NAJWYŻSZA IZBA KONTROLI
Delegatura w Białymstoku

LBI.410.023.10.2017
P/17/062

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

Mariusz Lenkiewicz – starszy inspektor kontroli państwowej, upoważnienie do kontroli nr LBI/161/2017 z 21 listopada 2017 r. (dowód: akta kontroli str. 1-2)

Jednostka kontrolowana

Urząd Gminy Szudziałowo, ul. Bankowa 1, 16-113 Szudziałowo (dalej: „*Urząd*")

Kierownik jednostki kontrolowanej

Tadeusz Tokarewicz – Wójt Gminy Szudziałowo[1] (dowód: akta kontroli str. 3)

II. Ocena kontrolowanej działalności[2]

Ocena ogólna

Najwyższa Izba Kontroli ocenia negatywnie zapewnienie przez Urząd właściwej ochrony elektronicznych zasobów informacyjnych przed nieuprawnionym dostępem, przejęciem lub zniszczeniem w latach 2016 – 2017.

Uzasadnienie oceny ogólnej

Stwierdzono bowiem nieprawidłowości polegające w szczególności na:

- niezastosowaniu środków technicznych mających zapewnić ochronę przetwarzania danych osobowych, w stopniu wymaganym art. 36 ustawy z dnia 29 sierpnia 1997 r. o ochronie danych osobowych[3] (głównie nieodpowiednie zabezpieczenia dostępu do pomieszczenia serwerowni i systemu operacyjnego oraz niezapewnienie pracownikom możliwości korzystania z bezpiecznej elektronicznej poczty służbowej),
- niemonitorowaniu dostępu do informacji, o którym mowa w § 20 ust. 2 pkt. 7 lit. a 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[4],
- sporządzaniu kopii zapasowych dwóch systemów informatycznych z nieodpowiednią częstotliwością, tj. niezgodnie z § 2 pkt IV.3 obowiązującej w Urzędzie Instrukcji zarządzania systemem informatycznym oraz niesprawdzania poprawności ich wykonania,
- niezgłoszeniu do Generalnego Inspektora Ochrony Danych Osobowych (dalej: „*GIODO*") trzech przetwarzanych w Urzędzie zbiorów danych oraz gromadzenia danych osobowych – w dwóch (z 16) zbiorach – w zakresie szerszym niż zgłoszony do GIODO.

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 wykorzystywane były systemy informatyczne służące do obsługi spraw związanych z ewidencją ludności, opłatami i podatkami lokalnymi, gospodarką nieruchomościami, gospodarką odpadami, świadczeniami rodzinnymi, wychowawczymi i opiekuńczymi, zarządzaniem oświatą oraz

[1] Pełniący funkcję Wójta Gminy od 1 grudnia 2014 r.

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

[3] Dz. U. z 2016 r., poz. 922.

[4] Dz. U. z 2017 r. poz. 2247. Rozporządzenie zwane dalej: „*rozporządzeniem KRI*".

księgowością Urzędu, tj. m.in. „*Źródło*”, „*Selwin*”, „*Fiskus*”, „*CEiDG*”, „*Sygnity*”, „*System Informacji Oświatowej*”, „*Płatnik*”, „*Kadry i Płace*” oraz „*Księgowość budżetowa*”. Dane osobowe w Urzędzie przetwarzane były przez pracowników na 18 komputerach (w tym dwóch laptopach), z których 17 posiadało nieograniczony dostęp do Internetu.

(dowód: akta kontroli str. 221-223, 237)

Oględziny wszystkich komputerów Urzędu wykorzystywanych do przetwarzania danych osobowych, wykazały m.in., że: [1] wszyscy użytkownicy posiadali uprawnienia administratora systemu operacyjnego; [2] dostęp do systemu operacyjnego (na domyślnym loginie „*user*”) we wszystkich przypadkach zabezpieczony był hasłem; [3] na wszystkich komputerach zastosowano wygaszacz ekranu (lub automatyczne wylogowanie), uaktywniający się od trzech do 30 minut bezczynności użytkownika[5]; [4] na 13 komputerach zainstalowano program antywirusowy[6], który posiadał aktualną bazę wirusów; [5] na 16 komputerach zainstalowano systemy operacyjne Windows 7 i Windows 10, które były aktualizowane automatycznie[7], zgodnie z ustalonym harmonogramem. Szerzej problem nadanych pracownikom Urzędu uprawnień oraz dostępu do systemów operacyjnych opisano w dalszej części wystąpienia pokontrolnego, w sekcji „*Ustalone nieprawidłowości*”.

(dowód: akta kontroli str. 222-223, 230)

1.2. W Urzędzie 31 stycznia 2017 r. przeprowadzano okresową analizę poufności, integralności i rozliczalności systemów informatycznych pod kątem zagrożeń i ryzyka, o której mowa w § 20 ust. 2 pkt 3 rozporządzenia KRI. Wskazano w niej podstawowe zagrożenia występujące w systemach informatycznych (m.in. nieprzydzielenie użytkownikom indywidualnych identyfikatorów i niewłaściwe administrowanie systemem informatycznym), określono poziom ryzyka utraty bezpieczeństwa danych osobowych na poziomie niskim (7 pkt w skali od jednego do 100), zidentyfikowano największe zagrożenia (m.in. atak wirusa, odcięcie zasilania, pożar lub nieuprawniony dostęp do komputera), sformułowano wnioski i zaproponowano działania naprawcze (m.in. przestrzeganie przepisów powszechnie obowiązujących i procedur wewnętrznych w zakresie przetwarzania danych osobowych) oraz określono przebieg kontroli podatności systemu (m.in. poprzez monitorowanie czy użytkownicy logują się do systemu za pomocą identyfikatora i hasła, czy korzystają z wygaszacza ekranu, itp.).

Przed 2017 rokiem takie analizy nie były przeprowadzane, co szerzej opisano w dalszej części wystąpienia pokontrolnego, w sekcji „*Ustalone nieprawidłowości*”.

(dowód: akta kontroli str. 60-80, 236)

1.3. Wszyscy pracownicy przetwarzający dane osobowe posiadali uprawnienia administratora systemu i hasło dostępu do systemu operacyjnego oraz byli zaangażowani w proces przetwarzania danych osobowych w stopniu adekwatnym do zadań, jakie wynikały z ich zakresów obowiązków[8]. Hasło dwóch (z 16) użytkowników spełniało wymagania – określone w § 2 pkt IV.2 obowiązującej w Urzędzie Instrukcji Zarządzania Systemem Informatycznym oraz w załączniku 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 do przetwarzania danych osobowych – dla wysokiego poziomu bezpieczeństwa[9]. Szerzej problem ten opisano w dalszej części wystąpienia pokontrolnego, w sekcji „*Ustalone nieprawidłowości*”.

(dowód: akta kontroli str. 56-59, 222-224, 237-238)

---

[5] Powrót do systemu wymagał podania hasła użytkownika.

[6] Na pozostałych pięciu komputerach dostępny był Windows Defender, program dostępny przy systemie operacyjnym Windows 10.

[7] Na dwóch komputerach zainstalowany był system operacyjny Windows XP, dla którego wsparcie techniczne upłynęło w 2016 roku.

[8] W latach 2016 – 2017 nie zachodziły okoliczności, które wymagały dokonania zmiany uprawnień w systemach.

[9] Dz. U. Nr 100, poz. 1024. Rozporządzenie dalej zwane *„rozporządzeniem w sprawie dokumentacji i warunków technicznych”*.

1.4. W Urzędzie nie prowadzono zbiorczego rejestru dostępu do systemu operacyjnego zarówno w formie papierowej jak i elektronicznej (np. w postaci logów systemowych). Poszczególne elementy sieci informatycznej Urzędu generowały i przechowywały logi systemowe zgodnie z domyślnymi ustawieniami. Infrastruktura sieci informatycznej nie pozwalała na skuteczne monitorowanie dostępu do informacji gromadzonych w systemach informatycznych, co szerzej opisano w dalszej części wystąpienia pokontrolnego, w sekcji „*Ustalone nieprawidłowości*".

(dowód: akta kontroli str. 6-10, 234, 248-252)

1.5. W Urzędzie, zgodnie z § 20 ust. 2 pkt 7 lit. c rozporządzenia KRI, zapewniono środki uniemożliwiające nieautoryzowany dostęp do usług sieciowych i urządzeń serwerowni, poprzez zabezpieczenie ich hasłem znanym jedynie Administratorowi Systemu Informatycznego (dalej: „*ASI*"). Natomiast wprowadzone środki techniczne, mające na celu zabezpieczenie dostępu do systemów operacyjnych, jak również do pomieszczenia serwerowni, były niewystarczające, co opisano w dalszej części wystąpienia pokontrolnego, w sekcji „*Ustalone nieprawidłowości*". (dowód: akta kontroli str. 6-10)

1.6. W regulacjach wewnętrznych dotyczących ochrony danych osobowych nie uregulowano kwestii związanych z wykorzystaniem do pracy sprzętu niebędącego własnością Urzędu. (dowód: akta kontroli str. 236)

Konfiguracja sieciowa umożliwiała podłączenie do infrastruktury Urzędu sprzętu (np. laptopów, telefonów, tabletów lub dysków przenośnych) niestanowiącego własności pracodawcy, jednak nie było możliwe korzystanie z zasobów sieci informatycznej Urzędu za ich pomocą. Informacje o podłączeniu do komputerów nośników pamięci były domyślnie zapisywane w logach systemu komputerowego, jednak nie były trwale zabezpieczane. Na dwóch komputerach zainstalowano aplikację pulpitu zdalnego *TeamViewer*, z której korzystali pracownicy firmy zewnętrznej podczas realizacji prac serwisowych. Dostęp ten nie był objęty kontrolą ASI. Problemy te opisano szerzej w dalszej części wystąpienia pokontrolnego, w sekcji „*Ustalone nieprawidłowości*". (dowód: akta kontroli str. 6-10, 230)

1.7. Od 1 stycznia 2016 r. do 13 grudnia 2017 r. nie wystąpiły przypadki wykrycia nieautoryzowanych działań związanych z przetwarzaniem informacji.

(dowód: akta kontroli str. 90-96)

1.8. W Urzędzie użytkowane były dwa komputery przenośne, które nie miały szyfrowanych dysków. Dostęp do ich systemów operacyjnych był zabezpieczony hasłem (lub pinem). Komputery te nie były użytkowane poza siedzibą Urzędu i w procedurach wewnętrznych nie przewidziano zdalnego dostępu użytkowników tych komputerów do zasobów sieci lokalnej. (dowód: akta kontroli str. 6-10, 222-223)

1.9. W umowach Urzędu z podmiotami zewnętrznymi w przedmiocie serwisowania i aktualizacji programów wykorzystywanych do gromadzenia i przetwarzania danych osobowych zawarte były zapisy gwarantujące odpowiedni poziom bezpieczeństwa informacji, co było zgodne z § 20 ust. 2 pkt 10 rozporządzenia KRI. Obejmowały one w szczególności zobowiązanie podmiotów zewnętrznych do: [1] przetwarzania danych osobowych wyłącznie w celu oraz w zakresie związanym z realizacją zawartych umów; [2] zastosowania środków technicznych i organizacyjnych zapewniających ochronę danych, co najmniej w zakresie określonym w art. 36 – 39a ustawy o ochronie danych osobowych; [3] zachowania w tajemnicy informacji uzyskanych w trakcie realizacji umów.

(dowód: akta kontroli str. 118-159)

1.10. 13 (z 18) komputerów wchodzących w skład sieci lokalnej było zabezpieczonych przed działaniem oprogramowania, którego celem byłoby uzyskanie nieuprawnionego dostępu do systemu informatycznego. Zabezpieczenia dokonano dedykowanym do tego celu oprogramowaniem antywirusowym[10]. Pozostałe komputery zabezpieczono oprogramowaniem dostarczonym przez producenta systemu operacyjnego, które – zdaniem biegłego powołanego przez NIK[11] – należy uznać za mniej skuteczne niż aplikacje

[10] Badane komputery posiadały aktualne wersje aplikacji zabezpieczających.
[11] W dziedzinie bezpieczeństwa systemów informatycznych.

dedykowane do tego celu. W trakcie kontroli NIK na pięciu stanowiskach pracy doinstalowane zostało również dedykowane oprogramowanie.

ASI wyjaśnił, że: „*wcześniej (…) uważał, że nie mógł zainstalować programu antywirusowego na wszystkich komputerach, ponieważ przekroczy limit licencji. Po zgłębieniu tematu licencji okazało się, że może jednak to zrobić i program ten po przeprowadzonych przez NIK oględzinach zainstalował na wszystkich komputerach*".

Dostęp do sieci lokalnej kontrolowany był przez firewall[12], zainstalowany na routerze Cisco. Było to zgodne z pkt III załącznika do rozporządzenia w sprawie dokumentacji i warunków technicznych. (dowód: akta kontroli str. 6-10, 222-223, 230-231, 248-249)

1.11. Poczta elektroniczna wykorzystywana przez pracowników do celów służbowych, zakładana była przez każdego z nich samodzielnie, na ogólnie dostępnych domenach komercyjnych, co opisano w dalszej części wystąpienia pokontrolnego, w sekcji „*Ustalone nieprawidłowości*". (dowód: akta kontroli str. 203, 219, 222-223, 230)

1.12. Sposób wykonywania kopii zbiorów danych (nie rzadziej niż raz na tydzień) oraz miejsce ich przechowywania (na stanowiskach pracy) określone zostały w obowiązującej w Urzędzie Instrukcji Zarządzania Systemem Informatycznym. W praktyce, w przypadku dwóch systemów informatycznych kopie zapasowe baz danych wykonywane były na nośnikach zewnętrznych, natomiast w przypadku dwóch innych systemów sporządzane były na komputerach użytkowników[13]. Szerzej problem opisano w dalszej części wystąpienia pokontrolnego, w sekcji „*Ustalone nieprawidłowości*".
(dowód: akta kontroli str. 56-59, 233)

1.13. Pracownicy Urzędu dysponowali możliwością ściągania aplikacji i plików wykonalnych, co szerzej opisano w dalszej części wystąpienia pokontrolnego, w sekcji „*Ustalone nieprawidłowości*". Większość komputerów (16 z 18) objętych było wsparciem producenta. Nie prowadzono odrębnej ewidencji programów zainstalowanych na poszczególnych komputerach Urzędu. (dowód: akta kontroli str. 6-10, 222-223)

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 komputerach służących do obsługi systemu „*Źródło*" – były aktualizowane przez dostawcę oprogramowania, zgodnie z ustalonym harmonogramem.
(dowód: akta kontroli str. 6-10)

1.15. W Urzędzie nie były opracowane regulacje wewnętrzne w zakresie dokonywania płatności drogą elektroniczną. Płatności były dokonywane za pośrednictwem systemu bankowości elektronicznej (*Home Banking*), poprzez stronę internetową banku. Po sprawdzeniu dokumentu pod względem merytorycznym i formalno-rachunkowym oraz zatwierdzeniu go do wypłaty, wyznaczony pracownik sporządzał projekt przelewu, który był następnie zatwierdzany przez osoby uprawnione, z wykorzystaniem narzędzi uwierzytelniających. (dowód: akta kontroli str. 236-237)

Ustalone nieprawidłowości

W działalności kontrolowanej jednostki w przedstawionym wyżej zakresie stwierdzono nieprawidłowości, które wymieniono poniżej.

1. W Urzędzie nie zastosowano odpowiednich środków technicznych, mających za zadanie zapewnienie ochrony przetwarzania danych osobowych, w stopniu wymaganym art. 36 ustawy o ochronie danych osobowych.
   a) Wszyscy pracownicy Urzędu posiadali uprawnienia administratora systemu operacyjnego. W Konsekwencji m.in. dysponowali możliwością ściągania aplikacji i plików wykonalnych oraz posiadali uprawnienia do instalowania ich na stacjach komputerowych, do których mieli dostęp.

[12] Zapora sieciowa chroniąca sieć wewnętrzną jednostki przed dostępem z zewnątrz (np. sieci publicznej, Internetu).
[13] W okresie objętym kontrolą nie wystąpiła konieczność odtworzenia zbioru danych ze sporządzonej kopii bezpieczeństwa.

ASI wyjaśnił, że nie widział potrzeby zakładania kont uwierzytelniających, ponieważ nie miał wcześniej styczności z obsługą informatyczną jednostki samorządu terytorialnego. W trakcie kontroli NIK – 1 grudnia 2017 r. – wszystkim pracownikom Urzędu założono uwierzytelnione konta użytkowników systemu operacyjnego.

(dowód: akta kontroli str. 6-10, 230-231, 248-249)

b) Wszyscy pracownicy Urzędu wykorzystywali do celów służbowych bezpłatną pocztę elektroniczną, założoną na domenach internetowych należących do podmiotów komercyjnych, użytkowaną – w przypadku sześciu pracowników Urzędu – również do celów prywatnych.

ASI wyjaśnił, że nie zdawał sobie sprawy, że taki stan jest nieprawidłowy. Po przeprowadzonych oględzinach wykupił domenę pocztową szudzialowo-gmina.pl i założył wszystkim pracownikom Urzędu konta imienne oraz konta zależne od stanowiska dla wójta, sekretarza, skarbnika, sekretarza i kierownika urzędu stanu cywilnego. Takie konta założył też pracownikom innych jednostek organizacyjnych Gminy, tj. m.in. Szkoły Podstawowej w Szudziałowie, Szkoły Podstawowej w Babikach, Zakładu Gospodarki Komunalnej i Gminnego Ośrodka Pomocy Społecznej.

Wójt Gminy wyjaśnił, że w grudniu 2014 roku, kiedy obejmował urząd Wójta, *„stan był fatalny, jeżeli chodzi o zapewnienie bezpieczeństwa danych. Dziś jest o wiele lepiej, ale zdajemy sobie sprawę, że potrzeba jeszcze wiele pracy z naszej strony*". Dodał, że: „*Po przeprowadzonych przez NIK oględzinach, ASI dokonał już niezbędnych działań, w celu zabezpieczenia danych osobowych przetwarzanych w sieci komputerowej Urzędu*". (dowód: akta kontroli str. 203, 219, 248-252)

c) Dostęp do pomieszczenia serwerowni Urzędu (w dniu przeprowadzenia oględzin) zabezpieczony był jedynie kratą zamykaną na kłódkę, co nie zapewniało odpowiedniego poziomu bezpieczeństwa znajdującym się tam serwerom i innym sprzętom komputerowym, m.in. przed przypadkowym lub umyślnym zalaniem.

ASI wyjaśnił, że „*Drzwi do serwerowni, dlatego nie są zamykane, bo nie ma w tym pomieszczeniu odpowiedniej wentylacji. W przypadku ich stałego zamknięcia uważam, że serwery mogłyby się przegrzać i stracić na wydajności".* Dodał, że: „(…) *do momentu przeprowadzenia remontu lub zakupu klimatyzatora, drzwi do serwerowni będą zamykane, gdyż temperatura na zewnątrz na to pozwala. Pragnę jednak nadmienić, że od 2016 roku poczyniłem wiele starań w celu doprowadzenia pomieszczenia serwerowni jak i serwerów do stanu użyteczności i normalności*".

Wójt Gminy wyjaśnił, że taka forma zamykania serwerowni spowodowana była „(…) *chęcią zapewnienia w serwerowni naturalnego chłodzenia dla lepszej cyrkulacji powietrza*". (dowód: akta kontroli str. 6-10, 230, 248-252)

2. Hasło dostępu do komputerów 14 (z 16) pracowników Urzędu nie spełniało wymogów określonych w § 2 pkt IV.2 Instrukcji Zarządzania Systemami Informatycznymi Urzędu oraz w cz. A pkt IV ust. 2 załącznika do rozporządzenia w sprawie dokumentacji i warunków technicznych dla wysokiego poziomu zabezpieczeń, w odniesieniu do określonej w tych przepisach ilości znaków oraz zmiany hasła.

ASI wyjaśnił, że „*uważał to za stan normalny".*

W trakcie kontroli NIK wszystkim pracownikom założono konta użytkowników z hasłem spełniającym wymogi ww. przepisów. Jak wyjaśnił ASI „*cykliczna zmiana haseł zostanie wdrożona w najbliższych dniach*". (dowód: akta kontroli str. 6-10, 224, 230, 248-252)

3. W Urzędzie nie monitorowano dostępu do przetwarzanych informacji, w celu zapewnienia im ochrony przed kradzieżą, nieuprawnionym dostępem, uszkodzeniami lub zakłóceniami, o których mowa w § 20 ust. 2 pkt 7 lit. a rozporządzenia KRI, ponieważ: [1] nie prowadzono zbiorczego rejestru dostępu do systemu, [2] nie zabezpieczono przed modyfikacją i zniszczeniem logów zapisywanych na komputerach użytkowników, a informacji w nich zawartych nie przetwarzano automatycznie, [3] nie zabezpieczono trwale informacji o podłączeniu do komputerów zewnętrznych nośników pamięci, [4] nie nadzorowano pracowników firmy zewnętrznej

podczas realizacji prac serwisowych przy wykorzystaniu aplikacji pulpitu zdalnego *TeamViewer*[14], zainstalowanej na dwóch komputerach.

ASI wyjaśnił, że: „*Stan techniczny serwerowni nie pozwala na dzień dzisiejszy do skutecznego monitorowania, z uwagi na brak wydzielonego serwera na potrzeby Urzędu".* Dodał, że niezbędna byłaby: „*Przebudowa struktury sieci informatycznej, zakup serwera, stworzenie wewnętrznej domeny urzędu i podłączenie wszystkich stanowisk do domeny oraz zainstalowanie oprogramowania do zarządzania bezpieczeństwem informacji, co z kolei wiąże się ze znacznymi nakładami finansowymi".*

Wójt Gminy wyjaśnił natomiast, że do tej pory nie było możliwości technicznych, aby skutecznie monitorować dostęp do informacji. Dodał, że: „*Gmina nie dysponuje odrębnym serwerem, do którego podpięte byłyby komputery użytkowników. Po oględzinach sprawa ta została przeanalizowana z ASI i Sekretarzem Gminy i ustaliliśmy, że monitorowanie odbywać się będzie na razie bezpośrednio na komputerach użytkowników w formie kontroli doraźnych, natomiast docelowo będziemy starali się w przyszłości wygospodarować środki na zmodernizowanie naszej sieci komputerowej, aby ASI mógł monitorować przepływ danych z poziomu niezależnego serwera*".

W zakresie programu *TeamViewer* ASI wyjaśnił natomiast, że: „*W trakcie oględzin nie miał możliwości nadzoru nad zdalnym dostępem do systemów informatycznych przez ten program*". Dodał, że: „*Na dzień dzisiejszy nadzór sprawowany jest z pozycji konta administratora na stanowisku komputerowym, w którym ww. program jest używany, a użytkownik nie może uruchomić sam oprogramowania do zdalnego dostępu, bo nie ma takich uprawnień*". (dowód: akta kontroli str. 6-10, 230-231, 234, 248-253)

4. Kopie zapasowe baz danych systemów „*Budżet*" i „*Sygnity*" tworzone były niesystematycznie, z częstotliwością od jednego do trzech miesięcy, co było niezgodne z § 2 pkt IV.3 obowiązującej w Urzędzie Instrukcji Zarządzania Systemem Informatycznym, przewidującym, że takie kopie tworzone powinny być „*nie rzadziej niż raz w tygodniu*". Ponadto kopie przechowywane były na komputerach użytkownika, na których były tworzone. ASI nie sprawdzał poprawności ich wykonania, co nie zapewniało odpowiedniego poziomu bezpieczeństwa przechowywanych danych.

   ASI wyjaśnił, że: „*w tym momencie jesteśmy na etapie ustalania harmonogramu częstotliwości tworzenia kopii zapasowych, co w terminie późniejszym chcemy również ująć w procedurze wewnętrznej*". Dodał, że w trakcie kontroli NIK dokonano zmiany sposobu tworzenia kopii zapasowych i są one tworzone raz w tygodniu „(…) *na dysku zewnętrznym, zabezpieczonym hasłem i zaszyfrowanym, przechowywanym w bezpiecznym miejscu w pokoju Pani Sekretarz*".

   Zdaniem NIK, rutynowe kopiowanie plików, programów komputerowych i dokumentów o znaczeniu krytycznym oraz przechowywanie tych kopii w bezpiecznej, zdalnej lokalizacji jest zazwyczaj najbardziej opłacalnym działaniem, jakie jednostka może podjąć w celu ograniczenia przerw w działaniu. Stwarza to możliwości odzyskiwania systemu informacji i jego przywrócenie do stanu pierwotnego.

   (dowód: akta kontroli str. 6-10, 230-233, 248-249)

5. W Urzędzie dopiero w 2017 roku przeprowadzono udokumentowaną, okresową analizę ryzyka utraty integralności, dostępności lub poufności informacji, mimo że obowiązek ten został wprowadzony z dniem 31 maja 2012 r. (§ 20 ust. 2 pkt 3 rozporządzenia KRI).

   Wójt Gminy wyjaśnił, że: „*Od 2015 roku dokonywaliśmy powoli zmiany podejścia do polityki bezpieczeństwa po poprzednikach. W 2017 roku dokonaliśmy już całościowej zmiany polityki bezpieczeństwa i wówczas przeprowadziliśmy analizę integralności, dostępności i poufności informacji*". (dowód: akta kontroli str. 236, 250-252)

   W ocenie NIK, przeprowadzenie analizy dopiero po pięciu latach obowiązywania tego wymogu nie zapewnia rzetelnej wiedzy o występowaniu ww. ryzyk.

[14] Aplikacja umożliwiająca zdalny dostęp do komputerów Urzędu w celu naprawy zainstalowanych na nich programów.

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. W trakcie kontroli NIK rozpoczęto działania naprawcze mające na celu zwiększenie tej skuteczności.

2. Dokumentacja i procedury dotyczące ochrony danych

Opis stanu faktycznego

2.1. Urząd zgłosił do rejestracji do GIODO 16 zbiorów danych osobowych, z których zarejestrowanych zostało 13, w tym m.in: „*Ewidencja ludności i dowody osobiste*", „*Warunki zabudowy i zagospodarowania terenu*", „*Podatki i opłaty lokalne*", „*Rejestracja pojazdów*", „*Zezwolenia na sprzedaż napojów alkoholowych"*, *„Gospodarka nieruchomościami"*, *„Ochrona i kształtowanie środowiska"*, *„Świadczenia rodzinne"*, *„Fundusz alimentacyjny"* i *„Karta dużej rodziny"*. Do dnia zakończenia kontroli nie ujęto w rejestrze prowadzonym przez GIODO[15] zgłoszonych przez Urząd w 2015 roku zbiorów „*Rejestr mieszkańców*" i „*Rejestr cudzoziemców*" oraz zgłoszonego 12 grudnia 2017 r. – w trakcie kontroli NIK – zbioru danych „*Gospodarowanie odpadami komunalnymi*". Urząd nie występował w latach 2016 – 2017 do GIODO o wykreślenie z rejestru zbiorów danych osobowych. Szerzej problem zgłaszania GIODO zbiorów danych do zarejestrowania opisano w dalszej części wystąpienia pokontrolnego, w sekcji „*Ustalone nieprawidłowości*".
(dowód: akta kontroli str. 211, 226, 230, 254)

Zgłoszenia zbiorów danych do rejestracji zawierały wszystkie niezbędne elementy określone w art. 41 ust 1 ustawy o ochronie danych. (dowód: akta kontroli str. 188-202)

2.2. W Urzędzie nie powołano Administratora Bezpieczeństwa Informacji. Jak wyjaśnił Wójt Gminy, wynikało to w głównej mierze z uwagi na konieczność stworzenia nowego etatu, na co Gmina nie ma wystarczających środków finansowych.
(dowód: akta kontroli str. 232, 250-252)

2.3. Wójt Gminy, jako administrator danych osobowych, w latach 2016 – 2017 nadzorował opracowanie i aktualizowanie[16] dokumentacji opisującej sposób przetwarzania danych osobowych oraz środków technicznych i organizacyjnych zapewniających ich ochronę Nieskuteczny był nadzór nad przestrzeganiem zasad w nich określonych, co szerzej opisano w dalszej części wystąpienia pokontrolnego, w sekcji „*Ustalone nieprawidłowości*".
(dowód: akta kontroli str. 11-50, 56-59)

Osoby upoważnione do przetwarzania danych osobowych (oprócz ASI) zostały zapoznane z przepisami o ich ochronie. Nowo zatrudnieni pracownicy byli szkoleni z zakresu ochrony danych osobowych. Szkolenia dotyczyły m.in. obowiązków osób upoważnionych do przetwarzania danych osobowych, odpowiedzialności za naruszenie zasad przetwarzania i ochrony danych osobowych, a także zapoznanie z obowiązującą w Urzędzie dokumentacją z tego zakresu. (dowód: akta kontroli str. 204-208, 218, 248-249)

2.4. W Urzędzie prowadzona była ewidencja osób upoważnionych do przetwarzania danych osobowych, która obejmowała 12 pracowników jednostki. Zawierała ona elementy określone w art. 39 ust. 1 pkt 1-3 ustawy o ochronie danych osobowych, tj. imię i nazwisko osoby upoważnionej, datę nadania i ustania upoważnienia do przetwarzania danych osobowych oraz jego zakres, a także identyfikatory użytkowników w systemie informatycznym. (dowód: akta kontroli str. 46-48)

Zakres upoważnień Wójta Gminy i pracowników Urzędu do przetwarzania danych w systemach informatycznych był zgodny z realizowanymi przez nich zadaniami.
(dowód: akta kontroli str. 177-180, 229, 237-238)

2.5. W Urzędzie nie opracowywano procedur wewnętrznych dotyczących ochrony danych osobowych, poza polityką bezpieczeństwa informacji, instrukcją zarządzania systemami informatycznymi i procedurą alarmową, które opisane zostały w dalszej części, w pkt. 2.10 i 3.7 wystąpienia pokontrolnego. (dowód: akta kontroli str. 236)

[15] Dostępnym na stronie internetowej *www.egiodo.gov.pl*.
[16] Politykę bezpieczeństwa informacji i instrukcję zarządzania systemem informatycznym zaktualizowano 30 stycznia 2017 r.

2.6. Na stanowisko ASI powołano[17] przedstawiciela firmy zewnętrznej. ASI zobowiązany był m.in. do: [1] administrowania serwerem i siecią Urzędu; [2] przestrzegania procedur operacyjnych i bezpieczeństwa opracowanych dla systemu; [3] regularnego tworzenia i sprawdzania poprawności wykonania kopii zapasowych zasobów danych osobowych; [4] zastosowania wysokiego poziomu zabezpieczeń systemów służących do przetwarzania danych osobowych; [5] zastosowania odpowiednich środków technicznych i organizacyjnych zapewniających ochronę przetwarzania danych osobowych. ASI nie wywiązał się jednak ze swoich obowiązków, co opisano w dalszej części wystąpienia pokontrolnego, w sekcji „*Ustalone nieprawidłowości*". (dowód: akta kontroli str. 97-115, 235)

2.7. Pierwszy audyt z zakresu bezpieczeństwa informacji przeprowadzono dopiero 30 stycznia 2017 r., co szerzej opisano w dalszej części wystąpienia pokontrolnego, w sekcji „*Ustalone nieprawidłowości*". W raporcie z audytu określono potrzebę przeprowadzenia okresowej kontroli placówki pod kątem ochrony danych osobowych oraz weryfikacji zabezpieczeń fizycznych i programowych w pomieszczeniach, w których przetwarzano dane osobowe. Do dnia zakończenia kontroli NIK taka kontrola nie została przeprowadzona. Wójt Gminy wyjaśnił, że: „(…) *kontrola planowana była na styczeń 2018 roku przed koniecznością sporządzenia corocznego audytu, aby na bieżąco być z problemami, które zostałyby ujawnione w toku naszej wewnętrznej kontroli*".
(dowód: akta kontroli str. 82-83, 253)

2.8. W latach 2016 – 2017 trzech (z 16) pracowników Urzędu zaangażowanych w proces przetwarzania informacji brało udział w szkoleniach z zakresu ochrony danych osobowych, które obejmowały m.in.: podstawy prawne ochrony danych osobowych, zabezpieczenie danych, dokumentację przetwarzania danych oraz planowane zmiany w zakresie ochrony danych osobowych. Szerzej problem szkoleń z tematyki ochrony danych osobowych opisano w dalszej części wystąpienia pokontrolnego, w sekcji „*Ustalone nieprawidłowości*".
(dowód: akta kontroli str. 204-208, 227-228)

2.9. W okresie objętym kontrolą w Urzędzie nie były przeprowadzane zewnętrzne kontrole w zakresie bezpieczeństwa danych osobowych. Nie wpływały do Urzędu również skargi związane z nieuprawnionymi przypadkami ujawnienia danych osobowych.
(dowód: akta kontroli str. 232)

2.10. W Urzędzie opracowano i wdrożono[18] dokumentację związaną z przetwarzaniem danych osobowych, tj. Politykę Bezpieczeństwa Informacji oraz Instrukcję Zarządzania Systemem Informatycznym, które zawierały elementy określone w §§ 4 i 5 rozporządzenia w sprawie dokumentacji i warunków technicznych. Na dzień kontroli nie wymagały one aktualizacji. (dowód: akta kontroli str. 11-80, 236)

W Instrukcji Zarządzania Systemem Informatycznym wprowadzony został wysoki poziom bezpieczeństwa (17 z 18 komputerów, na których przetwarzano dane osobowe było połączonych z siecią publiczną[19]), co odpowiadało wymaganiom określonym w § 6 rozporządzenia w sprawie dokumentacji i warunków technicznych. Ponadto określono sposób uwierzytelnienia użytkowników (hasło o odpowiedniej złożoności, z ustaloną okresową jego zmianą). Postanowienia Instrukcji nie były jednak realizowane, co opisano szerzej w pkt 1 wystąpienia pokontrolnego, w sekcji „*Ustalone nieprawidłowości*".
(dowód: akta kontroli str. 56-59)

Ustalone nieprawidłowości

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

1. Urząd nie zgłosił GIODO do zarejestrowania trzech zbiorów danych osobowych przetwarzanych w Urzędzie, które dotyczyły: gospodarowania odpadami komunalnymi, oświadczeń majątkowych radnych i pracowników Urzędu oraz prac Gminnej Komisji

[17] Umowy z 1 kwietnia 2015 r. i 1 kwietnia 2016 r.
[18] Zarządzeniami Wójta Gminy z 30 czerwca 2015 r. i 31 stycznia 2017 r. w sprawie wprowadzenia polityki bezpieczeństwa oraz przyjęcia instrukcji zarządzania systemem informatycznym.
[19] Poza stanowiskami wydzielonymi do obsługi Systemu Rejestrów Państwowych.

Rozwiązywania Problemów Alkoholowych[20], co stanowiło naruszenie art. 40 ustawy o ochronie danych osobowych. (dowód: akta kontroli str. 209-210, 226)

Jak wyjaśnił Wójt Gminy *„(…) taka sytuacja wynikała z przeoczenia. Wniosek o zgłoszenie zbioru dotyczącego gospodarowania odpadami, tj. rejestr składanych przez mieszkańców deklaracji został w trakcie kontroli wysłany do GIODO, a pozostałe zgłosimy i zaktualizujemy wkrótce*". (dowód: akta kontroli str. 250-252)

2. Do 31 stycznia 2017 r. w Urzędzie nie przeprowadzano audytu wewnętrznego w zakresie bezpieczeństwa informacji, co było niezgodne z przepisem § 20 ust. 2 pkt 14 rozporządzenia KRI, w myśl którego bezpieczeństwo informacji realizowane jest m.in. poprzez zapewnienie przeprowadzenia audytu bezpieczeństwa, nie rzadziej niż raz na rok. Tymczasem pierwszy taki audyt przeprowadzony został w Urzędzie 31 stycznia 2017 r., mimo obowiązywania rozporządzenia KRI od 31 maja 2012 r.

   Wójt Gminy wyjaśnił, że audyt wewnętrzny w zakresie bezpieczeństwa informacji przeprowadzono po dokonaniu całościowej zmiany wewnętrznych procedur, co miało miejsce w styczniu 2017 roku. (dowód: akta kontroli str. 82-83, 236, 250-252)

3. Wójt Gminy nie wyegzekwował od ASI realizacji obowiązków wynikających z zawieranych – pomiędzy Urzędem a ASI – umów w zakresie: [1] przestrzegania procedur operacyjnych i bezpieczeństwa opracowanych dla systemu; [2] regularnego tworzenia i sprawdzania poprawności wykonania kopii zapasowych zasobów danych osobowych; [3] zastosowania wysokiego poziomu zabezpieczeń systemów służących do przetwarzania danych osobowych; [4] zastosowania odpowiednich środków technicznych i organizacyjnych zapewniających ochronę przetwarzania danych osobowych. Oględziny systemów informatycznych wykazały nierealizowanie tych obowiązków, co szerzej opisane zostało w pkt 1 wystąpienia pokontrolnego, w sekcji „*Ustalone nieprawidłowości*".

   Wójt Gminy wyjaśnił, że nie kontrolował zgodności pracy ASI z zapisami umowy. Dodał, że ASI bardzo pomógł w zapewnieniu sprawnej obsługi informatycznej Urzędu.

   Zdaniem NIK, przyczyną nierealizowania przez ASI obowiązków wynikających z umowy z Urzędem mógł być fakt niezapoznania się ASI z Polityką Bezpieczeństwa Informacji i Instrukcją Zarządzania Systemem Informatycznymi przez ponad 10 miesięcy ich obowiązywania w Urzędzie (od 31 stycznia do 12 grudnia 2017 r. [21]). ASI wyjaśnił, że nie zapoznał się z wewnętrznymi regulacjami dotyczącymi bezpieczeństwa informacji ponieważ *„(…) nie miał na to czasu i robił to co było niezbędne i wskazane przez pracowników Urzędu*". Niezapoznanie ASI z przepisami o ochronie danych osobowych oraz nienadzorowanie przestrzegania przez niego zasad określonych w procedurach wewnętrznych dotyczących bezpieczeństwa informacji skutkowało naruszeniem art. 36a ust. 2 pkt 1 lit. b i c ustawy o ochronie danych osobowych.

   W latach 2016 – 2017, w związku z umową z ASI Urząd poniósł koszt w wysokości 33,3 tys. zł. (dowód: akta kontroli str. 97-115, 185-187, 218, 230, 235, 248-252)

4. W Urzędzie nie przeprowadzono dla 13 (z 16) pracowników zaangażowanych w proces przetwarzania informacji szkoleń uwzględniających tematykę zagrożenia bezpieczeństwa informacji, skutki naruszenia zasad informacji (w tym odpowiedzialność prawna) oraz stosowanie środków zabezpieczających bezpieczeństwo informacji (w tym

[20] Dane w niezgłoszonych GIODO do zarejestrowania zbiorach przetwarzane były w Urzędzie w związku z niezbędnymi do realizacji uprawnieniami, wynikającymi z następujących ustaw: [1] w przypadku zbioru „*gospodarowanie odpadami komunalnymi*" – dane przetwarzano od 1 stycznia 1997 r. w związku z wejściem w życie ustawy z dnia 13 września 1996 r. o utrzymaniu czystości i porządku w gminach (Dz. U. z 2017 r., poz. 1289); [2] w przypadku zbiorów „*oświadczenia majątkowe radnych"* i „*oświadczenia majątkowe pracowników Urzędu*" – dane przetwarzano odpowiednio od 1 stycznia 1998 r. i 1 stycznia 2003 r. w związku ze zmianami art. 24h ustawy z dnia 8 marca 1990 r. o samorządzie gminnym (Dz. U. z 2017 r., poz. 1875); [3] w przypadku zbioru „*prace Gminnej Komisji Rozwiązywania Problemów Alkoholowych*" (w którym przetwarzane były dane wrażliwe dotyczące stanu zdrowia osób z problemem alkoholowym) – dane przetwarzano od 13 maja 1983 r. – w związku z wejściem w życie ustawy z dnia 26 października 1982 r. o wychowaniu w trzeźwości i przeciwdziałania alkoholizmowi (Dz. U. z 2016 r. poz. 487). Obowiązek zgłoszenia GIODO zbiorów danych do rejestracji funkcjonuje od 30 kwietnia 1998 r.

[21] Tego dnia, tj. w trakcie kontroli NIK, ASI zapoznał się z wewnętrznymi regulacjami Urzędu dotyczącymi bezpieczeństwa informacji.

urządzenia i oprogramowanie minimalizujące ryzyko błędów ludzkich). Stanowiło to naruszenie § 20 ust. 2 pkt 6 rozporządzenia KRI.

Wójt Gminy wyjaśnił, że: „*Do tej pory szkoleni byli Ci pracownicy, którzy mieli najwięcej do czynienia z przetwarzaniem danych osobowych, ale niebawem planowane jest takie szkolenie zorganizowane dla wszystkich pracowników Urzędu".*

(dowód: akta kontroli str. 204-208, 227-228, 250-252)

Ocena cząstkowa

Najwyższa Izba Kontroli ocenia negatywnie opracowanie i wdrożenie dokumentacji oraz procedur ochrony danych i zgłaszanie rejestracji zbiorów do GIODO.

3. Sposób przechowywania oraz zabezpieczenia danych

Opis stanu faktycznego

3.1. W załączniku do PBI „*Wykaz pomieszczeń, w których przetwarzane są dane osobowe*" określony został sposób ich zabezpieczenia, poprzez określenie szczególnego rodzaju zabezpieczeń, który był zgodny z rzeczywistym (z jednym wyjątkiem – w trakcie kontroli NIK zaktualizowano ww. załącznik).

W Urzędzie od 2017 roku wprowadzona została „*polityka kluczy*", która określała podstawowe zasady postępowania z kluczami do pomieszczeń Urzędu, w których przetwarzane były dane osobowe. (dowód: akta kontroli str. 11-55, 116-117)

3.2. W Urzędzie nie prowadzono rejestru zasobów informatycznych, co szerzej opisano w dalszej części wystąpienia pokontrolnego, w sekcji „*Ustalone nieprawidłowości*".

(dowód: akta kontroli str. 236)

3.3. W okresie objętym kontrolą w Urzędzie nie dokonywano likwidacji lub naprawy sprzętu będącego nośnikiem danych. (dowód: akta kontroli str. 232)

3.4. W Urzędzie niszczenie dokumentów odbywało się za pomocą niszczarek, co było zgodne z regulacjami wewnętrznymi. Urząd nie korzystał z usług firm zewnętrznych w tym zakresie. (dowód: akta kontroli str. 11-50)

3.5. W Urzędzie nie określono zasad użytkowania komputerów przenośnych. Wójt Gminy i Sekretarz użytkujący takie komputery nie korzystali z nich poza siedzibą jednostki. Pracownikom tym nie umożliwiono również zdalnego dostępu do zasobów sieci lokalnej Urzędu, co – jak wyjaśnił Wójt Gminy – „*nie jest to im niezbędne do wykonywania obowiązków i nie planuje się w tym względzie żadnych zmian*".

(dowód: akta kontroli str. 222-223, 250-252)

3.6. Sprzątanie pomieszczeń, w których przetwarzano dane osobowe odbywało się we wszystkie dni pracy Urzędu, od godziny 7^{00} do 9^{00} i od 14^{00} do 20^{00}, tj. również poza godzinami pracy Urzędu[22]. Osoba sprzątająca uzyskała zgodę Wójta Gminy, tj. Administratora Danych Osobowych do przebywania w obszarze przetwarzania danych poza godzinami pracy Urzędu. Sprzątanie pomieszczenia serwerowni odbywało się pod nadzorem ASI. (dowód: akta kontroli str. 229, 247)

Zgodnie z przyjętymi w Urzędzie uregulowaniami, dokumenty zawierające dane osobowe były przechowywane w szafach zamykanych na klucz. Za prawidłowe zabezpieczenie danych osobowych oraz miejsc ich przechowywania odpowiedzialni byli kierownicy komórek organizacyjnych Urzędu. (dowód: akta kontroli str. 116-117, 240-241)

3.7. W obowiązujących w Urzędzie: Instrukcji Zarządzania Systemem Informatycznym, Analizie poufności, integralności i rozliczalności systemów informatycznych pod kątem zagrożeń i ryzyka oraz w Procedurze alarmowej[23] były instrukcje wykonywania przeglądów i konserwacji systemów oraz nośników informacji służących do przetwarzania danych (określono m.in. zakres i metodę przeprowadzenia kontroli) oraz procedury postępowania w przypadku uchybienia lub zagrożenia[24]. Przeglądy i konserwacje – zgodnie z wyjaśnieniem Wójta i ASI – były wykonywane na bieżąco.

(dowód: akta kontroli str. 11-50, 90-93, 248-252)

[22] Urząd był otwarty od poniedziałku do piątku, w godzinach 7^{30} – 15^{30}.

[23] Powołanej 31 stycznia 2017 r. jako uzupełnienie do Polityki bezpieczeństwa Urzędu.

[24] Do dnia zakończenia czynności kontrolnych nie stwierdzono w Urzędzie żadnych uchybień lub zagrożeń.

3.8. Wszystkie komputery wykorzystywane przez pracowników Urzędu i serwery w pomieszczeniu serwerowni zostały zabezpieczone przed utratą zasilania, za pomocą zasilaczy awaryjnych UPS. W Urzędzie nie opracowano natomiast rozwiązań na wypadek wystąpienia sytuacji nadzwyczajnych, np. awarii, długotrwałego braku zasilania, procedur dotyczących przywracania systemów po awarii oraz planu ciągłości działania umożliwiającego kontynuację wykonywania zadań publicznych, co szerzej opisane zostało w dalszej części wystąpienia pokontrolnego w sekcji „*Uwagi dotyczące badanej działalności*". Urząd nie posiadał dodatkowego źródła zasilania na wypadek długotrwałych przerw w dostawie prądu. (dowód: akta kontroli str. 6-10, 222-223)

3.9. W Urzędzie od 1 stycznia 2016 r. do 13 grudnia 2017 r. nie wystąpiły przypadki fizycznej utraty danych. (dowód: akta kontroli str. 232)

Ustalone nieprawidłowości

W działalności jednostki w przedstawionym wyżej zakresie stwierdzono nieprawidłowość, polegającą na nieprowadzeniu w Urzędzie, wbrew wymogom § 20 ust. 2 pkt 2 rozporządzenia KRI, rejestru zasobów informatycznych, który określałby m.in rodzaj oprogramowania służącego do przetwarzania danych.

Wójt Gminy wyjaśnił, że: „*uważał, że księga inwentarzowa, w której prowadzone są dane dotyczące komputerów była wystarczająca*" Dodał, że: „*uzupełni rejestr o wszystkie dane wskazane w rozporządzeniu*". (dowód: akta kontroli str. 236, 250-252)

Uwagi dotyczące badanej działalności

NIK zwraca uwagę, że w Urzędzie nie opracowano, wewnętrznych regulacji dotyczących rozwiązań na wypadek wystąpienia sytuacji nadzwyczajnych, np.: długotrwałego braku zasilania bądź przywracania systemów po awarii, a także planu ciągłości działania umożliwiającego kontynuację wykonywania zadań jednostki. Plan ten powinien określić systemy i aplikacje o znaczeniu krytycznym oraz wszystkie podporządkowane lub powiązane plany. Istotne jest, aby plany te były jasno udokumentowane, przekazane pracownikom i aktualizowane w celu odzwierciedlenia bieżącej działalności Urzędu. Obowiązek zabezpieczenia systemu informatycznego służącego do przetwarzania danych osobowych przed utratą danych spowodowaną awarią zasilania lub zakłóceniami w sieci zasilającej wynika z regulacji rozdziału A pkt III załącznika do rozporządzenia w sprawie dokumentacji i warunków technicznych. (dowód: akta kontroli str. 232)

Ocena cząstkowa

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

4. Przetwarzanie zasobów informacyjnych zgodnych z zakresem działalności jednostki kontrolowanej

Opis stanu faktycznego

4.1. Wójt Gminy prowadził rejestr danych osobowych, który zawierał nazwy 63 zbiorów[25] oraz informacje o systemach informatycznych zastosowanych do przetwarzania danych osobowych. Spośród wskazanych zbiorów, 51 prowadzonych było w formie papierowej, a 12 w formie elektronicznej. (dowód: akta kontroli str. 41-45, 226)

4.2. W okresie objętym kontrolą nie dokonywano aktualizacji zbiorów danych zgłoszonych do GIODO. W 14 (z 16) zbiorach zakres przetwarzanych danych był zgodny z danymi wskazanymi w zgłoszeniach do GIODO, a w dwóch przetwarzano dane w szerszym zakresie niż zgłoszono, co szerzej opisano w dalszej części wystąpienia pokontrolnego, w sekcji „*Ustalone nieprawidłowości*". (dowód: akta kontroli str. 41-45, 226)

4.2. We wszystkich zbiorach danych prowadzonych w Urzędzie zakres gromadzonych i przetwarzanych danych osobowych był niezbędny do realizacji zadań Urzędu. (dowód: akta kontroli str. 226)

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. 247)

[25] 47 zbiorów stanowiło uszczegółowienie 16 zbiorów zgłoszonych do GIODO lub dane pracowników, które nie podlegały zgłoszeniu do GIODO.

4.4. Urząd posiadał dostęp do trzech zewnętrznych systemów informatycznych zawierających zbiory danych osobowych, tj. Źródło, Sepi i EWOPIS. Spełniono wymagania dostępu do tych systemów, poprzez uzyskanie odpowiednich upoważnień (Źródło[26]) lub zgłoszeń (Sepi, EWOPIS). (dowód: akta kontroli str. 181-184)

Ustalone nieprawidłowości

W działalności kontrolowanej jednostki w przedstawionym wyżej zakresie stwierdzono nieprawidłowość, polegającą na niezaktualizowaniu zgłoszonego do GIODO zakresu przewarzania danych w dwóch (z 16) zbiorów danych, co stanowiło naruszenie art. 41 ust. 1 pkt 3a i ust. 2 ustawy o ochronie danych osobowych. Przetwarzane przez pracowników Urzędu dane obejmowały (oprócz danych zgłoszonych do rejestracji) także serię i nr dowodu osobistego, datę i miejsce urodzenia (w przypadku zbioru „*Opłaty i podatki lokalne*") oraz miejsce pracy (w przypadku zbioru „*Świadczenia rodzinne*"). Zgodnie z art. 41 ust. 2 ww. ustawy, zmiana w zbiorze danych powinna być zgłoszona w terminie 30 dni od dnia jej dokonania.

Wójt Gminy wyjaśnił, że: *„(…) taki stan wynikał z przeoczenia*". Dodał, że: „*(…) w najbliższym czasie poproszę pracowników o analizę danych zgłoszonych do GIODO i zbiorczo dokonamy aktualizacji zamieszczonych danych o rodzaju przetwarzanych informacji w rejestrach zgłoszonych do GIODO*".

(dowód: akta kontroli str. 226, 250-252)

Ocena cząstkowa

Najwyższa Izba Kontroli ocenia pozytywnie mimo stwierdzonej nieprawidłowości sposób przetwarzania zasobów informacyjnych, który był zgodny z zakresem działalności Urzędu.

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[27] wnosi o:

1. Wyegzekwowanie od Administratora Systemu Informatycznego realizacji obowiązków wynikających z umowy na świadczenie usług informatycznych.
2. Zapewnienie odpowiednich środków technicznych, mających za zadanie odpowiednią ochronę przetwarzania danych osobowych, stosownie do wymogów art. 36 ustawy o ochronie danych osobowych , ze szczególnym uwzględnieniem odpowiedniego zabezpieczenia dostępu do pomieszczenia serwerowni.
3. Zapewnienie zmiany – nie rzadziej niż co 30 dni – haseł dostępu do systemów operacyjnych, stosownie do § 2 pkt IV.2 Instrukcji Zarządzania Systemem Informatycznym.
4. Sporządzanie kopii zapasowych baz danych zgodnie z § 2 pkt IV.3 Instrukcji Zarządzania Systemem Informatycznym oraz sprawdzanie poprawności ich wykonania.
5. Przeprowadzanie okresowych analiz ryzyka utraty integralności, dostępności lub poufności informacji oraz – nie rzadziej niż raz w roku – okresowego audytu bezpieczeństwa informacji.
6. Prowadzenie rejestru zasobów informatycznych zgodnie z wymogami określonymi w § 20 ust. 2 pkt 2 rozporządzenia KRI.
7. Zapewnienie skutecznego monitorowania dostępu do zasobów informacyjnych Urzędu.
8. Zaktualizowanie lub zgłoszenie do GIODO wszystkich zbiorów danych przetwarzanych w Urzędzie.
9. Zorganizowanie pracownikom zaangażowanym w proces przetwarzania informacji szkolenia uwzględniającego zakres określony w § 20 ust. 2 pkt 6 rozporządzenia KRI.

[26] Użytkownicy korzystający z tego systemu informatycznego nie mieli dostępu do Internetu.
[27] Dz. U. z 2017 r. poz. 524. Ustawa zwana dalej „*ustawą o NIK*".

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 19 stycznia 2018 r.

Kontroler Mariusz Lenkiewicz starszy inspektor kontroli państwowej	DYREKTOR DELEGATURY Najwyższej Izby Kontroli w Białymstoku z up. WICEDYREKTOR Robert Skwarko
..... *podpis*	..... *podpis*