NAJWYŻSZA IZBA KONTROLI
Delegatura w Białymstoku

LBI.410.023.17.2017
P/17/062

02269617

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	Marek Zapolski – doradca ekonomiczny, upoważnienie do kontroli nr LBI/173/2017 z 30 listopada 2017 r. (dowód: akta kontroli str. 1-2)
Jednostka kontrolowana	Miejsko-Gminny Ośrodek Pomocy Społecznej w Czarnej Białostockiej, 16-020 Czarna Białostocka, ul. Torowa 9 (dalej: „M-GOPS" lub „Ośrodek")
Kierownik jednostki kontrolowanej	Agnieszka Dyda – dyrektor Ośrodka[1] (dowód: akta kontroli str. 3)

II. Ocena kontrolowanej działalności[2]

Ocena ogólna

Najwyższa Izba Kontroli ocenia negatywnie zapewnienie przez M-GOPS[3] właściwej ochrony elektronicznych zasobów informacyjnych przed nieuprawnionym dostępem, przejęciem lub zniszczeniem.

Uzasadnienie oceny ogólnej

Stwierdzono bowiem nieprawidłowości, polegające w szczególności na:

- nadaniu wszystkim użytkownikom komputerów uprawnień administratora w systemie operacyjnym tych urządzeń,
- niezapewnieniu właściwego bezpieczeństwa tworzonym kopiom zapasowym baz danych systemów dziedzinowych Ośrodka,
- nieanalizowaniu i niezabezpieczeniu przed modyfikacją lub zniszczeniem logów systemów operacyjnych komputerów,
- niewywiązaniu się z obowiązków dotyczących utrzymywania aktualności inwentaryzacji sprzętu i oprogramowania służącego do przetwarzania informacji obejmującej ich rodzaj i konfigurację oraz przeprowadzania corocznych audytów wewnętrznych z zakresu bezpieczeństwa informacji,
- niedopełnieniu obowiązku zgłoszenia do rejestru prowadzonego przez GIODO[4] trzech przetwarzanych w Ośrodku zbiorów danych osobowych[5],
- posiadaniu dokumentacji opisującej sposób przetwarzania danych osobowych, która nie zawierała wszystkich elementów określonych w § 4 pkt 3 – 4 oraz § 5 pkt 1 4 – 5 i 8 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].

---

1 Od 30 grudnia 2006 r.
2 Najwyższa Izba Kontroli stosuje 3-stopniową skalę ocen: pozytywna, pozytywna mimo stwierdzonych nieprawidłowości, negatywna.
3 Kontrolą objęty został okres od 1 stycznia 2016 r. do zakończenia czynności kontrolnych.
4 Generalnego Inspektora Ochrony Danych Osobowych (dalej: „GIODO").
5 „Ryczałty energetyczne", „Świadczenia za życiem", „Wspieranie rodziny i pieczy zastępczej".
6 Dz. U. Nr 100, poz. 1024. Rozporządzenie zwane dalej rozporządzeniem MSWiA.

III. Opis ustalonego stanu faktycznego

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

Opis stanu faktycznego

1.1. Ośrodek wyposażony był w 11 stacjonarnych zestawów komputerowych oraz jeden laptop, połączonych w sieć, bez wydzielonego serwera odpowiedzialnego za zarządzenie siecią i współdzielenie zasobów. Komputery wchodzące w skład sieci działały na systemie operacyjnym MS Windows – dwa na niewspieranej już przez producenta wersji XP (wsparcie ustało 8 kwietnia 2014 r.), pozostałe dziesięć na wersji 7. Do gromadzenia i przetwarzania danych wykorzystywano dziewięć systemów, z tego sześć[7] firmy INFO-R Spółka Jawna Kuc Urszula, Kuc Rafał. Ponadto Ośrodek korzysta z Samorządowej Elektronicznej Platformy Informacyjnej (dalej SEPI), systemu QNT do prowadzenia pełnej obsługi księgowości oraz spraw kadrowo-płacowych, systemu PŁATNIK służącego do zgłaszania, wyrejestrowania osób z ubezpieczenia zdrowotnego i społecznego ZUS, systemu SMATDOC wykorzystywanego do wspomagania i rejestrowania obiegu dokumentów. Ośrodek korzysta też z platformy EMP@TIA, za pośrednictwem której posiada dostęp do zewnętrznych systemów takich, jak: Pesel, E-Podatki, ZUS, AC Rynek Pracy, Eksmoon, NFZ-CWU, CEIDG, CBB, Centralna Aplikacja Statystyczna.

(dowód: akta kontroli str. 19-22)

Oględziny zestawów komputerowych wykazały, że:

- dostęp do systemu operacyjnego możliwy był jedynie po zalogowaniu się i wprowadzenia przez użytkownika hasła o złożoności odpowiadającej wymaganiom rozporządzenia MSWiA dla danego poziomu bezpieczeństwa,
- każdy użytkownik komputera posiadał uprawnienia administratora systemu operacyjnego,
- systemy operacyjne w poszczególnych komputerach były zabezpieczone hasłem, lecz nie była wymuszona okresowa ich zmiana,
- w systemach dziedzinowych istniała konieczność zmiany hasła co miesiąc,
- na wszystkich urządzeniach zainstalowano i na bieżąco aktualizowano program antywirusowy,
- tylko na jednym spośród sześciu komputerów nie było uaktywnionej funkcji wygaszacza ekranu, który na pozostałych uruchamiał się od dwóch do 10 minut po zaprzestaniu używania urządzeń; ponowne uruchomienie systemu wymagało podania loginu i hasła użytkownika,
- na żadnym z komputerów nie stwierdzono oprogramowania służącego do monitorowania ich pracy i ruchu sieciowego,
- na żadnym komputerze dane zgromadzone na dysku twardym nie były szyfrowane,
- nie prowadzono rejestru dostępu do poszczególnych zestawów komputerowych,
- wszystkie stanowiska komputerowe przetwarzające dane osobowe posiadały dostęp do poczty elektronicznej za pośrednictwem operatorów komercyjnych i otwartego Internetu,
- aktualizację systemów dziedzinowych samodzielnie wykonywał użytkownik, korzystając ze strony internetowej producenta oprogramowania. (dowód: akta kontroli str. 4-18)

1.2. Według stanu na 4 grudnia 2017 r. w Ośrodku zatrudnionych było 24 pracowników, w tym: dyrektor, siedmiu pracowników socjalnych (w tym jeden na urlopie macierzyńskim), jeden asystent rodziny, dziewięciu opiekunów, pięciu pracowników administracyjnych (w tym główna księgową), jeden pracownik gospodarczy. Administratorem danych osobowych był dyrektor Ośrodka (dalej „ADO"). W M-GOPS nie powołano administratora bezpieczeństwa informacji (dalej „ABI") oraz administratora systemów informatycznych (dalej „ASI"). Kwestie dotyczące ABI i ASI opisano szerzej w punkcie 2.2 i 2.3 wystąpienia.

(dowód: akta kontroli str. 34-40)

---

[7] NEMEZIS, IZYDA, CHEOPS, AMAZIS, TALES, HELIOS.

1.3. Spośród 24 pracowników zatrudnionych w Ośrodku, uprawnienia do przetwarzania informacji w systemach nadano 12 osobom oraz siedmiu pracownikom zewnętrznym, zatrudnianym w Powiatowym Urzędzie Pracy w Białymstoku (dalej: „PUP w Białymstoku"), co opisano w punkcie 2.4 wystąpienia. Przyjęte w lutym 2017 roku, Polityka Bezpieczeństwa[8] (dalej „PB") i „Instrukcja zarządzania systemem informatycznym służącym do przetwarzania danych osobowych Miejsko-Gminnego Ośrodka Pomocy Społecznej w Czarnej Białostockiej[9]" (dalej „Instrukcja zarządzania systemem informatycznym (...)"), nie określały zasad nadania, zawieszenia, cofnięcia lub wygaszenia uprawnień do przetwarzania danych. Spośród 12 pracowników, którym nadano uprawnienia dostępowe do systemów informatycznych, czterech nie posiadało zaświadczenia potwierdzającego odbycie szkolenia z zakresu ochrony danych osobowych. Kwestie z tym związane opisano w dalszej części wystąpienia, w sekcji „Ustalone nieprawidłowości". Każdy pracownik przetwarzający informacje posiadał własny login i hasło do systemu operacyjnego jednostek komputerowych i dostępnych w nich systemów dziedzinowych. Hasło to posiadało odpowiednią złożoność. W okresie objętym kontrolą nie zachodziły okoliczności związane z ruchem kadrowym i zmianą stanowiska pracy, które wymagałyby dokonania zmiany uprawnień użytkowników w systemach informatycznych. Nie stwierdzono też przypadków użytkowania jednego konta przez kilku użytkowników.

(dowód: akta kontroli str. 163-175, 302-322, 328-329)

1.4. W okresie objętym kontrolą nie prowadzono rejestru dostępu do systemów. Logi systemowe na dyskach lokalnych gromadzono domyślnie na każdym z komputerów (w postaci rejestru zdarzeń systemu Windows). Według opinii biegłego, powołanego na podstawie art. 49 ust. 1 i 2 ustawy z dnia 23 grudnia 1994 r. o Najwyższej Izbie Kontroli[10] (dalej „ustawa o NIK"), logi te nie były zabezpieczone, co szerzej zostało opisane w dalszej części wystąpienia pokontrolnego, w sekcji „Ustalone nieprawidłowości".

(dowód: akta kontroli str. 23-24, 31-33)

1.5. Środkiem zabezpieczającym przed nieautoryzowanym dostępem do wszystkich systemów operacyjnych komputerów było hasło użytkownika, przy czym nie była wymuszana jego okresowa zmiana co 30 dni. Aplikacje dziedzinowe wykorzystywane w M-GOPS wymuszały zmianę hasła dostępowego co 30 dni. W ramach sieci LAN Ośrodka nie działała sieć WI-FI. Urządzenia sieciowe były zabezpieczone przed fizyczną ingerencją osób do tego nieupoważnionych z racji umieszczenia ich w przeznaczonej do tego serwerowni Urzędu Miejskiego w Czarnej Białostockiej. (dowód: akta kontroli str. 31-33)

1.6. W § 3 pkt 5 Instrukcji Zarządzania systemem informatycznym (...) wskazano, że użytkownikom nie wolno korzystać z prywatnego sprzętu informatycznego, w tym oprogramowania oraz nośników pamięci. Według opinii biegłego: *„Konfiguracja sieciowa umożliwia podłączenie do infrastruktury jednostki sprzęt (laptopy, telefony, tablety) niestanowiący własności pracodawcy. Informacje o podłączeniu do komputerów nośników pamięci np. pendrive lub dysk przenośny, są domyślnie zapisywane w logach systemu komputerowego. Router, na którym zbudowana jest sieć LAN, gromadzi w logach informacje o urządzeniach jakie były podłączane do sieci. Dane o podłączeniu do poszczególnych komputerów, nośników pamięci np. pendrive lub dysk przenośny, są gromadzone w logach ich systemów operacyjnych".* (dowód: akta kontroli str. 31-33, 221)

1.7. Z wyjaśnień dyrektora Ośrodka wynika, że w latach 2016 – 2017 (do 22 grudnia) w M-GOPS nie odnotowano działań związanych z nieautoryzowanym przetwarzaniem informacji, tj. przypadków naruszenia bezpieczeństwa systemu informatycznego lub utraty integralności, dostępności lub poufności informacji. (dowód: akta kontroli str. 45)

1.8. Według opinii biegłego: *„W badanej jednostce nie przewidziano zdalnego dostępu do zasobów sieci lokalnej i taki dostęp nie funkcjonował".* Od 23 grudnia 2013 r. w Ośrodku nie wykorzystywano dwóch terminali mobilnych, użyczonych przez Ministerstwo Pracy i Polityki Socjalnej do rejestracji danych opisujących sytuację rodziny w trakcie wywiadu środowiskowego w ramach projektu EMP@TIA. (dowód: akta kontroli str. 31-33, 287-289)

---

[8] Zarządzenia nr 1/2017 dyrektora Ośrodka w sprawie wprowadzenia Polityki Bezpieczeństwa przetwarzania danych.
[9] Załącznik Nr 2 do ww. zarządzenia dyrektora M-GOPS.
[10] Dz. U. z 2017 r. poz. 524.

Dyrektor ośrodka wyjaśniła, że nie wykorzystywano terminali z uwagi na problemy z ich konfiguracją. *„W dniu 11 stycznia 2018 r. zostały skonfigurowane poprawnie i został przeprowadzony pierwszy wywiad środowiskowy".* (dowód: akta kontroli str. 326-327)

1.9. W czerwcu 2014 roku dyrektor M-GOPS zawarła umowę z Burmistrzem Czarnej Białostockiej na objęcie bezpłatną opieką serwisową sprzętu i oprogramowania komputerowego Ośrodka. W ramach opieki serwisowej, informatyk Urzędu Miejskiego w Czarnej Białostockiej zobowiązany był do:

- udzielania konsultacji telefonicznych i osobistych,
- usunięcia awarii sprzętu i oprogramowania,
- instalowanie nowych wersji oprogramowania,
- szkolenie użytkowników sprzętu,
- doradztwa w zakresie rozbudowy sprzętu komputerowego, reinstalacji oprogramowania, dokonywania dodatkowych instalacji oprogramowania,
- bieżącego optymalizowania konfiguracji oprogramowania i sprzętu komputerowego,
- awaryjnego odtwarzania danych archiwalnych,
- weryfikowania stosowanych zabezpieczeń przed wtargnięciem wirusa do systemu informatycznego,
- wsparcia informatycznego przy prowadzeniu strony internetowej.

(dowód: akta kontroli str. 47-48)

Do dnia kontroli ww. informatykowi nie udzielono upoważnienia do dostępu do tych danych, co szerzej opisano w dalszej części wystąpienia, w sekcji „Ustalone nieprawidłowości".

Informatyk Urzędu Miejskiego w Czarnej Białostockiej oświadczył, że nie posiada upoważnienia do dostępu do danych osobowy, jednak jest świadomy obowiązku zachowania ich w tajemnicy. Wskazał też, że konsultacje z pracownikami Ośrodka odbywają się często i udzielana jest im doraźna pomoc w usunięciu problemów. W latach 2016 – 2017 dwukrotnie wystąpiły awarie bazy danych systemu AMAZIS, co wymagało pomocy producenta w celu jej naprawy. Oświadczył też, że nie szkolił pracowników M-GOPS, a jedynie udzielał im instruktażu na stanowisku pracy.

(dowód: akta kontroli str. 52-53)

Ośrodek nie posiada umowy z producentem systemów dziedzinowych na przetwarzanie danych osobowych. Warunki umów licencyjnych (zawieranych corocznie) nie przewidują też regulacji dotyczących zachowania w poufności danych w przypadkach udostępniania producentowi baz danych do naprawy, co opisano w dalszej części wystąpienia, w sekcji „Ustalone nieprawidłowości". (dowód: akta kontroli str. 229-283)

1.10. Wszystkie komputery wchodzące w skład lokalnej sieci M-GOPS zabezpieczone były aktualnym oprogramowaniem antywirusowym. Zastosowana aplikacja bezpieczeństwa nie posiada jednak konsoli centralnego zarządzania, wykorzystywanej do kontroli zagrożeń ze strony złośliwego oprogramowania. W opinii biegłego zastosowanie konsoli centralnej tworzy możliwość, że system antywirusowy *„poza funkcją ochrony przez złośliwym oprogramowaniem, udostępnia narzędzia do monitorowania i zabezpieczenia komputerów działających w sieci lokalnej".* (dowód: akta kontroli str. 31-33)

Dyrektor Ośrodka wyjaśniła, że program antywirusowy *„nie posiada modułu zarządzania centralnego. Nie ma wytycznych, co do konieczności stosowania modułu centralnego zarządzania oprogramowaniem antywirusowym".* (dowód: akta kontroli str. 45)

1.11. M-GOPS nie posiadał własnej serwerowni. Dostęp do wewnętrznej sieci Ośrodka zabezpieczony był na każdej stacji roboczej przez oprogramowanie firewall, dostarczone z programem antywirusowym. M-GOPS nie posiadał fizycznego firewall'a separującego sieć LAN od Internetu, do którego dostęp uzyskano na podstawie umowy zawartej ze spółką Orange Polska S.A. Ośrodek nie korzystał z możliwości posługiwania się pocztą elektroniczną przewidzianą w systemie Elektroniczne Zarządzanie Dokumentami oraz proponowaną przez informatyka Urzędu Miejskiego w Czarnej Białostockiej możliwością korzystania z poczty w systemie Active.office. Do przekazywania informacji służbowych

w formie elektronicznej wykorzystywany był (na wszystkich stanowiskach komputerowych) ogólnodostępny portal. Ogłoszenia i informacje publiczne M-GOPS zamieszczał w Biuletynie Informacji Publicznej Urzędu Miejskiego w Czarnej Białostockiej. W ocenie biegłego *„Wykorzystywanie w pracy M-GOPS kont poczty elektronicznej hostowanych przez operatorów komercyjnych (...), może stwarzać potencjalne niebezpieczeństwo dla danych Ośrodka".* (dowód: akta kontroli str. 31-33, 134-138)

Dyrektor Ośrodka wyjaśniła, że: *„Poczta elektroniczna EZD nie była wykorzystywana, gdyż nie było takiej potrzeby, wprowadzono możliwość użytkowania poczty do przekazywania informacji służbowych w systemie Active.office. Zarządzeniem Nr 9/2017 z dnia 19 grudnia 2017 r. (...) pracownicy zostali zobowiązani do używania powyższej poczty".* (dowód: akta kontroli str. 45-46)

1.12. W Instrukcji zarządzania systemem informatycznym (...) wskazano, że dane osobowe mogą być przechowywane na: [1] serwerach zlokalizowanych w obszarach wyznaczonych do przetwarzania danych osobowych, [2] wymiennych nośnikach elektronicznych, [3] na poszczególnych stacjach roboczych. Według Instrukcji nośniki zawierające kopie zapasowe powinny być przechowywane w innym pomieszczeniu niż to, w którym umieszczony jest serwer przetwarzający dane osobowe, w odpowiednio zabezpieczonej szafie, do której dostęp mogą mieć wyłącznie osoby upoważnione. W Instrukcji nie określono częstotliwości sporządzania i testowania kopii oraz okresu ich przechowywania. Ośrodek dysponował 22 płytami CD (przechowywanymi w gabinecie dyrektora), na których sporządzono kopie danych przetwarzanych w systemach od 9 stycznia 2009 r. do 8 kwietnia 2011 r., z tego: 12 płyt sporządzono w 2009 roku (w każdym miesiącu), osiem – w 2010 roku i dwie – w 2011 roku. W grudniu 2017 roku zakupiono dysk zewnętrzny do przechowywania baz danych z programów wykorzystywanych w Ośrodku. Przyczyny zaniechania obowiązku sporządzania kopii baz danych opisano w dalszej części wystąpienia, w sekcji „Ustalone nieprawidłowości".

(dowód: akta kontroli str. 52-53, 54, 220-225)

1.13. Biegły stwierdził, że pracownicy M-GOPS mają możliwość ściągania aplikacji, gdyż posiadają pełne uprawnienia do zarządzania systemem operacyjnym komputera, co opisano w dalszej części wystąpienia, w sekcji „Ustalone nieprawidłowości". Podczas oględzin urządzeń nie stwierdzono jednak zainstalowanych nieautoryzowanych aplikacji. Nie mniej jednak biegły ocenił, że istniejąca *„możliwość zapisywania na obsługiwanych komputerach pików wykonywalnych jak i uruchamiania ich, stwarza niebezpieczeństwo kopiowania danych do tego nieprzeznaczonych i zainfekowania komputerów złośliwym oprogramowaniem.* (dowód: akta kontroli str. 31-33)

W Ośrodku nie prowadzono ewidencji programów zainstalowanych na poszczególnych stacjach komputerowych. Dopiero w trakcie kontroli informatyk Urzędu Miejskiego w Czarnej Białostockiej (świadczący usługi serwisowe) sporządził wykazy zainstalowanego oprogramowania na każdej jednostce. (dowód: akta kontroli str. 7-18)

Dyrektor Ośrodka wyjaśniła, że: *„Nie sporządzano wykazów zainstalowanych oprogramowań na komputerach z uwagi na przeoczenie. Wykaz zainstalowanego oprogramowania został wykonany w dniu 14 grudnia 2017 r. przez informatyka".*

(dowód: akta kontroli str. 326-327)

1.14. Według opinii biegłego: *„Wszystkie zbadane komputery posiadały aktualne wersje systemów operacyjnych. Aktualizacje były wykonywane zgodnie z domyślnie ustawionym przez dostawcę systemu operacyjnego harmonogramem. Aktualna była również wersja oprogramowania dziedzinowego. Tryb jego aktualizacji wynikał również z domyślnych ustawień aplikacji".* (dowód: akta kontroli str. 31-33)

1.15. Płatności elektronicznie Ośrodek realizował na podstawie umowy o świadczenie przez PKO BP S.A. obsługi kasowej wypłat świadczeń pieniężnych na rzecz osób uprawnionych dokonywanych przez M-GOPS, zawartej 7 kwietnia 2016 r. Przelewy realizowano po złożeniu podpisu elektronicznego przez dwóch pracowników, którym Polska Wytwórnia Papierów Wartościowych S.A. w Warszawie wystawiła certyfikaty, zgodnie z umową o świadczenie usług certyfikacyjnych, zawartą 4 sierpnia 2016 r.

(dowód: akta kontroli str. 56-70)

Ustalone nieprawidłowości

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

1. Osoby świadczącej pomoc w zakresie usuwania awarii sprzętu komputerowego, wykorzystywanego od przetwarzania danych w Ośrodku, nie zobowiązano do zachowania w poufności danych osobowych, z którymi mogła mieć styczność podczas wykonywania tych czynności. Z osobą tą nie zawarto umowy gwarantującej odpowiedni poziom bezpieczeństwa informacji, stosownie do § 20 ust. 2 pkt 10 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[11].

   Dyrektor Ośrodka wyjaśniła, że: *„Umowy nie zawarto uznając, że ośrodek pomocy społecznej jest jednostką organizacyjną gminy, a osobą świadczącą pomoc jest osoba zatrudniona przez gminę, która jest zobowiązana do zachowania tajemnicy'.* Dodała, że: *„Osobę świadczącą pomoc w zakresie usuwania awarii sprzętu wykorzystywanego do przetwarzania danych w Ośrodku nie zobowiązano do zachowania poufności w odniesieniu do danych osobowych z uwagi na to, że nie jest to osoba z zewnątrz, a zatrudniona na potrzeby gminy i świadcząca usługi w ośrodku pomocy społecznej, tj. jednostce organizacyjnej gminy i jest zobowiązana do zachowania poufności w ramach pełnienia swoich obowiązków".* (dowód: akta kontroli str. 143-150)

2. Każdy użytkownik komputera wykorzystywanego do przetwarzania danych osobowych posiadał uprawnienia administratora systemu operacyjnego, a więc mógł samodzielnie zainstalować nieautoryzowane aplikacje. Możliwość zapisywania i uruchamiania na komputerach takich pików stwarza niebezpieczeństwo kopiowania danych lub zainfekowania komputerów złośliwym oprogramowaniem. Było to sprzeczne z przepisem § 20 ust. 2 pkt 4 rozporządzenia KRI, zgodnie z którym kierownictwo podmiotu publicznego jest obowiązane do podejmowania działań zapewniających, że osoby zaangażowane w proces przetwarzania informacji posiadają stosowne uprawnienia i uczestniczą w tym procesie w stopniu adekwatnym do realizowanych zadań oraz obowiązków, mających na celu zapewnienie bezpieczeństwa informacji.

   Dyrektor Ośrodka wyjaśniła, że: *„Do dnia kontroli żadnemu z pracowników Ośrodka nie powierzono obowiązków związanych z administrowaniem systemami informatycznymi, w których gromadzono dane osobowe w związku z tym, iż żadna z osób zatrudnionych w ops nie ma przygotowania informatycznego i nie było możliwości powierzenia tych obowiązków, a powierzenie osobie spoza ośrodka nie było możliwe ze względu na ograniczone środki finansowe".*

   (dowód: akta kontroli str. 31-33, 143-150)

3. Nie prowadzono rejestru dostępu do systemów. Logi systemowe na dyskach lokalnych gromadzone były domyślnie na każdym z komputerów (w postaci rejestru zdarzeń systemu Windows). Według opinii biegłego *„logi te nie były zabezpieczone przed modyfikacją, ani automatycznie analizowane".* Monitorowanie dostępu do informacji jest – w myśl § 20 ust. 2 pkt 7 lit. a rozporządzenia KRI – jednym z elementów zarządzania bezpieczeństwem informacji, zmierzającym do zapewnienia ochrony przetwarzanych informacji przed kradzieżą, nieuprawnionym dostępem, uszkodzeniami lub zakłóceniami.

   Dyrektor Ośrodka wyjaśniła, że: *„Ośrodek nie posiada sprzętu komputerowego do gromadzenia i tworzenia kopii logów centralnie. Nie posiada też systemu (oprogramowania) do autoanalizy logów systemowych".*

   (dowód: akta kontroli str. 31-33, 143-150)

4. W Instrukcji zarządzania systemem informatycznym nie określono częstotliwości sporządzania kopii danych przetwarzanych w Ośrodku. Jedynie w 2009 roku kopie te co miesiąc sporządzano na płytach CD. Natomiast w okresie objętym kontrolą ograniczono się do archiwizowania danych na oddzielnych partycjach dysku twardego każdego komputera, za pomocą funkcjonalności BACKUP, co nie zapewnia im ochrony w przypadku trwałego uszkodzenia lub kradzieży urządzenia. Było to niezgodne

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

z przepisem cz. A pkt IV ust. 4 lit. a załącznika do rozporządzenia MSWiA, zgodnie z którym kopie zapasowe przechowuje się w miejscach zabezpieczających je przed uszkodzeniem lub zniszczeniem. Przechowywanie tych kopii w miejscu skąd pochodzą dane stwarza duże ryzyko ich utraty, np. w przypadku wystąpienia pożaru, w wyniku którego zniszczeniu może ulec zarówno baza danych jak i jej kopia zapasowa.

Dyrektor Ośrodka wyjaśniła, że: *„W instrukcji zarządzania systemem informatycznym zostało pominięte określenie częstotliwości kopii bazy danych, gdyż uznano że są one zgrywane na komputerach. W późniejszym okresie nie sporządzono kopii bazy danych na płytach CD. Po podpisaniu umowy z urzędem zmieniono sposób sporządzania kopii zapasowych. Od tamtej pory na stanowisku komputerowym posiadającym bazę, kopie zapasowe wykonywane są codziennie (na oddzielnej partycji) podczas zamykania systemu. Dane okresowo zgrywane na dysk zewnętrzny (od niedawna). Nie ma harmonogramu sporządzania takich kopii".*

(dowód: akta kontroli str. 43-46, 190-228)

5. Umowy licencyjne na poszczególne systemy informatyczne wykorzystywane w M-GOPS do przetwarzania danych osobowych nie zawierały regulacji zobowiązujących dostawcę programu do zachowania w tajemnicy i nieudostępniania danych osobowych przekazanych przez Ośrodek w przypadku konieczności usunięcia awarii systemowych. Było to sprzeczne z przepisem § 20 ust. 2 pkt 10 rozporządzenia KRI, w myśl którego w umowach zawiera się zapisy gwarantujące odpowiedni poziom bezpieczeństwa informacji.

   Dyrektor Ośrodka wyjaśniła, że: *„Producent oprogramowania dziedzinowego firma INFO-R Sp.Jaw nie ma możliwości zdalnego dostępu do systemów informatycznych zainstalowanych w komputerach Ośrodka. Nie zawarto z w/w podmiotem umowy na przetwarzanie danych osobowych w dostarczonych systemach zobowiązującej do zachowania poufności danych w przypadku usunięcia awarii w bazach danych. W przypadkach uszkodzenia w bazie danych była ona spakowana i zabezpieczona hasłem, a następnie przesyłana na serwer producenta w celu naprawy, po dokonaniu naprawy producent zabezpieczył hasłem bazę danych i umożliwił pobranie jej ze swojego serwera. Dostęp do serwera firmy INFO-R wymaga podania indywidualnego loginu i hasła. Powyższa firma jest jedynym podmiotem, który może naprawić bazę danych. W przypadku wystąpienia sytuacji dokonania naprawy bazy danych zostanie zawarta umowa do zachowania poufności danych osobowych w naprawianych bazach danych".* (dowód: akta kontroli str. 229-283, 326-328)

6. Pracownicy Ośrodka wykorzystywali do celów służbowych pocztę elektroniczną, założoną na domenie internetowej należącej do podmiotu komercyjnego, co nie zapewnia odpowiedniego bezpieczeństwa danym zgromadzonym w M-GOPS. Wyjaśnienia dyrektor Ośrodka przytoczono w pkt. 1.11. niniejszego wystąpienia.

Ocena cząstkowa

Najwyższa Izba Kontroli ocenia negatywnie skuteczność przyjętych w M-GOPS 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. Z Rejestru GIODO wynika, że M-GOPS dokonał rejestracji ośmiu[12] zbiorów danych osobowych. Natomiast w PB wyszczególnionych było 11 takich zbiorów. I tak:

- do GIODO nie zgłoszono trzech zbiorów danych przetwarzanych w Ośrodku, tj.: „Ryczałty energetyczne", „Świadczenia za życiem", „Wspieranie rodziny i pieczy zastępczej",
- zbiory „System Kadrowo-Płacowy M-GOPS", „Rejestr pracowników i świadczeniobiorców Miejsko-Gminnego Ośrodka Pomocy Społecznej – Płatnik"

[12] „Wykaz świadczeniobiorców w Miejsko-Gminnym Ośrodku Pomocy Społecznej", „Zespół Interdyscyplinarny ds. Przeciwdziałania Przemocy w Rodzinie w Gminie Czarna Białostocka", „Świadczenia Rodzinne", „Fundusz Alimentacyjny", „Dodatki mieszkaniowe", „Zaliczka alimentacyjna", „Stypendia i zasiłki szkolne", „Świadczenia wychowawcze".

nie podlegały zgłoszeniu do GIODO, na podstawie art. 43 ust. 1 pkt 4 ustawy z dnia 29 sierpnia 1997 r. o ochronie danych osobowych[13] (dalej: „uodo"),

– w PB nie ujęto dwóch zarejestrowanych przez GIODO zbiorów, tj. „Zaliczka alimentacyjna" oraz zbioru danych przetwarzanych w systemie Elektronicznego Zarządzania Dokumentami dalej: EZD). (dowód: akta kontroli str. 71-99)

Kwestie związane z brakiem rejestracji prowadzonych zbiorów danych osobowych w Ośrodku opisano w dalszej części wystąpienia, w sekcji „Ustalone nieprawidłowości".

Ośrodek nie dysponował dokumentacją potwierdzającą, że w okresie objętym kontrolą do GIODO zgłoszono nowe zbiory danych. Nie występowano też o wykreślenie zbiorów danych osobowych. Brak było również dokumentacji, że GIODO odmówił zarejestrowania jakiegoś zbioru danych. (dowód: akta kontroli str. 71-99, 328-329)

2.2. Do dnia kontroli[14] nie skorzystano z możliwości powołania ABI, o którym mowa w art. 36a ust. 1 uodo.

Dyrektor Ośrodka wyjaśniła, że: *„Powierzenie dodatkowych obowiązków dla zatrudnionych pracowników jest zbyt dużym obciążeniem".* (dowód: akta kontroli str. 100-105, 328-329)

2.3. W myśl przepisu art. 36b uodo, w przypadku niepowołania ABI, zadania określone w art. 36a ust 2 pkt 1 uodo, z wyłączeniem obowiązku sporządzania sprawozdania, powinien realizować ADO. Z ustaleń kontroli wynika, że zadania te nie były realizowane, co przedstawiono w dalszej części wystąpienia, w sekcji „Ustalone nieprawidłowości".
(dowód: akta kontroli str. 100-105)

2.4. Prowadzona w Ośrodku ewidencja osób upoważnionych do przetwarzania danych osobowych, o której mowa w art. 39 ust. 1 uodo, zawierała jedynie wykaz imion i nazwisk 12 pracowników (w tym jedno dwukrotnie), którym wydano stosowne upoważnienia. W rejestrze tym nie zamieszczono informacji o siedmiu pracownikach PUP w Białymstoku, których upoważniono do przetwarzania danych osobowych beneficjentów Ośrodka, udostępnianych w portalu SEPI. Kwestie związane z poprawnością prowadzonego rejestru upoważnień przedstawiono w dalszej treści wystąpienia, w sekcji „Ustalone nieprawidłowości". Analiza zakresów obowiązków sześciu pracowników M-GOPS i wydanych im upoważnień do przetwarzania danych osobowych wykazała, że posiadali oni dostęp do zbiorów danych osobowych wynikający z wyznaczonych im zadań oraz upoważnienia[15]. (dowód: akta kontroli str. 106-133)

W Ośrodku od 20 lutego 2017 r. obowiązywała Instrukcja zarządzania systemem informatycznym (...). Analiza jej treści wykazała, że niektóre kwestie nie zostały uregulowane – np. nie określono zasad sprawowania kontroli nad tym, jakie dane osobowe, kiedy i przez kogo zostały do zbioru wprowadzone oraz komu były przekazywane, co opisano w dalszej części wystąpienia, w sekcji „Ustalone nieprawidłowości".
(dowód: akta kontroli str. 220-225)

2.5. W okresie objętym kontrolą dyrektor Ośrodka nie wydawała wewnętrznych aktów prawnych, procedur, instrukcji, poleceń dotyczących sposobu gromadzenia i przetwarzania zasobów informacyjnych. (dowód: akta kontroli str. 100-105, 328-329)

2.6. Do dnia kontroli pracownikom Ośrodka i osobom spoza nie powierzono obowiązków związanych z administrowaniem systemami informatycznymi (ASI), pomimo wyznaczenia zadań w § 11 i 12 Instrukcji zarządzania systemem informatycznym (...).
(dowód: akta kontroli str. 224-225)

Dyrektor Ośrodka wyjaśniła, że: *„Do dnia kontroli żadnemu z pracowników Ośrodka nie powierzono obowiązków związanych z administrowaniem systemami informatycznymi, w których gromadzono dane osobowe w związku z tym, iż żadna z osób zatrudnionych w ops nie ma przygotowania informatycznego i nie było możliwości powierzenia tych*

---

[13] Dz. U. z 2016 poz. 922.
[14] 4 grudnia 2017 r.
[15] Upoważnienia te zostały wydane 20 lutego 2017 r., a ich zakres obejmował dostęp do danych przetwarzanych we wszystkich (sześciu) systemach dziedzinowych.

obowiązków, a powierzenie osobie spoza ośrodka nie było możliwe ze względu na ograniczone środki finansowe". (dowód: akta kontroli str. 143-150)

2.7. W okresie objętym kontrolą nie prowadzono okresowych audytów wewnętrznych z zakresu bezpieczeństwa informacji, wymaganych w § 20 ust. 2 pkt 14 rozporządzenia KRI. Przyczyny tego stanu opisano w dalszej części wystąpienia, w sekcji „Ustalone nieprawidłowości". (dowód: akta kontroli str. 328-329)

2.8. Z analizy akt osobowych 24 pracowników Ośrodka wynika, że:

- osiem osób posiada zaświadczenia „O ukończeniu szkolenia ochrona danych osobowych", zorganizowanego w marcu 2014 roku (w zaświadczeniu nie określono zakresu szkolenia),
- dwie osoby posiadają certyfikat ukończonego szkolenia podstawowego z zakresu obsługi Systemu Elektronicznego Obiegu Dokumentów dla zwykłych użytkowników pełnej wersji systemu SEOD w urzędach i jednostkach podległych, które zrealizowano w październiku 2014 roku, w ramach projektu „Wdrażanie elektronicznych usług dla ludności województwa podlaskiego – część II administracja samorządowa" (w zaświadczeniu nie określono zakresu szkolenia),
- dwie osoby posiadają Certyfikat ukończenia szkolenia „Technologie Informatyczne", które odbyło się w marcu 2014 roku w ramach projektu systemowego „Szkolenia z nowych technologii pracowników 45+ zatrudnionych w instytucjach pomocy i integracji społecznej ze szczególnym uwzględnieniem pracowników socjalnych". Zakres tematyczny (56 godzinnego) szkolenia obejmował obsługę systemów biurowych MS Office (Word, Excel, Power Point), praktyczne zastosowanie programów MS Office, szkolenie: z systemów webowych, z systemów obiegu dokumentów i z narzędzi informatycznych. (dowód: akta kontroli str. 151-162)

W okresie objętym kontrolą dyrektor Ośrodka nie organizowała szkoleń z tematyki objętej kontrolą, w tym dotyczących zmiany przepisów o ochronie danych osobowych, która ma wejść w życie 25 maja 2018 r., w związku z implementacją rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (ogólne rozporządzenie o ochronie danych)[16], co opisano w dalszej części wystąpienia, w sekcji *„Ustalone nieprawidłowości".*

Dyrektor Ośrodka wyjaśniła, że: *„W związku z tym, iż jest koniec roku i środki finansowe przeznaczone na szkolenia zostały wykorzystane, szkolenie pracowników w zakresie zmian ochrony danych osobowych zostało zaplanowane w budżecie na rok 2018".*

(dowód: akta kontroli str. 100-105)

2.9. W okresie objętym kontrolą w Ośrodku nie prowadzono zewnętrznych kontroli w zakresie działania systemów informatycznych oraz rejestrów publicznych, które używano do realizacji zadań, w tym zleconych z zakresu administracji rządowej (np. przy przyznaniu i wypłacie świadczeń z Funduszu Alimentacyjnego, udzielaniu świadczeń wychowawczych, nadawaniu uprawnień wynikających z Karty Dużej Rodziny). W okresie tym nie zarejestrowano[17]też skarg związanych z przypadkami ujawnienia danych osobowych.

(dowód: akta kontroli str. 176-185, 328-329)

2.10. W okresie objętym kontrola w Ośrodku obowiązywały:

1. „Polityka Bezpieczeństwa w Miejsko-Gminnym Ośrodku Pomocy Społecznej", stanowiąca załącznik do zarządzenia nr 8/08 dyrektora M-GOPS z 16 grudnia 2008 r. (20 lutego 2017 r. utraciła moc w związku z wprowadzeniem nowej). Analiza jej treści wykazała, że była ona niezgodna z § 4 rozporządzenia MSWiA, bowiem nie opisywała sposobu przepływu danych pomiędzy poszczególnymi systemami AMAZIS, IZYDA, a także nie definiowała okoliczności pobierania informacji za pośrednictwem SEPI, portalu Emp@tia oraz EZD. (dowód: akta kontroli str. 186-189)

[16] Dz.U.UE.L.2016.119.1.

[17] Analizie poddano rejestr o symbolu 051 Skargi i wnioski załatwione bezpośrednio

2. „Instrukcja zarządzania systemem informatycznym służącym do przetwarzania danych osobowych w Miejsko-Gminnym Ośrodku Pomocy Społecznej w Czarnej Białostockiej", wprowadzona zarządzeniem nr 2/2014 dyrektora Ośrodka z 26 kwietnia 2014 r. (z dniem 20 lutego 2017 r. została zastąpiona nową). (dowód: akta kontroli str. 190-192)

3. „Polityka bezpieczeństwa przetwarzania danych w Miejsko-Gminnym Ośrodku Pomocy Społecznej, wprowadzona zarządzeniem Nr 1/2017 dyrektora M-GOPS z 20 lutego 2017 r. Analiza jej treści wykazała, że zawierała ona elementy wymienione w § 4 rozporządzenia MSWiA, z wyjątkiem braku opisu sposobu przepływu danych pomiędzy poszczególnymi systemami, co opisano w dalszej części wystąpienia, w sekcji „Ustalone nieprawidłowości". (dowód: akta kontroli str. 193-225)

4. „Instrukcja zarządzania systemem informatycznym służącym do przetwarzania danych osobowych Miejsko-Gminnego Ośrodka Pomocy Społecznej w Czarnej Białostockiej, stanowiąca załącznik nr 2 do zarządzenia dyrektora Ośrodka z 20 lutego 2017 r. Analiza jej treści wykazała, że zawierała ona elementy wyszczególnione w § 5 rozporządzenia MSWiA, z wyjątkiem: [1] opisu procedury nadawania, zawieszania, cofania lub wygaszania uprawnień do systemów, [2] określenia procedury tworzenia kopii zapasowych, [3] wyznaczenia czasu ich przechowywania, [4] uregulowania poziomu bezpieczeństwa przetwarzania danych osobowych Nie prowadzono też rejestru tworzonych kopii, co opisano w dalszej części wystąpienia, w sekcji „Ustalone nieprawidłowości". (dowód: akta kontroli str. 220-225)

W żadnym z ww. dokumentów nie określono poziomu bezpieczeństwa przetwarzania danych osobowych w systemach informatycznych M-GOPS, mimo takiego wymogu określonego w § 6 ust. 1 rozporządzenia MSWiA, a także 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 poniżej, w sekcji „Ustalone nieprawidłowości". (dowód: akta kontroli str. 100-105)

Ustalone nieprawidłowości

W działalności kontrolowanej jednostki w przedstawionym zakresie stwierdzono następujące nieprawidłowości:

1. Do GIODO (wbrew postanowieniom art. 40 ust. uodo) nie zgłoszono do rejestracji trzech zbiorów danych osobowych: „Ryczałty energetyczne", „Świadczenia za życiem", „Wspieranie rodziny i pieczy zastępczej".

   Dyrektor Ośrodka wyjaśniła, że *„W GIODO nie zarejestrowano zbioru:*

   - *ryczałty energetyczne, gdyż uznano, iż nie ma tam danych wrażliwych,*
   - *wspieranie rodziny i pieczy zastępczej uznano, że należy do zbioru podopiecznych Ośrodka, który jest zgłoszony do GIODO „Wykaz świadczeniobiorców w Miejsko-Gminnym Ośrodku Pomocy Społecznej w Czarnej Białostockiej",*
   - *świadczenia za życiem do dnia 4 grudnia 2017 r. nie wpłynął żaden wniosek dotyczący powyższej ustawy".* (dowód: akta kontroli str. 71-75, 100-105)

   Najwyższa Izba Kontroli zwraca uwagę, że obowiązkowi rejestracji w GIODO podlegają wszystkie zbiory danych osobowych (nawet te, które nie zawierają danych wrażliwych). Zbiór „Świadczenia za życiem" z założenia będzie zawierał dane wrażliwe (np. dotyczące dziecka z ciężkim i nieodwracalnym upośledzeniu albo nieuleczalną chorobą zagrażającą życiu), a zatem zgodnie z art. 41 ust. 3 uodo powinien być zgłoszony do GIODO przed rozpoczęciem przetwarzania w nim takich danych.

2. Obowiązująca od 16 grudnia 2008 r. do 19 lutego 2017 r. oraz obecna PB były niezgodne z § 4 rozporządzenia MSWiA, bowiem nie opisywały m.in. sposobu przepływu danych pomiędzy poszczególnymi systemami. Natomiast w obowiązującej Instrukcji zarządzania systemem informatycznym (...) nie określono procedury nadawania uprawnień do przetwarzania danych i rejestrowania tych uprawnień w systemie informatycznym oraz wskazania osoby odpowiedzialnej za te czynności, procedury tworzenia kopii zapasowych zbiorów danych oraz programów i narzędzi programowych służących do ich przetwarzania oraz okresu przechowywania kopii, co było sprzeczne z § 5 pkt 1, 4 i 5 rozporządzenia MSWiA. Nie opracowano też procedury wykonywania przeglądów i konserwacji systemów oraz nośników informacji

służących do przetwarzania danych. W myśl § 5 pkt 8 rozporządzenia MSWiA, procedury takie powinny stanowić element instrukcji zarządzania systemem informatycznym.

Dyrektor Ośrodka wyjaśniła, że: *„W ramach pełnienia swoich obowiązków, będąc na jednym ze szkoleń, poruszono temat polityki bezpieczeństwa przetwarzania danych osobowych w jednostce, korzystając z doświadczeń innych jak wygląda ten dokument postanowiono zmienić politykę bezpieczeństwa ośrodka".* Dodała, że: *„W PB nie opisano szczegółowego przepływu danych, gdyż na poziomie instalowania zakupionych programów nie posiadano wiedzy jakie dane z programu można pobierać".* Wyjaśniła też, że: *„W instrukcji zarządzania systemem informatycznym nie określono procedury nadawania uprawnień do przetwarzania danych i rejestrowania tych uprawnień w systemie informatycznym z uwagi na pominięcie tego zapisu".*

(dowód: akta kontroli str. 100-105, 143-150, 186-228)

3. Regulacje składające się na politykę bezpieczeństwa informacji, określoną w § 2 pkt 15 rozporządzenia KRI, nie odpowiadały wszystkim wymogom § 20 ust. 1 rozporządzenia MSWiA. W szczególności nie wskazano w nich, że przetwarzanie danych osobowych w systemie informatycznym M-GOPS – zgodnie z § 6 ust. 1 i 4 rozporządzenia MSWiA – wymaga wysokiego poziomu bezpieczeństwa.

   Dyrektor Ośrodka wyjaśniła, że przeoczono ten zapis.

   (dowód: akta kontroli str. 100-105, 186-228)

4. Wykaz zbiorów danych osobowych prowadzono nierzetelnie. Nie wykazano w nim bowiem prowadzonego zbioru „Zaliczka na fundusz alimentacyjny", co było sprzeczne z § 4 pkt 2 rozporządzenia MSWiA.

   Dyrektor Ośrodka wyjaśniła, że: *„W załączniku nr 2 do Polityki Bezpieczeństwa Ewidencja zbiory danych osobowych przetwarzanych w Miejsko-Gminnym Ośrodku Pomocy Społecznej omyłkowo nie ujęto zbioru zarejestrowanego przez GIODO Zaliczka alimentacyjna – 152470".* (dowód: akta kontroli str. 100-105, 193-216)

5. Ewidencja osób upoważnionych do przetwarzania danych osobowych nie odpowiadała wymogom określonym w art. 39 ust. 1 uodo, gdyż nie zawierała: daty nadania i ustania oraz zakresu upoważnienia do przetwarzania danych osobowych i identyfikatora użytkownika w systemie informatycznym. Ponadto nie ujęto w niej pracowników PUP w Białymstoku upoważnionych przez Dyrektora M-GOPS do przetwarzania danych osobowych beneficjentów pomocy społecznej, za pośrednictwem platformy SEPI.

   Dyrektor Ośrodka wyjaśniła, że: *„Ewidencja osób upoważnionych nie odpowiadała wymogom określonym w art. 39 ust. 1 uodo, gdyż pominięto zapisy, które powinny być określone w tejże ewidencji, a ponadto nie skorzystano z przykładowego załącznika".*

   (dowód: akta kontroli str. 100-133, 328-329)

6. Do przetwarzania danych beneficjentów Ośrodka dopuszczono czterech pracowników, którzy nie posiadali zaświadczeń o odbyciu szkolenia z zakresu ochrony danych osobowych. Obowiązek zapewnienia szkoleń osobom zaangażowanym w proces przetwarzania informacji, z uwzględnieniem zagrożenia jej bezpieczeństwa, skutków naruszenia zasad bezpieczeństwa, konsekwencji prawnych i środków zapewniających jej bezpieczeństwo, wynika z § 20 ust. 2 pkt 6 rozporządzenia KRI.

   Dyrektor Ośrodka wyjaśniła, że: *„W ośrodku osoby, które nie posiadają zaświadczeń o odbyciu szkolenia z zakresu danych osobowych, są to osoby nowo zatrudnione, podczas przyjęcia do pracy zostały zobowiązane do zapoznania się i przestrzegania ustawy o ochronie danych osobowych. Przeszkolenie tych osób zostanie dokonane w najbliższym czasie. W związku z tym, iż jest koniec roku i środki finansowe przeznaczone na szkolenia zostały wykorzystane, szkolenie pracowników w zakresie zmian ochrony danych osobowych zostało zaplanowane w budżecie na rok 2018".*

   (dowód: akta kontroli str. 34-40, 100-107, 151-162)

7. ADO nie realizował zadań określonych w art. 36a ust 2 pkt 1 uodo, tj. dokonywania sprawdzeń zgodności przetwarzania danych osobowych z przepisami o ochronie danych osobowych oraz nadzorowania opracowania i aktualizowania dokumentacji, o której

mowa w art. 36 ust. 2 tej ustawy. Nie określono zasad sprawowania kontroli nad tym, jakie dane osobowe, kiedy i przez kogo zostały do zbioru wprowadzone oraz komu są przekazywane, co było sprzeczne z art. 38 uodo.

Dyrektor Ośrodka wyjaśniła, że: *„W PB nie opisano zasad sprawowania kontroli jakie dane osobowe, kiedy i przez kogo zostały wprowadzone oraz komu są przekazywane, gdyż zatrudnieni pracownicy są osobami kompetentnymi, posiadającymi wiedzę, jakie dane mogą być wprowadzane do systemu i komu, jakie dane mogą być przekazywane".*
(dowód: akta kontroli str. 100-105, 328-329)

8. W okresie objętym kontrolą nie dopełniono obowiązku ustalonego w § 20 ust. 2 pkt 14 rozporządzenia KRI w zakresie prowadzenia nie rzadziej niż raz w roku audytów wewnętrznych z zakresu bezpieczeństwa informacji.

   Dyrektor Ośrodka wyjaśniła, że: *„Do dnia kontroli nie dysponowano odpowiednio przygotowanymi pracownikami do przeprowadzenia audytu wewnętrznego, nie potrafiliśmy tego zrobić, nie posiadano środków na opłacenie firmy, która specjalizuje się w powyższym zakresie".* (dowód: akta kontroli str. 100-105, 328-329)

Ocena cząstkowa

Najwyższa Izba Kontroli ocenia negatywnie opracowanie i wdrożenie dokumentacji i procedur wymaganych przepisami ustawy o ochronie danych osobowych.

3. Sposób przechowywania oraz zabezpieczenia danych

Opis stanu faktycznego

3.1. Ośrodek od lutego 2017 roku zajmował na parterze dwa pomieszczenia oraz II piętro w budynku Urzędu Miejskiego w Czarnej Białostockiej. Dysponował 14 pomieszczeniami, z tego dziewięcioma biurowymi. Pracownicy Ośrodka obsługiwali interesantów w pomieszczeniach biurowych. Wszystkie lokale Ośrodka były zabezpieczone drzwiami zwykłymi, zamykanymi na klucz. W oknach pomieszczeń nie było zamontowanych krat, rolet lub folii antywłamaniowej. Budynek Urzędu był wyposażony w dwustrefowy system alarmu włamania i napadu, który obejmował: w strefie I wejście tylne do budynku od strony parkingu wewnętrznego oraz klatkę schodową, korytarze i pomieszczenia na poddaszu (zajmowane przez Ośrodek), a w strefie II – wejście boczne, wejście główne hol przy wejściu głównym oraz korytarze i pomieszczenia na parterze i I piętrze. W budynku Urzędu zainstalowano monitoring wizyjny zewnętrzny i wewnętrzy obejmujący korytarze na każdym piętrze, w tym zajmowanym przez M-GOPS. Zainstalowano też system przeciwpożarowy, tj. czujki dymowe, sygnalizatory alarmowe, wewnętrzne hydranty, oświetlenie awaryjne, zasilanie awaryjne (podtrzymujące), gaśnice proszkowe. Na wyposażeniu Ośrodka nie było sejfów, a ich rolę spełniało sześć metalowych (wolnostojących) szaf zamykanych na klucz.
(dowód: akta kontroli str. 4-6, 328-329)

Zarządzeniem Nr 6/17 Burmistrza Czarnej Białostockiej z 11 stycznia 2017 r. wprowadzono Instrukcję określającą procedury postępowania z kluczami oraz zabezpieczeniami pomieszczeń w Urzędzie Miejskim w Czarnej Białostockiej. Zgodnie z jego § 1 pkt 2, klucze do pomieszczeń użytkowanych przez M-GOPS pozostawać powinny w dyspozycji tej jednostki, a – zgodnie z §1 pkt 3 – zasady postępowania z kluczami oraz zabezpieczenia pomieszczeń zajmowanych przez Ośrodek miał ustalić dyrektor tej jednostki. Do dnia kontroli zasad tych nie ustalono, co opisano w dalszej części wystąpienia, w sekcji „Ustalone nieprawidłowości". (dowód: akta kontroli str. 226-228)

3.2. W okresie objętym kontrolą w Ośrodku nie przeprowadzano inwentaryzacji zasobów informatycznych, w celu ustalenia specyfikacji technicznej każdej ze stacji roboczych oraz zainstalowanych wersji oprogramowania. Konieczności takiej nie określono też w Instrukcji zarządzania systemami informatycznymi (...), co opisano w dalszej części wystąpienia pokontrolnego, w sekcji „Ustalone nieprawidłowości". (dowód: akta kontroli str. 229-283)

3.3. W okresie objętym kontrolą nie zlecano na zewnątrz napraw sprzętu będącego nośnikiem danych (tj. komputerów, dysków). Stwierdzone awarie usuwane były w Ośrodku przez informatyka Urzędu Miejskiego w Czarnej Białostockiej świadczącego usługi serwisowe. W sierpniu 2016 roku do Punktu Zbierania Odpadów Komunalnych z Ośrodka przekazano cztery komputery. Na okoliczność tę sporządzono protokół przekazania oraz protokół zniszczenia dysków twardych komputerów. W protokole tym nie opisano metody likwidacji danych zawartych na tych nośnikach. (dowód: akta kontroli str. 284-286)

Dyrektor Ośrodka wyjaśniła, że: *„W protokole zniszczenia dysków twardych nie opisano metody likwidacji danych (...) uznając, iż działania przyjęte przez informatyka są profesjonalne i odpowiadają wymogom związanym z procedurą tych dysków (oświadczenie informatyka w załączeniu)".* (dowód: akta kontroli str. 145, 150)

3.4. W § 18 PB wskazano, że wydruki robocze, błędne lub zdezaktualizowane powinny być niezwłocznie niszczone przy użyciu niszczarki do papieru lub w inny sposób zapewniający skuteczne ich usunięcie. Do niszczenia dokumentów papierowych w Ośrodku wykorzystywano sześć niszczarek. (dowód: akta kontroli str. 204, 328-329)

3.5. W § 13 Instrukcji zarządzania systemem informatycznym (...) opisano zasady postępowania z komputerami przenośnymi poza siedzibą jednostki. Wskazano, że osoba używająca taki komputer powinna: (1) stosować ochronę kryptograficzną wobec danych osobowych przetwarzanych na tym komputerze, (2) zabezpieczyć dostęp do komputera na poziomie systemu operacyjnego – identyfikator i hasło, (3) nie zezwalać na używanie komputera osobom nieupoważnionym do dostępu do danych osobowych, (4) nie wykorzystywać komputera przenośnego do przetwarzania danych osobowych w obszarach użyteczności publicznej, (5) zachować szczególną ostrożność przy podłączaniu do sieci publicznych poza obszarem przetwarzania danych osobowych. Ośrodek w okresie objętym kontrola dysponował trzema urządzeniami mobilnymi, tj. laptop Notebook Lenovo (będący w dyspozycji dyrektora Ośrodka) oraz dwoma terminalami mobilnymi ACER TMB (użyczonymi przez Ministerstwo Pracy i Polityki Socjalnej do rejestracji danych opisujących sytuację rodziny w trakcie wywiadu środowiskowego w ramach projektu EMP@TIA). Terminale te od 23 grudnia 2013 r. do 10 stycznia 2018 r. były niewykorzystywane. (dowód: akta kontroli str. 225, 287)

Wyjaśnienia dyrektor M-GOPS na temat niewykorzystywania terminali mobilnych przytoczono w pkt. 1.8. niniejszego wystąpienia.

3.6. Sprzątaniem pomieszczeń zajmuje się pracownik gospodarczy Ośrodka. Odbywało się ono w godzinach pracy M-GOPS, w obecności pracowników jednostki.
(dowód: akta kontroli str. 328-329)

3.7. Do dnia kontroli w Ośrodku nie opracowano procedury, a w związku z tym nie wykonywano przeglądów i konserwacji systemów oraz nośników informacji służących do przetwarzania danych, co opisano w dalszej części wystąpienia, w sekcji „Ustalone nieprawidłowości". (dowód: akta kontroli str. 328-329)

3.8. W październiku 2017 roku w Ośrodku dokonano analizy szacowania ryzyka występowania okoliczności negatywnie wpływających na poziom bezpieczeństwa. Spośród 24 zagrożeń, zidentyfikowano 14 oraz określono metody przeciwdziałania tym zagrożeniom. Na przykład:

- zapewnienie obsługi informatycznej w celu szybkiej naprawy ma przeciwdziałać awariom serwera i infrastruktury sieciowej,
- zapewnienie aktualnej wersji systemu antywirusowego ma zapobiec atakom wirusów komputerowych,
- odpowiednie przeszkolenie pracowników oraz udzielenie im pomocy w zakresie potrzeby ma przeciwdziałać występowaniu błędów użytkownika,
- odpowiedni poziom złożoności haseł oraz ich okresowa wymiana ma zapobiegać uzyskaniu dostępu osoby nieupoważnionej do stacji roboczej lub do serwera,
- odpowiednie zabezpieczenie szafy teleinformatycznej ma zabezpieczyć dostęp do niej przez osoby nieupoważnione,
- podnoszenie świadomości wśród pracowników oraz monitorowanie ich pracy ma zapobiec złośliwemu działaniu użytkowników oraz używaniu prywatnych nośników danych (pendrive),
- instalacja alarmu p.poż., wyposażenie budynku w sprzęt gaśniczy, zakaz używania otwartego ognia w budynku, stosowanie właściwych zabezpieczeń instalacji elektrycznej ma zapobiec pożarom. (dowód: akta kontroli str. 41-42)

Do dnia kontroli nie opracowano procedury przywracania systemów po awarii oraz planu ciągłości działania, umożliwiającego kontynuację wykonywania zadań publicznych, co opisano w dalszej części wystąpienia, w sekcji „Uwagi dotyczące badanej działalności". Dyrektor Ośrodka wyjaśniła, że: *„Nie opracowano procedury przywracania systemów po awarii oraz planu ciągłości działania z uwagi na spiętrzenie innych zadań, uzupełnienie powyższego zostało zaplanowane w najbliższym czasie".*

(dowód: akta kontroli str. 143-150, 328-329)

3.9. Dyrektor Ośrodka wyjaśniła, że w latach 2016 – 2017 nie wystąpiły przypadki nieautoryzowanych działań związanych z przetwarzaniem danych.

(dowód: akta kontroli str. 43-45, 328-329)

Ustalone nieprawidłowości

W działalności kontrolowanej jednostki w przedstawionym zakresie stwierdzono następujące nieprawidłowości:

1. Do dnia kontroli, wbrew postanowieniom § 1 pkt 3 załącznika Nr 1 do zarządzenia Burmistrza Czarnej Białostockiej Nr 6/2017 z dnia 11 stycznia 2017 r. w sprawie wdrożenia instrukcji określającej procedury postępowania z kluczami oraz zabezpieczenia pomieszczeń w Urzędzie Miejskim w Czarnej Białostockiej, nie określono zasad postępowania z kluczami oraz zabezpieczenia pomieszczeń zajmowanych przez M-GOPS.

   Dyrektor Ośrodka wyjaśniła, że: *„W ośrodku pomocy społecznej był przyjęty zwyczaj dotyczący zarządzania kluczami. Dnia 15 grudnia 2017 r. zarządzeniem Nr 8/2017 określono procedurę postępowania z kluczami oraz zabezpieczenia pomieszczeń w Miejsko-Gminnym Ośrodku Pomocy Społecznej w Czarnej Białostockiej (kopia w załączeniu)".* (dowód: akta kontroli str. 143-150, 227-228)

2. W okresie objętym kontrolą nie przeprowadzano inwentaryzacji zasobów informatycznych Ośrodka, czym naruszono § 20 ust. 2 pkt 2 rozporządzenia KRI. Zgodnie z powołanym przepisem kierownik jednostki powinien zapewnić utrzymywanie aktualności inwentaryzacji sprzętu i oprogramowania, służącego do przetwarzania informacji obejmującej ich rodzaj oraz konfigurację, co ma umożliwić szybkie odtworzenie informatycznego środowiska pracy po nagłym zdarzeniu losowym (np. pożar, zalanie).

   Dyrektor Ośrodka wyjaśniła, że: *„W ramach prowadzonej działalności pominięto wskazaną potrzebę inwentaryzacji zasobów informatycznych ustalających specyfikację techniczną każdej stacji roboczej oraz zainstalowane wersje oprogramowania".*

   (dowód: akta kontroli str. 143-150, 328-329)

   W trakcie kontroli informatyk Urzędu Miejskiego w Czarnej Białostockiej (świadczący usługi serwisowe rzecz Ośrodka) sporządził dla każdego komputera indywidualną kartę, w której zawarto niezbędne informacje o konfiguracji urządzenia.

   (dowód: akta kontroli str. 7-18)

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 M-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 MSWiA. (dowód: akta kontroli str. 143-150, 328-329)

Ocena cząstkowa

Najwyższa Izba Kontroli ocenia pozytywnie mimo stwierdzonych nieprawidłowości, przestrzeganie w M-GOPS 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

W okresie objętym kontrolą Ośrodek dysponował dziewięcioma systemami informatycznymi, do przetwarzania danych, z tego sześcioma (dziedzinowymi), tj.:

- system HELIOS wykorzystywany do ewidencjonowania zdarzeń związanych z przyznaniem i wypłatą zasiłków okresowych, stałych, jednorazowych, przyznania pomocy w formie obiadów dzieciom w szkole i dorosłym oraz świadczenia usług opiekuńczych,
- system AMAZIS wykorzystywany do ewidencjonowania zdarzeń związanych z wypłatą świadczeń rodzinnych oraz przyznaniem i wypłatą różnych dodatków,
- system NEMEZIS wykorzystywany do obsługi Funduszu Alimentacyjnego oraz ewidencjonowania zdarzeń z tym związanych,
- system IZYDA wykorzystywany do ewidencjonowania spraw związanych z wypłatą świadczeń wychowawczych, tzw. „500 Plus",
- system TALES wykorzystywany do ewidencjonowania przyznawanych stypendiów szkolnych oraz wydatków na cele edukacyjne,
- system CHEOPS wykorzystywany do ewidencjonowania dodatków mieszkaniowych oraz wypłaconych ryczałtów energetycznych. (dowód: akta kontroli str. 290-302)

Aktualizacje ww. oprogramowania dokonywana była przez uprawnionych pracowników, za pośrednictwem strony internetowej producenta. (dowód: akta kontroli str. 19-22)

Ponadto w Ośrodku wykorzystywano system QNT do prowadzenia pełnej obsługi księgowości oraz spraw kadrowo-płacowych, system PŁATNIK służący do zgłaszania, wyrejestrowania osób z ubezpieczenia zdrowotnego i społecznego ZUS oraz system SMATDOC wykorzystywany do wspomagania i rejestrowania obiegu dokumentów.

(dowód: akta kontroli str. 19-22)

4.2. W okresie objętym kontrolą nie występowano o dokonanie aktualizacji danych w rejestrze prowadzonym przez GIODO, mimo że w przypadku jednego zbioru zachodziła taka konieczność wynikająca z powierzenia przetwarzania danych innemu podmiotowi, co szerzej opisano w dalszej części wystąpienia pokontrolnego, w sekcji „Ustalone nieprawidłowości". (dowód: akta kontroli str. 104-105, 328-329)

4.3. Zakres gromadzonych i przetwarzanych w GOPS danych osobowych był niezbędny do realizacji przypisanych mu zadań, wynikających m.in. z ustawy z dnia 12 marca 2004 r. o pomocy społecznej[18], ustawy z dnia 11 lutego 2016 r. o pomocy państwa w wychowywaniu dzieci[19], ustawy z dnia 29 lipca 2005 r. o przeciwdziałaniu przemocy w rodzinie[20], ustawy z dnia 5 grudnia 2014 r. o Karcie Dużej Rodziny[21] oraz w rozporządzeniach wykonawczych.

W okresie objętym kontrolą nie przeprowadzano naboru osób do pracy w GOPS.

(dowód: akta kontroli str. 300-301)

4.4. W latach 2016 – 2017 Ośrodek korzystał ze zbiorów danych osobowych, których administratorami były podmioty zewnętrzne, w tym z Samorządowej Elektronicznej Platformy Informatycznej SEPI (aktualizowanej na bieżąco przez PUP w Białymstoku). W ramach projektu EMP@TIA, realizowanego przez Ministerstwo Pracy i Polityki Socjalnej; Ośrodek uzyskał też dostęp do Centralnego Systemu Informacji Zabezpieczenia Społecznego, w tym z możliwości pobierania danych z systemów: Pesel, E-podatki, ZUS, AC Rynek Pracy, Eksmoon, NFZ-CWU, CEIDG, CBB, Centralnej Aplikacji Statystycznej. Uzyskanie dostępu do ww. zbiorów nie wymagało spełnienia przez M-GOPS specjalnych warunków takich, jak np. stworzenie wydzielonego łącza internetowego czy budowy określonej struktury sieci. (dowód: akta kontroli str. 108-133)

---

[18] Dz. U. z 2017 r. poz. 1769, ze zm.
[19] Dz. U. z 2017 r. poz. 1851, ze zm.
[20] Dz. U. z 2015 r. poz. 1390.
[21] Dz. U. z 2017 r. poz. 1832.

Ustalone nieprawidłowości

W działalności kontrolowanej jednostki w przedstawionym zakresie stwierdzono nieprawidłowość, polegającą na niezaktualizowaniu zgłoszenia rejestracyjnego do GIODO dotyczącego zbioru „Wykaz świadczeniobiorców w Miejsko-Gminnym Ośrodku Pomocy Społecznej", w związku z powierzeniem PUP w Białymstoku przetwarzania danych w tym zbiorze za pośrednictwem SEPI. Stanowiło to naruszenie przepisu art. 41 ust. 1 pkt 2 i ust. 2 uodo, zgodnie z którym w terminie 30 dni od dokonania zmiany ADO ma obowiązek zgłosić GIODO każdą zmianę dotyczącą informacji przekazywanych w związku z rejestracją zbioru.

Dyrektor Ośrodka wyjaśniła, że: *„Do GIODO nie zgłoszono faktu powierzenia siedmiu pracownikom PUP w Białymstoku przetwarzania danych osobowych beneficjentów Ośrodka w systemie SEPI z uwagi na niedopatrzenie.* (dowód: akta kontroli str. 100-133, 328-329)

Ocena cząstkowa

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

IV.Wnioski

Wnioski pokontrolne

Przedstawiając powyższe oceny i uwagi wynikające z ustaleń kontroli, Najwyższa Izba Kontroli, na podstawie art. 53 ust. 1 pkt 5 ustawy o NIK, wnosi o:

1. Dopełnienie obowiązku zgłoszenia do GIODO trzech zbiorów danych oraz uzupełnienie informacji o podmiotach przetwarzających dane, zgodnie z wymogami zawartymi w art. 40 i 41 uodo oraz rzetelne prowadzenie wykazu zbiorów danych osobowych.
2. Odebranie użytkownikom uprawnień administratora systemu operacyjnego komputerów wykorzystywanych do przetwarzania danych oraz nadanie tym osobom uprawnień odpowiadających zakresom ich obowiązków.
3. Przechowywanie kopii zapasowych baz danych systemów dziedzinowych w miejscu gwarantującym zabezpieczenie ich przed uszkodzeniem.
4. Zaktualizowanie PB i Instrukcji zarządzania systemem informatycznym, stosownie do wymogów § 20 ust. 1 rozporządzenia KRI oraz w § 4 pkt 3 – 4, § 5 pkt 1, 4 – 5, 8 i § 6 rozporządzenia MSWiA.
5. Przeprowadzanie inwentaryzacji sprzętu informatycznego i nośników informacji przetwarzanych w Ośrodku oraz dokonywanie ich okresowych przeglądów i konserwacji, w celu wykonania kontroli określonej w § 20 ust. 2 pkt 12 lit. h rozporządzenia KRI.
6. Wywiązanie się z obowiązków określonych w art. 36a ust 2 pkt 1 art. 38 uodo.
7. Analizowanie i zabezpieczenie przed modyfikacją lub zniszczeniem logów systemów operacyjnych komputerów wykorzystywanych w M-GOPS.
8. Wyegzekwowanie od pracowników korzystania wyłączne z autoryzowanego systemu poczty elektronicznej do przekazywania informacji służbowych.
9. Prowadzenie ewidencji osób upoważnionych do przetwarzania danych osobowych zgodnie z wymogiem określonym w art. 39 ust. 1 uodo.
10. Wywiązywanie się z obowiązków wynikających z § 20 ust. 2 pkt 14 rozporządzenia KRI, dotyczących prowadzenia audytów wewnętrznych z zakresu bezpieczeństwa informacji.
11. Zobowiązanie na piśmie osoby świadczącej pomoc w zakresie usuwania awarii sprzętu komputerowego do zachowania w poufności danych osobowych znajdujących się na urządzeniach Ośrodka.
12. Zapewnienie w umowach licencyjnych na systemy informatyczne wykorzystywane w Ośrodku regulacji zobowiązujących dostawcę programu do zachowania w tajemnicy i nieudostępniania danych osobowych przekazywanych przez M-GOPS.
13. Zapewnienie szkoleń, o których mowa w § 20 ust. 2 pkt 6 rozporządzenia KRI, wszystkim pracownikom zaangażowanym w proces przetwarzania informacji.

V. Pozostałe informacje i pouczenia

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

Prawo zgłoszenia zastrzeżeń

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

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 22 stycznia 2018 r.

Kontroler
Marek Zapolski
doradca ekonomiczny

.....
podpis

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

.....
podpis