-134, 209-210)

1.2. W Urzędzie nie udokumentowano przeprowadzania okresowych analiz ryzyka utraty integralności, dostępności oraz poufności informacji, co szerzej przedstawiono w dalszej części wystąpienia, w sekcji „Ustalone nieprawidłowości". (dowód: akta kontroli str. 265)

1.3. Wszyscy pracownicy Urzędu (14 osób) posiadali uprawnienia użytkowników nadane przez ASI oraz własny login i hasło. Nadane uprawnienia były adekwatne do zadań wynikających z ich zakresów czynności. Hasła dostępu 12 użytkowników spełniały wymagania określone w załączniku (rozdział B pkt VIII) 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[6] (dalej „rozporządzenie w sprawie dokumentacji i warunków technicznych"), bowiem ich złożoność odpowiadała wysokiemu poziomowi bezpieczeństwa. Dostęp do komputera z systemami ŹRÓDŁO, SELwin i USCwin (bez dostępu do Internetu) był zabezpieczony hasłem, odpowiadającym wymogom rozdziału A pkt IV załącznika do powołanego rozporządzenia., natomiast dostęp do laptopa ASI był zabezpieczony czytnikiem linii papilarnych.

W latach objętych kontrolą zmiana stanowiska pracy dotyczyła ASI. Został on zatrudniony na stanowisku inspektora ds. wojskowych, obronnych i gospodarczych na miejsce osoby, która przeszła na emeryturę. Zmiana ta nie skutkowała koniecznością wprowadzenia zmian uprawnień tego pracownika w systemach informatycznych Urzędu. Zagadnienia dotyczące zatrudnienie ASI szerzej opisano w pkt 2.6. niniejszego wystąpienia.
(dowód: akta kontroli str. 4, 80-81, 112-133)

1.4. W latach objętych kontrolą w Urzędzie nie prowadzono rejestru dostępu do systemu w formie papierowej i elektronicznej. Każda z końcówek klienckich (komputerów) zapisywała logi związane ze swoją pracą, ale nie były one zabezpieczone przed modyfikacją i zniszczeniem, co opisano w dalszej części wystąpienia, w sekcji „Ustalone nieprawidłowości". Tryb zarządzania logami (ich zawartość i czas przechowywania) był zgodny z ustawieniami domyślnymi przewidzianymi przez producenta (nie ustalono zakresu ustawień routera, gdyż był on administrowany poza Urzędem). Logi routera, serwera i aplikacji na nim działających były zabezpieczone przed dostępem użytkowników systemu.

---

[6] Dz. U. Nr 100 poz. 1024.

Informacje zawarte w logach nie były przetwarzane automatycznie przez administratora sytemu. (dowód: akta kontroli str. 112-134, 215)

1.5. W Urzędzie zapewniono środki uniemożliwiające nieautoryzowany dostęp na poziomie systemów operacyjnych poprzez zastosowanie wymuszenia okresowej zmiany hasła. Dwie sieci WI-FI, stanowiące integralną część sieci LAN, były zabezpieczone poprzez filtrację adresów MAC, a dostęp do nich posiadały wybrane osoby. Nie gromadzono logów dotyczących pracy i dostępu do sieci, ze względu na zrealizowanie jej na niskiej klasy urządzeniu. Funkcjonujące w Urzędzie regulacje w zakresie bezpieczeństwa systemów informatycznych nie uwzględniały zagadnień związanych z dostępem do bezprzewodowej sieci komputerowej. (dowód: akta kontroli str. 7-34, 112-134, 214)

1.6. Wewnętrzne akty prawne dotyczące gromadzenia i przetwarzania danych osobowych nie regulowały kwestii związanych z wykorzystywaniem przez pracowników sprzętu niebędącego własnością pracodawcy. Konfiguracja sieciowa umożliwiała podłączenie do infrastruktury Urzędu sprzętu komputerowego niestanowiącego własności pracodawcy, ale nie było możliwe korzystanie z jej zasobów za pomocą takiego sprzętu. Informacje o podłączeniu do komputerów nośników pamięci (np. pendrive, dysk przenośny) były domyślnie zapisywane w logach systemu komputerowego, lecz nie były zabezpieczone w sposób trwały. W toku oględzin komputerów nie stwierdzono przypadków wykorzystywania przez pracowników Urzędu prywatnego sprzętu do realizacji zadań służbowych. (dowód: akta kontroli str. 5-34, 215-216)

1.7. W Urzędzie w latach 2016 – 2017 (do 23 listopada), nie wykryto przypadków nieautoryzowanych działań związanych z przetwarzaniem informacji.
(dowód: akta kontroli str. 260)

1.8. W Urzędzie wykorzystywano trzy laptopy. W „Polityce bezpieczeństwa systemów informatycznych służących do przetwarzania danych osobowych w Urzędzie Gminy Sidra"[7] oraz w „Instrukcji zarządzania systemami informatycznymi służącymi do przetwarzania danych osobowych w Urzędzie Gminy Sidra"[8] nie przewidziano możliwości mobilnego przetwarzania danych osobowych oraz pracy na odległość. Na routerze CISCO zestawiono dwa VPN z siecią Urzędu Marszałkowskiego Województwa Podlaskiego i Centrum Informatyki ZETO S.A. Były one wykorzystywane odpowiednio do zarządzania routerem i realizacji prac serwisowych na serwerze EZD. Działanie aplikacji pulpitu zdalnego TeamViever, używanej przez ZETO S.A., nie było ewidencjonowane, co szerzej opisano w dalszej części wystąpienia, w sekcji „Ustalone nieprawidłowości".
(dowód: akta kontroli str. 5-34, 215-216)

1.9. W latach objętych kontrolą obowiązywały cztery umowy zawarte z Centrum Informatyki ZETO S.A. w zakresie serwisowania oraz udostępniania nowych wersji oprogramowania C. I. ZETO S.A., U I Info-System s.j., SYGNITI S.A.[9] Stosownie do postanowień § 20 ust. 2 pkt 10 rozporządzenia KRI, w umowach tych zawarto klauzule dotyczące zachowania bezpieczeństwa informacji. (dowód: akta kontroli str. 87-111)

1.10. Wszystkie komputery wchodzące w skład sieci lokalnej Urzędu zostały zabezpieczone programem antywirusowym, który automatycznie dokonywał aktualizacji bazy wirusów. Sieć była odseparowana od Internetu firewallem stanowiącym integralną część routera CISCO.
(dowód: akta kontroli str. 112-134, 214)

1.11. Poczta Urzędu znajdowała się na serwerze udostępnionym przez Centrum Informatyki ZETO S.A., na podstawie umów zawartych 17 września 2013 r. i 17 września 2017 r. Konta poczty służbowej pracowników Urzędu znajdowały się na platformie regionalnej Wrota Podlasia, utworzonej w wyniku realizacji projektu pn. *„Wdrażanie elektronicznych usług dla ludności w województwie podlaskim"*[10]. Poczta Urzędu oraz poczta pracowników Urzędu

---

[7] Dalej zwana „Polityką bezpieczeństwa".

[8] Dalej zwana „Instrukcją zarządzania systemami informatycznymi".

[9] Umowy z 1 kwietnia 2014 r. i 1 kwietnia 2017 r. dotyczące serwisowania i udostępniania nowych wersji programowania Budżet, Kadry i Płace, Podatki, KSZOB, Podatki IPE-PN, SELWIN, RWWIN, USC WIN oraz umowy z 1 października 2013 r. i 1 października 2016 r. dotyczące serwisowania i udostępniania nowych wersji programowania Księgowość i Opłata za gospodarowanie odpadami.

[10] Zapewnienie pracownikom Urzędu dostępu do poczty elektronicznej nastąpiło na podstawie umowy o współpracy w ramach Systemu Wrota Podlasia, zawartej 29 grudnia 2015 r. między Gminą Sidra a Województwem Podlaskim.

była odpowiednio zabezpieczona przed wiadomościami typu SPAM oraz przesyłaniem szkodliwego oprogramowania. (dowód: akta kontroli str. 112-133, 135-164)

1.12. Zagadnienia dotyczące tworzenia i przechowywania kopii bezpieczeństwa danych zostały uregulowane w Instrukcji zarządzania systemami informatycznymi. W myśl postanowień § 17 tej Instrukcji *„Administrator bezpieczeństwa informacji tworzy codziennie kopie awaryjne, sprawdzając co tydzień, pod kątem ich dalszej przydatności do odtworzenia danych w przypadku awarii systemu. Po ustaniu użyteczności kopii awaryjnych są one bezpowrotnie usuwane. Kopie awaryjne są przechowywane w innym pomieszczeniu niż przechowywane są zbiory danych osobowych eksploatowane na bieżąco"*. W Urzędzie proces tworzenia kopii bezpieczeństwa nie odpowiadał regulacjom wewnętrznym, co szerzej opisano w dalszej części wystąpienia, w sekcji „Ustalone nieprawidłowości".

ASI wyjaśnił, że w latach 2016 – 2017 (do 23 listopada) nie było konieczności przywracania danych z kopii bezpieczeństwa. Nie zaistniały też przypadki fizycznej utraty danych.
(dowód: akta kontroli str. 112-134, 215, 260-261)

1.13. Pracownicy Urzędu mieli możliwość ściągania aplikacji i plików wykonalnych, ale nie posiadali uprawnień do instalowania ich na stacjach komputerowych, do których mieli dostęp. Uprawnienia do konfiguracji systemów komputerów działających w sieci LAN posiadał tylko administrator. Spośród 16 komputerów pracujących w sieci LAN Urzędu, cztery, na których nie przetwarzano danych osobowych, posiadały system operacyjny Windows XP, niewspierany przez producenta tego oprogramowania, co szerzej opisano w dalszej części wystąpienia pokontrolnego, w sekcji „Uwagi dotyczące badanej działalności". (dowód: akta kontroli str. 112-134, 216)

ASI prowadził wykaz stacji roboczych znajdujących się w Urzędzie, w którym były ujęte dane dotyczące systemów operacyjnych zainstalowanych na komputerach. Ewidencja nie obejmowała pozostałych zainstalowanych programów, co szerzej opisano w pkt. 3.2. wystąpienia pokontrolnego. (dowód: akta kontroli str. 229-230)

1.14. W Urzędzie, zgodnie z § 20 ust. 2 pkt 12 lit. a rozporządzenia KRI, zadbano o aktualizację systemów operacyjnych oraz aplikacji bezpieczeństwa, które (poza zainstalowanymi na komputerze służącym do obsługi systemu ŹRÓDŁO) były aktualizowane zgodnie z harmonogramem domyślnie ustawionym przez dostawcę.
(dowód: akta kontroli str. 112-134, 216)

1.15. W Urzędzie nie wprowadzono wewnętrznych regulacji dotyczących dokonywania płatności drogą elektroniczną. Oględziny komputerów Urzędu wykazały, że płatności takich dokonywano przy wykorzystaniu komputera zlokalizowanego w Referacie Finansowym (pokój nr 9), na którym był zainstalowany program Home Banking. Dostęp do tego programu posiadało dwóch pracowników Referatu Finansowego. Logowanie następowało po podaniu loginu i hasła. Realizacja płatności wymagała autoryzacji dwóch z czterech osób uprawnionych do jej dokonywania[11], poprzez podanie PIN.
(dowód: akta kontroli str. 127-128, 265)

Ustalone nieprawidłowości

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

1. W latach objętych kontrolą w Urzędzie nie przeprowadzano okresowych analiz ryzyka utraty integralności, dostępności lub poufności informacji, co stanowiło naruszenie wymogów § 20 ust. 2 pkt 3 rozporządzenia KRI.

   ADO wyjaśnił: *„Nie przeprowadzano okresowych analiz ryzyka z uwagi na brak wiedzy w tym zakresie"*. Podobnej treści wyjaśnienia złożył ASI.
   (dowód: akta kontroli str. 257, 260, 265)

2. ADO nie zapewnił ochrony przetwarzanych danych poprzez monitorowanie dostępu do informacji, gdyż nie prowadzono zbiorczego rejestru dostępu do systemu w formie papierowej ani elektronicznej. Każdy z komputerów zapisywał logi związane ze swoją pracą, jednak nie były one zabezpieczone przed modyfikacją i zniszczeniem. Ponadto

[11] Uprawnienia do autoryzacji posiadali Wójt Gminy, Skarbnik, Sekretarz oraz inspektor zatrudniony w Referacie Finansowym Urzędu.

informacje zawarte w logach nie były przetwarzane automatycznie przez administratora systemu. Stanowiło to naruszenie wymogów zawartych w § 20 ust. 2 pkt 7 lit. a rozporządzenia KRI.

ADO wyjaśnił: *„Brak monitoringu dostępu do informacji wynikał z braku wiedzy mojej i pracowników Urzędu".* (dowód: akta kontroli str. 112-133, 215, 257)

3. Centrum Informatyki ZETO S.A. przy realizacji prac serwisowych składników systemu Urzędu korzystało z aplikacji pulpitu zdalnego TeamViever, który nie wymaga od podłączonego użytkownika jakiejkolwiek autoryzacji, korzysta z autoryzacji użytkownika udostępniającego pulpit. 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.

   ASI wyjaśnił: *„Nieprzeprowadzanie nadzoru nad aplikacją TeamViever wynikało z braku wiedzy jak należy to zrobić. Pracownik firmy ZETO, w rozmowie telefonicznej w dniu 11 grudnia 2017 r. poinformował mnie, że połączenie przez aplikację zdalnej pomocy TeamViever są logowane i w łatwy sposób firma może określić kto udział zdalnej pomocy".* (akta kontroli str. 215-216, 262)

4. Backupy baz danych programów wykorzystywanych do księgowości i obsługi podatków, robiono codziennie i zapisywano na przeznaczonym do tego serwerze, przy czym aktualnie wykonywany backup nadpisuje ostatnio wykonaną kopię, co sprawia, że przechowywana jest tylko kopia, która wykonana została najwcześniej – kopia z dnia minionego. Kopie nie są zapisywane na dyski optyczne. Pliki pracowników nie są backupowane. Ponadto dane z programów do ewidencji ludności SelWin oraz aktów stanu cywilnego USCwin kierownik USC archiwizowała na dysku twardym komputera, na którym były zainstalowane te programy. Raz na dwa tygodnie dane te zgrywała na pendrive. Archiwizacja danych programu Fiskus (wykorzystywanego do ewidencjonowania deklaracji dotyczących ustalenia wysokości opłaty za gospodarowanie odpadami komunalnymi) następowała raz na kwartał, na serwerze Urzędu, na którym znajdowała się baza danych tego programu. Sporządzanie kopii bezpieczeństwa nie odpowiadało wymogom zawartym w § 17 Instrukcji zarządzania systemami informatycznymi, w myśl których: *„Administrator bezpieczeństwa informacji tworzy codziennie kopie awaryjne, sprawdzając co tydzień, pod kątem ich dalszej przydatności do odtworzenia danych w przypadku awarii systemu. Po ustaniu użyteczności kopii awaryjnych są one bezpowrotnie usuwane. Kopie awaryjne są przechowywane w innym pomieszczeniu niż przechowywane są zbiory danych osobowych eksploatowane na bieżąco".*

   ASI wyjaśnił: *„Uważałem, że taki sposób archiwizacji zapewnia bezpieczeństwo danych i możliwość ich przywrócenia po ewentualnej awarii. Od 1 grudnia 2017 r. kopie bazy danych z programów do księgowości są dodatkowo kopiowane raz w tygodniu na serwerze Urzędu. Nie wiedziałem, że kwestie dotyczące archiwizacji zostały uregulowane w Instrukcji zarządzania systemami informatycznymi Urzędu".*
   (dowód: akta kontroli str. 20, 112-113, 123-129, 273)

Uwagi dotyczące badanej działalności

Najwyższa Izba Kontroli zwraca uwagę, że z dniem 8 kwietnia 2014 r. producent oprogramowania zakończył udzielanie wsparcia dla systemu operacyjnego Windows XP, a w konsekwencji oprogramowanie to, zainstalowane na czterech komputerach, może nie dość skutecznie chronić dane przetwarzane na tych urządzeniach.

ASI wyjaśnił: *„Komputery po zakończeniu wsparcia oprogramowania Windows XP (po 8 kwietnia 2014r.) były sukcesywnie wymieniane na komputery z Windowsem 7 oraz nowszym (wspieranym przez producenta) Z braku środków finansowych do wymiany zostały 4 komputery z Windowsem XP, które zostaną wymienione do końca roku 2017 (...)".*
(akta kontroli str. 116-117, 122, 132, 262)

Ocena cząstkowa

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

2. Dokumentacja i procedury dotyczące ochrony danych

Opis stanu faktycznego

2.1. ADO zgłosił do GIODO sześć (z 15) prowadzonych zbiorów danych, w tym pięć obejmujących: [1] akta stanu cywilnego, [2] ewidencję ludności i dowody osobiste, [3] rejestr przedpoborowych i poborowych, [4] podatki lokalne, [5] ewidencję pojazdów i kierowców (13 października 1999 r.) oraz zbiór oświadczenia majątkowe (31 maja 2011 r.). Ponadto 3 kwietnia 2017 r. Urząd dokonał rejestracji zbioru karta dużej rodziny[12]. Siedem zbiorów, na podstawie art. 43 ust. 1 ustawy o ochronie danych osobowych, nie podlegało rejestracji[13]. W okresie objętym kontrolą nie było przypadków odmowy rejestracji zbiorów.

Zgłoszenia zbiorów oświadczenia majątkowe oraz karta dużej rodziny zawierały elementy wymagane art. 41 ust. 1 pkt 1-7 ustawy o ochronie danych osobowych. W dokumentacji Urzędu nie ma natomiast wniosków o rejestrację pozostałych zbiorów danych. ADO wyjaśnił: *„Poprzedni Sekretarz Gminy zgłosił do rejestracji zbiory danych, ale nie wiem czy i komu przekazał te dokumenty po odejściu z pracy.*

(dowód: akta kontroli str. 176-200, 203-207, 209-210, 258)

Nie zgłoszono do rejestracji dwóch zbiorów – rejestr cudzoziemców i rejestr wyborców, co szczegółowo przedstawiono w dalszej części wystąpienia pokontrolnego, w sekcji „Ustalone nieprawidłowości". Wójt nie występował do GIODO o zmianę lub wykreślenie zbiorów danych osobowych.

W latach objętych kontrolą ADO nie przetwarzał danych osobowych w zarejestrowanym zbiorze danych ewidencja pojazdów i kierowców oraz nie wystąpił do GIODO o jego wykreślenie, co szczegółowo przedstawiono w dalszej części wystąpienia pokontrolnego, w sekcji „Ustalone nieprawidłowości".

Zakres danych przetwarzanych w pięciu zbiorach[14] zgłoszonych do GIODO i prowadzonych w okresie objętym kontrolą był zgodny z wykazanym w zgłoszeniach.

(dowód: akta kontroli str. 175-198, 209-210, 265, 274)

2.2. ADO nie skorzystał z uprawnienia określonego w art. 36a ust. 1 ustawy o ochronie danych osobowych i nie wyznaczył administratora bezpieczeństwa informacji, chociaż w *„Polityce bezpieczeństwa systemów informatycznych służących do przetwarzania danych osobowych w Urzędzie Gminy Sidra"*[15], ustalonej zarządzeniem Wójta z 20 września 2007 r., przewidziano powołanie takiej osoby oraz wyznaczono jej zadania. Wójt wyjaśnił: *„Nie wyznaczyłem administratora bezpieczeństwa informacji z powodu braku środków finansowych na zatrudnienie osoby posiadającej niezbędne kwalifikacje".*

(dowód: akta kontroli str. 6-14, 257)

2.3. W myśl postanowień art. 36b ustawy o ochronie danych osobowych, w przypadku niepowołania ABI jego zadania, wymienione w art. 36a ust. 2 pkt 1 wyżej powołanej ustawy (z wyłączeniem obowiązku sporządzania sprawozdania, o którym mowa w art. 36a ust. 2 pkt 1 lit. a tej ustawy), wykonuje ADO. W okresie objętym kontrolą ADO realizował jedno z trzech przypisanych mu zadań – zapewniał osobom upoważnionym do przetwarzania danych osobowych możliwość zapoznania z przepisami o ochronie takich danych. Przyczyny niewykonywania pozostałych zadań opisano w dalszej części wystąpienia, w sekcji „Ustalone nieprawidłowości".

ADO zorganizował szkolenie z zakresu ochrony danych osobowych dla wszystkich pracowników Urzędu, co szerzej opisano w pkt 2.8. niniejszego wystąpienia.

(dowód: akta kontroli str. 83-86, 218-219, 223, 226)

Wykaz zbiorów danych przetwarzanych w Urzędzie oraz nazwy programów do ich przetwarzania zostały zamieszczone w załączniku do Polityki bezpieczeństwa, ustalonej

---

[12] Po raz pierwszy ten zbiór danych został zgłoszony do rejestracji przez kierownika Gminnego Ośrodka Pomocy Społecznej w Sidrze. Pismem z 11 sierpnia 2016 r. GIODO poinformował kierownika GOPS, że zgodnie z art. 21 ust. 2 ustawy z dnia 5 grudnia 2014 r. o Karcie Dużej Rodziny (Dz. U. z 2016 r. poz. 195), administratorami danych osobowych przetwarzanych w zakresie niezbędnym do realizacji zadań wynikających z powołanej ustawy są wójt (gmina) oraz minister właściwy do spraw rodziny i dlatego podmioty te są zobowiązane do zgłoszenia zbioru do rejestracji. W rezultacie 3 kwietnia 2017 r. zbiór danych został zgłoszony do rejestracji przez Wójta.

[13] Zbiory danych: podatki od osób prawnych, podatek od środków transportowych od osób fizycznych i prawnych, księgowość, płace, płatnik, VAT, rejestr ewidencji działalności gospodarczej.

[14] Zbiór ewidencja pojazdów i kierowców nie był prowadzony przez Urząd w okresie objętym kontrolą.

[15] Zwana dalej „Polityką bezpieczeństwa".

20 września 2007 r. i nie zmienionej do czasu zakończenia kontroli NIK. W konsekwencji także wykaz zbiorów danych był nieaktualny. (dowód: akta kontroli str. 6-14, 112-134)

2.4. ADO prowadził *„Rejestr osób upoważnionych przez Wójta Gminy Sidra do dostępu i przetwarzania danych osobowych prowadzonych w Urzędzie Gminy Sidra w systemach informatycznych oraz zbiorach papierowych"*. Zawierał on elementy określone w art. 39 ust. 1 pkt. 1 i 2 ustawy o ochronie danych osobowych, tj. imiona i nazwiska osób upoważnionych oraz datę wydania i zakres upoważnienia do przetwarzania danych. Rejestr ten nie zawierał natomiast identyfikatora oraz nie ujęto w nim zmian wynikających z fluktuacji zatrudnienia oraz upoważnień do przetwarzania danych osobowych udzielonych w 2015 roku oraz 7 lutego i 2 sierpnia 2017 r., co szerzej przedstawiono w dalszej części wystąpienia, w sekcji *„Ustalone nieprawidłowości"*. (dowód: akta kontroli str. 165-166)

Zgodnie z Instrukcją zarządzania systemami informatycznymi, system informatyczny Urzędu był wyposażony w mechanizmy uwierzytelnienia użytkownika, a także kontrolę dostępu do danych. Nadzór nad tym sprawował administrator bezpieczeństwa informacji. System zapewniał każdej osobie, której dane przetwarzano odnotowanie informacji komu, kiedy i w jakim zakresie dane te zostały udostępnione.

Wójt wyjaśnił, że nie wie jak rozwiązano kwestie dotyczące nadzoru nad realizacją tych zadań, gdyż zajmowali się tym były i obecny Sekretarz Gminy.

(dowód: akta kontroli str. 19-22, 258)

Stosownie do wymogów art. 37 ustawy o ochronie danych osobowych, Wójt otrzymał od Ministra Spraw Wewnętrznych upoważnienie do przetwarzania danych osobowych zgromadzonych w rejestrze PESEL, rejestrze Dowodów Osobistych i rejestrze Stanu Cywilnego oraz w systemach teleinformatycznych, w których prowadzono te rejestry (System Rejestrów Państwowych ŹRÓDŁO), a także upoważnienie do udzielania dalszych imiennych upoważnień pracownikom Urzędu do przetwarzania danych osobowych w tych rejestrach, w związku z wykonywaniem powierzonych zadań (31 października 2014 r.). W dniu 13 stycznia 2015 r. Wójt upoważnił kierownika Urzędu Stanu Cywilnego oraz podinspektora do przetwarzania danych osobowych w ww. rejestrach i systemach teleinformatycznych. Pismem z 14 stycznia 2015 r. Wójt poinformował Ministerstwo Spraw Wewnętrznych o udzielonych upoważnieniach do przetwarzania danych osobowych.

(dowód: akta kontroli str. 168-171)

2.5. W latach objętych kontrolą w Urzędzie nie były wydawane wewnętrzne akty prawne dotyczące ochrony danych osobowych, poza opisanymi w pkt 2.10. niniejszego wystąpienia.

(dowód akta kontroli str. 265)

2.6. W latach 2016 – 2017 (do 23 listopada) zadania związane z prowadzeniem konsultacji i instruktażu pracowników Urzędu w zakresie funkcjonowania i obsługi oprogramowania komputerowego, usuwania nieprawidłowości w funkcjonowaniu oprogramowania, konserwacją platformy sprzętowej, opracowywaniem modyfikacji na potrzeby Urzędu oraz wykonywaniem kopii zapasowych danych realizował pracownik Urzędu[16], od 17 sierpnia 2014 r. do 31 lipca 2017 r. zatrudniony na stanowisku kierowcy, a od 1 sierpnia 2017 r. – na stanowisku podinspektora ds. wojskowych, obronnych i gospodarczych. Podstawę wykonywania tych zadań stanowiły umowy zlecenia z 31 grudnia 2015 r. i 31 grudnia 2016 r. ASI posiadał dostęp do wszystkich systemów przetwarzania danych zainstalowanych na komputerach działających w sieci Urzędu, jednak nie uzyskał od ADO stosownego upoważnienia, co szerzej przedstawiono w dalszej części wystąpienia, w sekcji „Ustalone nieprawidłowości". (dowód: akta kontroli str. 76-83, 266)

2.7. W latach objętych kontrolą przeprowadzono jeden audyt wewnętrzny z zakresu bezpieczeństwa informacji. Od 6 kwietnia do 12 maja 2017 r. wykonała go firma STS Elektronik Optimus S.A. Partner Stanisław Sakowicz w Białymstoku, na podstawie umowy zawartej 31 marca 2017 r. z Gminą Sidra. Audyt wykazał m.in., że:

- dokumentacja Urzędu dotycząca przetwarzania danych była niedostosowana do przepisów prawa i stosowanych procedur,

[16] Zwany a dalszej części wystąpienia Administratorem Sieci Informatycznej – „ASI".

- nie ustalono procedury zarządzania kluczami; każdy pracownik dysponował własnym kompletem kluczy,
- w serwerowni nie zainstalowano czujki alarmowej i przeciwpożarowej,
- nie sprawowano nadzoru nad poprawnością merytoryczną przetwarzanych danych,
- nie przeprowadzano okresowych analiz ryzyka utraty integralności, dostępności lub poufności informacji,
- nie prowadzono monitoringu dostępu do informacji umieszczonych na serwerze,
- nie podejmowano czynności zmierzających do wykrycia nieautoryzowanych działań związanych z przetwarzaniem informacji. (dowód: akta kontroli str. 35-70)

W związku z ustaleniami audytu Wójt opracował harmonogram wdrażania wydanych zaleceń. Ich realizację przewidziano na 2018 rok. Ponadto w czerwcu 2017 roku opracował i wdrożył Instrukcję ustalającą procedury postępowania z kluczami oraz zabezpieczenia pomieszczeń Urzędu, co szczegółowo przedstawiono w pkt 3.1. wystąpienia.
(dowód: akta kontroli str. 73-74, 242-246)

2.8. Wszyscy pracownicy Urzędu uczestniczyli w szkoleniu z zakresu ochrony danych osobowych i bezpieczeństwa informacji[17], przeprowadzonym 6 kwietnia 2017 r. przez STS Elektronik Optimus S.A. Partner Stanisław Sakowicz w Białymstoku, na podstawie umowy zawartej 31 marca 2017 r. (dowód: akta kontroli str. 84-86, 218-219, 226)

2.9. W latach 2016 – 2017 (do 23 listopada) w Urzędzie nie przeprowadzano kontroli w zakresie bezpieczeństwa danych osobowych. Nie odnotowano też wniesienia skarg dotyczących utraty danych osobowych. (dowód: akta kontroli str. 75)

2.10. Zarządzeniami nr 7, 8 i 9 z 20 września 2007 r. Wójt zatwierdził odpowiednio Politykę bezpieczeństwa, Instrukcję zarządzania systemami informatycznym oraz „Instrukcję ochrony danych osobowych"[18]. Polityka bezpieczeństwa zawierała trzy z pięciu elementów wymaganych postanowieniami § 4 rozporządzenia w sprawie dokumentacji i warunków technicznych, tj.: [1] wykaz pomieszczeń tworzących obszar przetwarzania danych osobowych, który jednak nie do końca pokrywał się z aktualnym obszarem przetwarzania danych, [2] wykaz zbiorów danych osobowych wraz ze wskazaniem programów zastosowanych do przetwarzania tych danych; przy czym liczba zbiorów danych i programów wykorzystywanych do ich przetwarzania nie odpowiadały stanowi faktycznemu, [3] określenie środków technicznych i organizacyjnych niezbędnych dla zapewnienia poufności, integralności i rozliczalności przetwarzanych danych. Brakujące elementy Polityki bezpieczeństwa opisano w dalszej części wystąpienia, w sekcji „Ustalone nieprawidłowości".

Instrukcja zarządzania systemami informatycznymi zawierała siedem z ośmiu elementów wymienionych w § 5 rozporządzenia w sprawie dokumentacji i warunków technicznych, z których jeden nie określał części danych, co szerzej opisano w dalszej części wystąpienia, w sekcji „Ustalone nieprawidłowości". W instrukcji opisano: [1] procedury nadawania uprawnień do przetwarzania danych i rejestrowania tych uprawnień w systemie informatycznym oraz wskazanie osoby odpowiedzialnej za te czynności, [2] stosowane metody i środki uwierzytelnienia oraz procedury związane z ich zarządzaniem i użytkowaniem, [3] procedury rozpoczęcia, zawieszenia i zakończenia pracy przeznaczone dla użytkowników systemu, [4] procedury tworzenia kopii zapasowych zbiorów danych, jednak bez wskazania programów i narzędzi programowych służących do ich przetwarzania, [5] miejsce przechowywania kopii zapasowych danych (*„Kopie awaryjne przechowywane są w innym pomieszczeniu niż przechowywane są zbiory danych*

[17] Zakres szkolenia obejmował: [1] definicje dotyczące ochrony danych osobowych i bezpieczeństwa informacji, dopuszczalność przetwarzania danych osobowych, obowiązek informacyjny, zapewnienie poufności, zasady udostępniania oraz powierzania danych osobowych, postępowanie z danymi osobowymi w wersji papierowej, [2] rejestrację danych osobowych, [3] odpowiedzialność karną, [4] zabezpieczenie fizyczne i organizacyjne, osobowe i informatyczne, [5] zasady bezpiecznego użytkowania sprzętu IT, korzystania z oprogramowania, Internetu, poczty elektronicznej, ochrony antywirusowej, [6] stosowanie środków zapewniających bezpieczeństwo informacji, urządzeń i oprogramowania minimalizującego ryzyko błędów ludzkich, [7] nadawanie upoważnień do przetwarzania danych osobowych, [8] politykę haseł, procedurę rozpoczęcia, zawieszenia i zakończenia pracy, [9] bezpieczeństwo w systemach teleinformatycznych, zagrożenia bezpieczeństwa informacji i ich konsekwencje, w tym odpowiedzialność karną.

[18] Zwana dalej „Instrukcją ochrony danych".

osobowych eksploatowanych na bieżąco"); nie wskazano natomiast sposobu i okresu przechowywania elektronicznych nośników informacji zawierających dane osobowe oraz kopii zapasowych danych, [6] sposób zabezpieczenia systemu informatycznego przed działalnością oprogramowania, którego celem jest uzyskanie nieuprawnionego dostępu do systemu informatycznego, [7] opis procedury wykonywania przeglądów i konserwacji systemów oraz nośników informacji służących do przetwarzania danych.

Instrukcja ochrony danych zawierała: [1] określenie pojęć związanych z przetwarzaniem danych, [2] procedurę wykonania obowiązku informacyjnego w odniesieniu do osób, których dane są przetwarzane, ale bez wskazania osoby odpowiedzialnej za realizację obowiązku informacyjnego, [3] obowiązki kadry zarządzającej w zakresie rejestracji zbiorów danych osobowych, [4] zasady zabezpieczenia zbiorów danych osobowych.

Ponadto nie wywiązano się z obowiązku, wynikającego z § 2 pkt 15 w związku z § 20 ust. 1 rozporządzenia KRI, wdrożenia regulacji wewnętrznych stanowiących politykę bezpieczeństwa informacji, co szerzej opisano w dalszej części wystąpienia pokontrolnego, w sekcji „Ustalone nieprawidłowości". (dowód: akta kontroli str. 5-34)

Ustalone nieprawidłowości

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

1. Nie zgłoszono do rejestracji GIODO dwóch spośród 15 prowadzonych zbiorów danych osobowych (rejestr cudzoziemców i rejestr wyborców), co naruszało wymogi art. 40 ustawy o ochronie danych osobowych. Ponadto nie dokonano wyrejestrowania zbioru rejestr pojazdów i kierowców, który nie był już prowadzony w Urzędzie.

   Wójt wyjaśnił: *„Brak zgłoszenia wynikał z przeoczenia Sekretarza Gminy, który prowadził te sprawy".* (dowód: akta kontroli str. 175, 209-210, 257, 265)

2. W latach objętych kontrolą ADO nie realizował zadań określonych w art. 36a ust. 2 pkt 1 lit. a, b w związku z art. 36b ustawy o ochronie danych osobowych, tj. nie sprawdzał zgodności przetwarzania danych osobowych z przepisami o ochronie tych danych i nie nadzorował opracowania i aktualizacji dokumentacji opisującej sposób przetwarzania danych oraz zastosowane środki techniczne i organizacyjne zapewniające ochronę przetwarzanych danych osobowych.

   Wójt wyjaśnił: *„Nie wykonywałem tych zadań z uwagi na brak czasu".*
   (dowód: akta kontroli str. 258, 265)

3. Prowadzony przez ADO *„Rejestr osób upoważnionych przez Wójta Gminy Sidra do dostępu i przetwarzania danych osobowych prowadzonych w Urzędzie Gminy Sidra w systemach informatycznych oraz zbiorach papierowych"* nie zawierał identyfikatorów osób przetwarzających dane w systemie informatycznym. Stanowiło to naruszenie wymogów art. 39 ust. 1 pkt 3 ustawy o ochronie danych osobowych. Ponadto Rejestr prowadzony był w sposób nierzetelny, gdyż: [1] nie zawierał daty ustania ważności upoważnienia pięciu osób, które odeszły z pracy przed 2016 rokiem, [2] nie wymieniono w nim czterech pracowników Urzędu, których Wójt w styczniu i sierpniu 2015 roku oraz 7 lutego i 2 sierpnia 2017 r. upoważnił do przetwarzania danych, a w przypadku kolejnej osoby nie zaktualizowano zakresu przetwarzania przez nią danych osobowych (zmiana na podstawie upoważnienia z 13 stycznia 2015 r.).

   Wójt wyjaśnił: *„Rejestr prowadził Sekretarz Gminy, który w marcu 2012 roku przeszedł na emeryturę. Nowy Sekretarz Gminy nie miał dostatecznej wiedzy i nie aktualizował na bieżąco tego Rejestru. Obecny Sekretarz Gminy od października 2017 roku przebywa na zwolnieniu lekarskim. Najprawdopodobniej jego powrót do pracy nastąpi w styczniu 2018 roku".* (dowód: akta kontroli str. 82,165-166, 170-172, 257)

4. ASI miał dostęp do wszystkich zbiorów danych Urzędu przetwarzanych elektronicznie, mimo że ADO upoważnił go tylko do przetwarzania danych z rejestru przedpoborowych i poborowych (upoważnienie z 2 sierpnia 2017 r.). Stanowiło to naruszenie art. 37 ustawy o ochronie danych osobowych, zgodnie z którym do przetwarzania danych mogą być dopuszczone wyłącznie osoby posiadające upoważnienie nadane przez administratora danych.

Wójt wyjaśnił: *„Nieudzielenie takiego upoważnienia wynikało z przeoczenia".*
(dowód: akta kontroli str. 76-82, 258)

5. ADO nie realizował obowiązku określonego w § 20 ust. 2 pkt 14 rozporządzenia KRI. Od wejścia w życie tego rozporządzenia (31 maja 2012 r.) przeprowadzono bowiem tylko jeden audyt w zakresie bezpieczeństwa informacji, mimo że wyżej powołany przepis obligował do przeprowadzania takiego audytu nie rzadziej niż raz na rok.

   Wójt wyjaśnił: *„Nieprzeprowadzanie corocznych audytów wynikało z braku środków finansowych w budżecie Gminy".* (dowód: akta kontroli str. 41-70, 258)

6. Dokumentacja dotycząca przetwarzania danych osobowych, ustalona 20 września 2007 r. nie była aktualizowana i w konsekwencji była niedostosowana do aktualnych przepisów prawa i stanu faktycznego dotyczącego przetwarzania danych w Urzędzie. Ponadto przyjęte regulacje nie zawierały wymaganych elementów.

   - W Polityce bezpieczeństwa nie zamieszczono opisu struktury zbiorów danych ze wskazaniem zawartości poszczególnych pól informacyjnych i powiązań między nimi, tj. elementów wymaganych przepisem § 4 ust. 3 i 4 rozporządzenia w sprawie dokumentacji i warunków technicznych. Wykaz pomieszczeń tworzących obszar, w którym przetwarzano dane osobowe nie w pełni pokrywał się z aktualnym obszarem przetwarzania danych (nie ujęto w nim dwóch pomieszczeń nr 7 i 8, w których w latach objętych kontrolą, także przetwarzano dane osobowe), a wykaz zbiorów danych osobowych i programów zastosowanych do ich przetwarzania nie odpowiadały stanowi faktycznemu. (dowód: akta kontroli str. 6-14)
   - W Instrukcji zarządzania systemami informatycznymi nie wskazano programów i narzędzi programowych służących do tworzenia kopii zapasowych zbiorów danych, a także sposobu i okresu przechowywania elektronicznych nośników informacji zawierających dane osobowe oraz kopii zapasowych danych, mimo takiego wymogu określonego w § 5 ust. 4 i 5 rozporządzenia w sprawie dokumentacji i warunków technicznych.

   Nie wywiązano się również z obowiązku, wynikającego z § 2 pkt 15 w związku z § 20 ust. 1 rozporządzenia KRI, wdrożenia regulacji wewnętrznych stanowiących politykę bezpieczeństwa informacji.

   Wójt wyjaśnił: *„Brak aktualizacji wynikał z zaniedbań pracowników – Sekretarzy Gminy, którzy zajmowali się tą dokumentacją".* (dowód: akta kontroli str. 6-34, 259)

Ocena cząstkowa

Najwyższa Izba Kontroli ocenia negatywnie opracowanie i wdrożenie dokumentacji oraz procedur dotyczących ochrony danych osobowych w Urzędzie.

3. Sposób przechowywania oraz zabezpieczenia danych

Opis stanu faktycznego

3.1. Zgodnie z Polityką bezpieczeństwa dane osobowe przetwarzane powinny być w wydzielonych pomieszczeniach, zabezpieczonych przed nieuprawnionym wejściem i wyposażonych w szafy dające gwarancję bezpieczeństwa przechowywanej dokumentacji. Wykaz wydzielonych pomieszczeń obejmował cztery pokoje oznaczone numerami 6, 9, 10 i 12. Nie wymieniono w nim dwóch pokoi nr 7 i nr 8, w których w latach objętych kontrolą, także przetwarzano dane osobowe.

Oględziny wykazały, że pomieszczenia, w których przetwarzano zbiory danych osobowych były zamykane na klucz. Na ich wyposażeniu znajdowały się zamykane szafy na dokumenty, w tym w dwóch pokojach były to szafy metalowe. Kraty w oknach zainstalowano w jednym pomieszczeniu, zajmowanym przez pracownika ds. obrony. Drzwi wejściowe do siedziby Gminy były zabezpieczone kratą zamykaną na kłódkę.

Archiwum zakładowe zostało wyposażone w czujnik zadymienia, termometr i higrometr, gaśnicę oraz niszczarkę dokumentów, w tym płyt CD. Nie zapewniono natomiast odpowiedniego wyposażenia serwerowni, co szerzej opisano w dalszej części wystąpienia, w sekcji „Uwagi dotyczące badanej działalności".
(dowód: akta kontroli str. 9-13, 232-236, 238-239)

W dniu 1 czerwca 2017 r. Wójt wprowadził Instrukcję określającą procedury postępowania z kluczami oraz zabezpieczania pomieszczeń Urzędu. Ustalił w niej m.in. miejsce

przechowywania kluczy (zbiorcza szafka w pokoju nr 4), sposób zarządzania kluczami do pomieszczeń służbowych, w tym dostęp do kluczy zapasowych, obowiązki w zakresie zabezpieczenia pomieszczeń oraz sposób dostępu do pomieszczeń po godzinach pracy. Ponadto ustalił, że sprzątaczka dysponująca kluczami do wszystkich pomieszczeń ponosi pełną odpowiedzialność za pozostawiony sprzęt i dokumentację. Ustalona procedura była przestrzegana. (dowód: akta kontroli str. 242-246)

3.2. ASI posiadał wykaz stacji roboczych znajdujących się w Urzędzie (wg stanu na 3 lipca 2017 r.). Zawierał on określenie typu stacji (komputer stacjonarny, laptop), nazwę zainstalowanego systemu operacyjnego, imię i nazwisko oraz stanowisko służbowe użytkownika komputera, informację o dostępie do otwartego Internetu. W przypadku czterech z 17 komputerów wskazano rodzaj licencji systemu operacyjnego. Wykaz nie obejmował natomiast informacji o zainstalowanych programach i aplikacjach oraz posiadanych licencjach, co opisano w dalszej części wystąpienia, w sekcji „Ustalone nieprawidłowości" (dowód: akta kontroli str. 229-230)

3.3. Zasady przekazywania do naprawy, przekazania innemu podmiotowi lub likwidacji dysków oraz innych nośników danych, określone w Instrukcji zarządzania systemami informatycznymi, były zgodne z wytycznymi zawartymi w punkcie VI załącznika do rozporządzenia w sprawie dokumentacji i warunków technicznych.

W Urzędzie nie stwierdzono dokumentów potwierdzających przekazywanie w latach 2016 – 2017 (do 23 listopada) komputerów, dysków lub innych nośników danych do naprawy, likwidacji lub podmiotom nieuprawnionym do przetwarzania danych.

(dowód: akta kontroli str. 21, 261, 266)

3.4. Stosownie do postanowień § 21 Instrukcji zarządzania systemami informatycznymi wydruki, które zawierają dane osobowe i są przeznaczone do usunięcia, należy zniszczyć w stopniu uniemożliwiającym ich odczytanie. Urząd dysponował tylko jedną niszczarką dokumentów. Stanowiła ona wyposażenie archiwum zakładowego. Kluczami do archiwum dysponowała wyłącznie kierownik Urzędu Stanu Cywilnego. Wójt wyjaśnił: *„Mimo, iż niszczarka znajduje się w archiwum, to pracownicy przetwarzający dane osobowe mogą z niej korzystać. Ponadto pracownicy Urzędu mogą korzystać z niszczarki znajdującej się w Biurze Obsługi Szkół, które mieści się na parterze budynku Urzędu".*

(dowód: akta kontroli str. 21, 232-234, 258)

3.5. Pracownikom Urzędu nie umożliwiono zdalnego dostępu do zasobów sieci lokalnej. Zagadnień tych nie uregulowano także w Polityce bezpieczeństwa, Instrukcji zarządzania systemami informatycznymi oraz Instrukcji bezpieczeństwa danych.

(dowód: akta kontroli str. 7-34, 215)

3.6. Sprzątanie pomieszczeń Urzędu, z wyjątkiem serwerowni, należało do obowiązków sprzątaczki zatrudnionej w ramach prac interwencyjnych[19]. Sprzątanie odbywało się po godzinie 15, tj. po zakończeniu pracy Urzędu. W dokumentacji Urzędu nie ma dowodów potwierdzających udzielenie zgody Wójta na przebywanie sprzątaczki po godzinach pracy Urzędu w pomieszczeniach, w których przetwarzane były dane osobowe, co opisano w dalszej części wystąpienia, w sekcji „Ustalone nieprawidłowości".

Pomieszczenia serwerowni były sprzątane przez pracownika, któremu powierzono obsługę informatyczną Urzędu. (dowód: akta kontroli str. 247-248, 267-272)

3.7. Zagadnienia dotyczące wykonywania przeglądów i konserwacji sprzętu komputerowego oraz przekazywania do naprawy i likwidacji nośników informacji do przetwarzania danych uregulowano w Instrukcji zarządzania systemami informatycznymi. W myśl postanowień Instrukcji: [1] przeglądy i konserwacje sprzętu komputerowego są dokonywane okresowo, przez wyspecjalizowaną firmę, pod nadzorem administratora bezpieczeństwa informacji (do rozpoczęcia kontroli NIK administrator nie został powołany), przy wyłączonych komputerach, aby zgromadzone dane nie były dostępne dla osób nieuprawnionych, [2] dyski lub inne nośniki zawierające dane osobowe naprawia się pod nadzorem osoby upoważnionej przez ADO lub przed naprawą usuwa się zapisane na nich dane,

[19] W latach objętych kontrolą sprzątaniem pomieszczeń Urzędu zajmowały się dwie osoby, jedna od 29 kwietnia 2016 r. do 30 kwietnia 2017 r., a kolejna od 1 maja 2017 r.

[3] w przypadku likwidacji dysków i innych nośników usuwa się z nich zapisane dane albo uszkadza w sposób uniemożliwiający odczytanie tych danych.

W latach objętych kontrolą serwisem oprogramowania zajmowało się Centrum Informatyki ZETO S.A., na podstawie umów zawartych 1 października 2013 r., 14 kwietnia 2014 r., 1 października 2016 r. i 1 kwietnia 2017 r. (dowód: akta kontroli str. 18-22, 87-111)

3.8. W Urzędzie nie opracowano procedur postępowania w sytuacjach nadzwyczajnych (awaria, długotrwały brak zasilania), w tym dotyczących zasad przywracania systemów po awarii oraz zachowania ciągłości działania i kontynuacji wykonywania zadań publicznych, co szerzej opisano w dalszej części wystąpienia, w sekcji „Uwagi dotyczące badanej działalności". W toku oględzin ustalono, że wszystkie komputery stacjonarne Urzędu były podłączone do urządzeń UPS, pozwalających na kilkuminutową pracę w przypadku przerw w dostawie energii elektrycznej. Urząd dysponował też agregatem prądotwórczym. (dowód: akta kontroli str. 112-134, 258, 266)

3.9. Jak wyjaśnił ASI, w latach 2016 – 2017 (do 23 listopada) w Urzędzie nie było przypadków fizycznej utraty danych. (dowód: akta kontroli str. 261)

Ustalone nieprawidłowości

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

1. Przyjęte zabezpieczenia serwera Urzędu przed uszkodzeniem były niewystarczające. W serwerowni nie zainstalowano bowiem klimatyzacji ani sygnalizacji przegrzania serwera oraz alarmu przeciwpożarowego bądź czujnika dymu. Bezpieczeństwu serwera i przechowywanych na nim danych nie sprzyjało także wykorzystywanie serwerowni jako magazynu zużytego sprzętu komputerowego. ADO wyjaśnił: *„W budżecie gminy nie było środków na zakup klimatyzatora. Wykorzystywanie tego pomieszczenia jako magazynu nastąpiło bez mojej wiedzy".* (dowód: akta kontroli str. 235-236, 258)

2. Nie gromadzono bieżących informacji o oprogramowaniu służącym do przetwarzania danych, obejmujących jego rodzaj i konfigurację mimo takiego wymogu określonego w § 20 ust. 2 pkt 2 rozporządzenia KRI. W myśl powołanego przepisu zarządzanie bezpieczeństwem informacji realizowane powinno być w szczególności przez zapewnienie przez kierownictwo podmiotu publicznego warunków umożliwiających realizację i egzekwowanie działań utrzymywania aktualności inwentaryzacji sprzętu i oprogramowania służącego do przetwarzania informacji obejmującej ich rodzaj i konfigurację.

   ASI wyjaśnił: *„Nie wiedziałem, że takie informacje powinny być zawarte w wykazie".* (dowód: akta kontroli str. 229-231)

3. Pomieszczenia Urzędu, w tym te, w których przetwarzano dane sprzątano po godzinach pracy Urzędu, przez sprzątaczki, które nie posiadały zgody Wójta na przebywanie w obszarze przetwarzania danych osobowych pod nieobecność osób przetwarzających takie dane. Stanowiło to naruszenie wymogów zawartych w części A pkt I załącznika do rozporządzenia w sprawie dokumentacji i warunków technicznych, zgodne z którymi przebywanie osób nieuprawnionych w obszarze przetwarzania danych osobowych jest dopuszczalne za zgodą administratora danych lub w obecności osoby upoważnionej do przetwarzania danych osobowych.

   Wójt wyjaśnił: *„Nie udzieliłem takiej zgody, ponieważ uważałem, że w zupełności wystarcza zawarta umowa o pracę".* (dowód: akta kontroli str. 247, 259, 267-272)

Uwagi dotyczące badanej działalności

Najwyższa Izba Kontroli zwraca uwagę na potrzebę opracowania wewnętrznych regulacji dotyczących rozwiązań na wypadek wystąpienia sytuacji nadzwyczajnych, np. długotrwałego braku zasilania bądź przywracania systemów po awarii, a także planu ciągłości działania umożliwiającego kontynuację wykonywania zadań jednostki. Plan ten powinien określić systemy i aplikacje o znaczeniu krytycznym oraz wszystkie podporządkowane lub powiązane plany. Istotne jest, aby plany te były jasno udokumentowane, przekazane pracownikom i aktualizowane w celu odzwierciedlenia bieżącej działalności GOPS. 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. Wójt wyjaśnił, że nieopracowanie takich procedur spowodowane było przeoczeniem.
(dowód: akta kontroli str. 112-134, 258, 266)

Ocena cząstkowa

Najwyższa Izba Kontroli ocenia pozytywnie, mimo stwierdzonych nieprawidłowości, przestrzeganie w Urzędzie przyjętych procedur dotyczących przechowywania i zabezpieczenia danych oraz zapewnienia im właściwej ochrony.

4. Przetwarzanie zasobów informacyjnych zgodnych z zakresem działalności jednostki kontrolowanej

Opis stanu faktycznego

4.1. W Urzędzie prowadzono 15 zbiorów danych, w tym pięć papierowo i dziesięć elektronicznie. Do gromadzenia i przetwarzania danych wykorzystywano systemy: [1] ŹRODŁO i SELwin – ewidencja ludności (rejestry mieszkańców, wyborców, cudzoziemców, dowodów osobistych), [2] USCwin – akta stanu cywilnego, [3] CEiDG – działalność gospodarcza, [4] Fiskus – gospodarka odpadami, [5] Podatki lokalne, [6] Płatnik. (dowód: akta kontroli str. 112-134, 209-210)

4.2. W latach 2016 – 2017 (do 23 listopada) Wójt nie zgłaszał aktualizacji danych zawartych w rejestrze prowadzonym przez GIODO, co szerzej opisano w pkt 2.1. niniejszego wystąpienia. (dowód: akta kontroli str. 265)

4.3. Zakres danych osobowych gromadzonych i przetwarzanych w Urzędzie był niezbędny do realizacji przypisanych zdań.

Urząd wywiązał się z obowiązku poinformowania kandydatów do pracy o konieczności zawarcia w dokumentach aplikacyjnych klauzuli dotyczącej zgody na przetwarzanie danych osobowych do celów realizacji procesu rekrutacji, zgodnie z ustawą o ochronie danych osobowych. (dowód: akta kontroli str. 112-134, 249-256)

4.4. Urząd posiadał dostęp do zewnętrznych zbiorów danych osobowych: ŹRÓDŁO i CEiDG. Dostęp do systemu ŹRÓDŁO uzyskał na podstawie upoważnienia z 31 października 2014 r. nadanego przez Ministra Spraw Wewnętrznych. Urząd spełnił wymogi związane z dostępem do tego systemu. Komputer przeznaczony do obsługi ŹRÓDŁO nie posiadał dostępu do Internetu (w konsekwencji system operacyjny jak i program antywirusowy nie były aktualne[20]). Dwóch pracowników przetwarzających dane w tym systemie posiadało stosowne upoważnienia. Dostęp do systemu CEiDG posiadał jeden pracownik Urzędu, który uzyskał go na podstawie zgłoszenia do Ministerstwa Gospodarki z 5 sierpnia 2015 r. (dowód: akta kontroli str. 112-113, 120, 168-171, 173-174)

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 dostępem do tych zbiorów.

IV. Wnioski

Wnioski pokontrolne

Przedstawiając powyższe oceny wynikające z ustaleń kontroli, Najwyższa Izba Kontroli, na podstawie art. 53 ust. 1 pkt 5 ustawy z dnia 23 grudnia 1994 r. o Najwyższej Izbie Kontroli[21], wnosi o:

1. Przeprowadzanie okresowych analiz ryzyka utraty integralności, dostępności lub poufności informacji.
2. Monitorowanie dostępu do zasobów informacyjnych Urzędu.
3. Dokonywanie archiwizacji baz danych zgodnie z ustalonymi zasadami, zapewniającymi możliwość przywrócenia danych po ewentualnej awarii.
4. Zgłaszanie do rejestracji GIODO wszystkich zbiorów danych przetwarzanych w Urzędzie oraz zmian w zakresie ich przetwarzania.

[20] Według stanu na dzień przeprowadzenia oględzin – 28 listopada 2017 r.
[21] Dz. U. z 2017 r. poz. 524. Ustawa zwana dalej „ustawą o NIK".

5. Realizowania przez ADO zadań określonych w art. 36a ust. 2 pkt 1 lit. a, b w związku z art. 36b ustawy o ochronie danych osobowych.
6. Dostosowanie wykazu zbioru danych przetwarzanych w Urzędzie oraz Rejestru osób uprawnionych do dostępu i przetwarzania tych danych do wymogów określonych w ustawie o ochronie danych osobowych.
7. Dopuszczenie ASI do dostępu do programów przetwarzających dane osobowe po udzieleniu stosownego upoważnienia.
8. Przeprowadzanie, nie rzadziej niż raz w roku, okresowego audytu bezpieczeństwa informacji.
9. Zaktualizowanie Polityki bezpieczeństwa i Instrukcji zarządzania systemami informatycznymi do obowiązujących przepisów prawnych, w tym uzupełnienie ich stosownie do wymogów § 20 ust. 1 rozporządzenia KRI oraz wdrożenie przyjętych zasad zapewniania bezpieczeństwa przetwarzanych danych.
10. Prowadzenie rejestru zasobów informatycznych zgodnie z wymogami określonymi w § 20 ust. 2 pkt 2 rozporządzenia KRI.
11. Zapewnienie obecności upoważnionego pracownika podczas sprzątania pomieszczeń, w których przetwarzane są dane osobowe po godzinach pracy Urzędu lub udzielenie sprzątaczce zgody na przybywanie w tych pomieszczeniach po zakończeniu pracy Urzędu.
12. Zapewnienie właściwej ochrony urządzeń znajdujących się w serwerowni.

V. Pozostałe informacje i pouczenia

Prawo zgłoszenia zastrzeżeń

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

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

Obowiązek poinformowania NIK o sposobie wykorzystania uwag i wykonania wniosków

Zgodnie z art. 62 ustawy o NIK, proszę o poinformowanie Najwyższej Izby Kontroli, w terminie 21 dni od otrzymania wystąpienia pokontrolnego, o sposobie wykorzystania uwag i wykonania wniosków pokontrolnych oraz o podjętych działaniach lub przyczynach niepodjęcia tych działań.

W przypadku wniesienia zastrzeżeń do wystąpienia pokontrolnego, termin przedstawienia informacji liczy się od dnia otrzymania uchwały o oddaleniu zastrzeżeń w całości lub zmienionego wystąpienia pokontrolnego.

Białystok, dnia 17 stycznia 2018 r.

Kontroler
Jerzy Chwiedosik
główny specjalista kontroli państwowej

.....
podpis

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

.....
podpis