NAJWYŻSZA IZBA KONTROLI
Delegatura w Białymstoku

LBI.410.023.06.2017
P/17/062

02259517

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

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	Krzysztof Gołębiewski – główny specjalista kontroli państwowej, upoważnienie do kontroli nr LBI/156/2017 z 15 listopada 2017 r. (dowód: akta kontroli str. 1-2)
Jednostka kontrolowana	Gminny Ośrodek Pomocy Społecznej w Narewce (zwany dalej „GOPS" lub „Ośrodkiem"), 17-220 Narewka, ul. Białowieska 5
Kierownik jednostki kontrolowanej	Elżbieta Potoniec, kierownik od 2 listopada 2003 r. (dowód: akta kontroli str. 3)

I. Ocena kontrolowanej działalności[1]

Ocena ogólna

Najwyższa Izba Kontroli ocenia pozytywnie, mimo stwierdzonych nieprawidłowości, działania GOPS[2] w zakresie zapewnienia właściwej ochrony elektronicznych zasobów informacyjnych przed nieuprawnionym dostępem, przejęciem lub zniszczeniem.

Uzasadnienie oceny ogólnej

Ośrodek wywiązał się z obowiązku opracowania i wdrożenia dokumentacji oraz procedur ochrony danych osobowych, określonych przepisami ustawy z dnia 29 sierpnia 1997 r. o ochronie danych osobowych[3]. Odpowiadały one wymogom zawartym w rozporządzeniu Ministra Spraw Wewnętrznych i Administracji z dnia 29 kwietnia 2004 r. w sprawie dokumentacji przetwarzania danych osobowych oraz warunków technicznych i organizacyjnych, jakim powinny odpowiadać urządzenia i systemy informatyczne do przetwarzania danych osobowych[4]. Dopełniono również obowiązku zgłoszenia zbiorów danych osobowych do rejestracji Generalnemu Inspektorowi Ochrony Danych Osobowych[5].

Dane osobowe, niezbędne do realizacji przypisanych Ośrodkowi zadań, gromadzono i przetwarzano w sposób zgodny z przepisami oraz przyjętymi procedurami. GOPS zapewnił także właściwą ochronę pomieszczeń, sprzętu oraz infrastruktury przed bezpośrednim działaniem czynników fizycznych i zdarzeń losowych, zgodną z obowiązującymi regulacjami wewnętrznymi w tym zakresie, a także przepisami rozporządzenia w sprawie dokumentacji oraz warunków technicznych.

Stwierdzone nieprawidłowości polegały na:

- nieprowadzeniu okresowych audytów bezpieczeństwa informacji wymaganych § 20 ust. 2 pkt 14 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[6],
- niezawarciu w umowie serwisowej sprzętu komputerowego, obowiązującej od 1 lipca 2015 r. do 30 czerwca 2016 r., zapisów gwarantujących odpowiedni poziom bezpieczeństwa informacji i ochrony danych, mimo wymogów określonych w § 20 ust. 2 pkt 10 rozporządzenia KRI,

---

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

[2] Kontrolą objęto okres od 1 stycznia 2016 r. do dnia zakończenia czynności kontrolnych oraz działania wcześniejsze mające wpływ na kontrolowaną działalność.

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

[4] Dz. U. Nr 100 poz. 1024 (rozporządzenie zwane dalej „rozporządzeniem w sprawie dokumentacji oraz warunków technicznych").

[5] Dalej „GIODO".

[6] Dz. U. z 2017 r. poz. 2247 (rozporządzenie zwane dalej: „rozporządzeniem KRI").

- niezapewnieniu pełnej kontroli administratora nad dostępem do zasobów sieciowych GOPS przez podmiot serwisujący,
- nieanalizowaniu i niezabezpieczeniu przed modyfikacją lub zniszczeniem logów systemów operacyjnych komputerów wykorzystywanych do przetwarzania danych,
- niezabezpieczeniu urządzeń sieciowych przed dostępem osób nieupoważnionych,
- nieujęciu w ewidencji osób upoważnionych do przetwarzania danych osobowych informacji o wszystkich osobach, którym udzielono takiego upoważnienia, mimo wymogu określonego w art. 39 ust. 1 ustawy o ochronie osobowych.

II. 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. Do gromadzenia i przetwarzania danych w GOPS wykorzystywano następujące systemy: [1] TOP-TEAM (w ramach którego działają programy dziedzinowe TT-Pomoc i TT-500+)[7], [2] Emp@tia[8], [3] System Informatyczny Karta Dużej Rodziny (SI KDR), [4] Centralna Aplikacja Statystyczna (CAS)[9], [5] Poczta Polska[10], [6] Płatnik[11], [7] eCorpoNet[12], [8] SmartDoc[13]. Ośrodek posiadał również program Cheops[14], który nie był wykorzystywany. (dowód: akta kontroli str. 50-54)

Oględziny wszystkich pięciu komputerów stacjonarnych wykorzystywanych do przetwarzania danych wykazały m.in., że:

- na każdym urządzeniu dostęp do systemu operacyjnego[15] możliwy był jedynie po wprowadzeniu nazwy użytkownika i hasła,
- comiesięczna zmiana hasła wymuszana była w sposób automatyczny zarówno w systemach dziedzinowych jak i w systemie operacyjnym,
- na wszystkich urządzeniach zainstalowano i na bieżąco aktualizowano program antywirusowy,
- na żadnym z komputerów nie stwierdzono użytkowania programów niezgodnie z warunkami licencji,
- na wszystkich jednostkach skonfigurowano wygaszacz ekranu uruchamiany po upływie 10 minut (powrót do systemu operacyjnego wymagał podania loginu i hasła użytkownika),
- wszystkie stanowiska komputerowe, na których znajdowały się systemy służące do przetwarzania danych posiadały dostęp do poczty służbowej oraz otwartego Internetu,
- dane na dyskach nie były szyfrowane,
- nie prowadzono rejestru dostępu do poszczególnych komputerów,
- na czterech komputerach zapewniono bieżącą aktualizację systemów operacyjnych (na jednym zainstalowany był system operacyjny nieposiadający wsparcia technicznego producenta, co szerzej opisano w dalszej części wystąpienia pokontrolnego, w sekcji „*Uwagi dotyczące badanej działalności*"). (dowód: akta kontroli str. 4-7)

---

[7] Wykorzystywane do gromadzenia i przetwarzania danych w zbiorach „*Pomoc społeczna*" i „*500+*".

[8] System umożliwiający wymianę informacji pomiędzy ośrodkami pomocy społecznej, centrami pomocy rodzinie, ZUS, urzędami pracy, urzędami skarbowymi, Centralną Ewidencją i Informacją o Działalności Gospodarczej, Centralną Ewidencją Pojazdów i Kierowców i in.

[9] Służąca przekazywaniu danych statystycznych gromadzonych w zbiorach „*Pomoc społeczna*", „*500+*" i „*Rejestr świadczeniobiorców*".

[10] System służący do rejestrowania korespondencji.

[11] System do przetwarzania danych kadrowych i danych ujętych w zbiorze „*Rejestr świadczeniobiorców*".

[12] System bankowości elektronicznej, służący do przetwarzania danych kontrahentów GOPS, danych kadrowych i danych zgromadzonych w zbiorze „*Rejestr świadczeniobiorców*".

[13] Rejestr korespondencji.

[14] System służący do przetwarzania danych w „*Rejestrze świadczeniobiorców*".

[15] Dwa zestawy komputerowe wyposażone były w system operacyjny Windows 7 Professional, jeden posiadał system Windows 7 Home Premium, jeden – Windows 8 Pro, a jeden – Windows XP Professional.

1.2. W czerwcu 2017 roku w Ośrodku przeprowadzono okresową analizę ryzyka utraty integralności, dostępności lub poufności informacji, wymaganą w § 20 ust. 2 pkt 3 rozporządzenia KRI. Na podstawie jej wyników opracowano plan postępowania z ryzykiem, obejmujący działania polegające m.in. na: [1] szkoleniach wewnętrznych personelu odpowiedzialnego za przygotowanie i obieg dokumentacji oraz osób odpowiedzialnych za wykonywanie dyspozycji Administratora Danych Osobowych[16] w systemach informatycznych, [2] stałym monitoringu rejestru osób upoważnionych i uprawnionych do przetwarzania danych, [3] monitorowaniu przez Administratora Systemów Informatycznych[17] stabilności działania systemów oraz prawidłowej pracy sprzętu informatycznego, [4] przeprowadzaniu wyrywkowych kontroli wykorzystania sprzętu zgodnie z przeznaczeniem i wewnętrznymi procedurami. (dowód: akta kontroli str. 123-135)

1.3. Każdy z pracowników zaangażowanych w przetwarzanie informacji w GOPS posiadał własny login i hasło, zarówno do systemu operacyjnego jednostek komputerowych, jak i dostępnych w nich systemów dziedzinowych. Nie stwierdzono przypadków użytkowania jednego konta przez kilku użytkowników. Uprawnienia administratora systemu operacyjnego posiadała osoba pełniąca funkcję ASI (informatyk zatrudniony w Urzędzie Gminy w Narewce) oraz Kierownik Ośrodka (w zakresie zbiorów danych, do których dostęp posiadali pracownicy GOPS). Analiza zakresów obowiązków wszystkich pracowników GOPS i wydanych dla nich upoważnień do przetwarzania danych osobowych wykazała, że posiadali oni dostęp do zbiorów danych osobowych wynikający z zakresów obowiązków oraz upoważnienia[18] do przetwarzania danych we wszystkich zbiorach, w których te dane przetwarzali (do dnia kontroli NIK, tj. do 12 grudnia 2017 r., nie cofnięto upoważnienia do przetwarzania danych osobowych byłemu pracownikowi GOPS, mimo że stosunek pracy z tą osobą ustał 30 czerwca 2016 r., co zostało opisane w dalszej treści wystąpienia pokontrolnego, w sekcji *„Uwagi dotyczące badanej działalności"*). Hasła dostępu poszczególnych użytkowników spełniały wymagania określone w *Instrukcji zarządzania systemami informatycznymi w GOPS* i w załączniku do rozporządzenia w sprawie dokumentacji oraz warunków technicznych i odpowiadały wymogom przyjętego w Ośrodku wysokiego poziomu bezpieczeństwa danych osobowych. (dowód: akta kontroli str. 136-197)

1.4. W Ośrodku nie prowadzono rejestru dostępu do systemów. Logi systemowe na dyskach lokalnych gromadzono domyślnie na każdym z komputerów (w postaci rejestru zdarzeń systemu Windows). Logi te nie były zabezpieczone przed modyfikacją, ani automatycznie analizowane, co szerzej zostało opisane w dalszej części wystąpienia pokontrolnego, w sekcji *„Ustalone nieprawidłowości"*. (dowód: akta kontroli str. 201)

1.5. Środkiem zabezpieczającym przed nieautoryzowanym dostępem do wszystkich systemów operacyjnych komputerów było hasło użytkownika, przy czym wymuszana była jego okresowa zmiana co 30 dni. W GOPS nie działała sieć WI-FI. Urządzenia sieciowe nie zostały zabezpieczone przed fizyczną ingerencją osób do tego nieupoważnionych (co zostało opisane w dalszej treści wystąpienia pokontrolnego, w sekcji *„Ustalone nieprawidłowości"*). (dowód: akta kontroli str. 201)

1.6. Konfiguracja sieciowa umożliwiała podłączenie do infrastruktury Ośrodka urządzeń niestanowiących jego własności (takich jak laptopy, telefony, tablety). Informacje o podłączeniu do komputerów nośników pamięci (np. pendrive lub dysku przenośnego) były domyślnie zapisywane w logach ich systemów operacyjnych. Dostęp do zasobów sieciowych uwierzytelniany był na poziomie użytkownika. Urządzenia sieciowe nie gromadziły i nie przechowywały w logach informacji o zewnętrznym sprzęcie podłączanym do sieci GOPS. Zasady korzystania ze sprzętu informatycznego niebędącego własnością Ośrodka omówiono w pkt. 3.5. wystąpienia. Kierownik GOPS wyjaśniła, że pracownicy nie używają swojego sprzętu domowego do pracy nad zadaniami powierzonymi w ramach obowiązków służbowych. (dowód: akta kontroli str. 201-202, 319)

---

[16] Dalej „ADO".
[17] Dalej „ASI".
[18] Upoważnienia te zostały wydane 19 czerwca 2017 r. wszystkim pracownikom GOPS przetwarzającym dane. Wcześniej formułowano je ogólnikowo, jako: *„upoważnienie do przetwarzania danych i obsługi systemu informatycznego oraz urządzeń wchodzących w jego skład, służących do przetwarzania danych osobowych"*.

1.7. Zgodnie z wyjaśnieniami kierownik Ośrodka oraz informatyka pełniącego obowiązki ASI, w latach 2016 – 2017 (do 4 grudnia) w GOPS nie odnotowano nieautoryzowanych działań związanych z przetwarzaniem informacji, tj. przypadków naruszenia bezpieczeństwa systemu informatycznego lub utraty integralności, dostępności lub poufności informacji.
(dowód: akta kontroli str. 204-207)

1.8. W Ośrodku nie funkcjonował zdalny dostęp do zasobów. (dowód: akta kontroli str. 202)

1.9. GOPS zawarł dwie umowy związane z nadzorem autorskim nad aplikacjami „TT- 500+" i „TT-Pomoc". Ustalono w nich obowiązki usługodawcy (spółki TOP-TEAM TT Sp. z o.o. w Warszawie), do których należały m.in.: [1] zapewnienie środków umożliwiających prawidłowe przetwarzanie i zabezpieczenie danych osobowych, [2] zachowanie w tajemnicy danych przekazanych przez GOPS i sposobów ich zabezpieczenia oraz nieprzetwarzanie ich w sposób inny niż określony w umowie (w szczególności nieudostępnianie uzyskanych danych osobowych osobom trzecim), [3] zniszczenie dostarczonych przez GOPS danych bezpośrednio po potwierdzeniu usunięcia zgłoszonych problemów związanych z funkcjonowaniem oprogramowania. W GOPS nie zapewniono jednak wystarczających środków uniemożliwiających nieautoryzowany dostęp do systemów operacyjnych i usług sieciowych (zagadnienie opisano w dalszej treści wystąpienia, w sekcji *„Ustalone nieprawidłowości"*). (dowód: akta kontroli str. 208-217, 323-330)

Od 1 lipca 2015 r. do 30 czerwca 2016 r. GOPS korzystał z serwisu sprzętu komputerowego na podstawie umowy zawartej z przedsiębiorstwem „NanoCom". Usługodawca zobowiązał się m.in do: [1] usuwania awarii w przypadku stwierdzenia błędu systematycznego w funkcjonowaniu sprzętu, [2] usuwania awarii sprzętu i oprogramowania powstałych z winy GOPS lub wskutek wypadków losowych, [3] konserwacji urządzeń raz na kwartał, [4] bieżącego optymalizowania konfiguracji sprzętu komputerowego, uwzględniającego potrzeby GOPS, [5] awaryjnego odtwarzania stanu oprogramowania i danych archiwalnych, [6] „weryfikowania" stosowanych zabezpieczeń antywirusowych. Pomimo wymogów określonych w § 20 ust. 2 pkt 10 rozporządzenia KRI, w umowie nie zawarto zapisów gwarantujących odpowiedni poziom bezpieczeństwa informacji i ochrony danych (co zostało opisane w dalszej treści wystąpienia, w sekcji *„Ustalone nieprawidłowości"*). Jak wyjaśniła kierownik GOPS, obecnie sprzęt jest serwisowany przez informatyka zatrudnionego w Urzędzie Gminy Narewka, pełniącego w Ośrodku funkcję ASI.
(dowód: akta kontroli str. 218-220, 318)

1.10. Wszystkie komputery wchodzące w skład lokalnej sieci Ośrodka zabezpieczone były aktualnym oprogramowaniem antywirusowym. Zastosowana aplikacja bezpieczeństwa posiadała konsolę centralnego zarządzania, wykorzystywaną do kontroli zagrożeń ze strony złośliwego oprogramowania. Nie wykorzystano jednak jej wszystkich możliwości, np. w postaci kontroli aplikacji – poprzez ustalenie zasad instalowania i korzystania z oprogramowania w sieci GOPS, czy tworzenia elektronicznego zestawienia wykorzystywanych urządzeń i oprogramowania. Dostęp do wewnętrznej sieci Ośrodka zabezpieczony był na każdej stacji roboczej przez oprogramowanie firewall, dostarczone z programem antywirusowym (GOPS nie posiadał fizycznego firewalla separującego sieć LAN od Internetu). Informatyk zatrudniony w Urzędzie Gminy w Narewce, udzielający wsparcia technicznego w Ośrodku, wyjaśnił: *„Kontrola aplikacji, jako funkcjonalność programu[19] (...) sprowadza się do możliwości ograniczenia dostępu do konkretnych aplikacji na poszczególnych stacjach roboczych. Technicznie polega to na utworzeniu tzw. czarnej i białej listy aplikacji. Funkcjonalność ta nie była wykorzystywana, ponieważ nie wystąpiły przesłanki, które by tego wymagały. Równocześnie pragnę nadmienić, iż w celu zapewnienia kontroli aplikacji na komputerach GOPS utworzono konta o ograniczonych uprawnieniach, które de facto zabezpieczają programy i aplikacje przed nieuprawnioną instalacją, modyfikacją lub usunięciem. W zakresie funkcjonalności programu (...) związanej z elektronicznym katalogiem sprzętu i oprogramowania wyjaśniam, iż w oparciu o nią nie było wykonywane zestawienie wykorzystywanych urządzeń. Ten stan wynikał z niewystarczającej mojej wiedzy w zakresie generowania i eksportowania z programu (...)*

[19] Antywirusowego.

pełnych ewidencji sprzętu. Funkcjonalność, o której mowa była wykorzystywana do weryfikacji / porównania informacji zebranych w trakcie spisu z natury".
(dowód: akta kontroli str. 202, 222)

1.11. Ośrodek nie posiada własnej serwerowni. Dostęp do Internetu uzyskano na podstawie umowy zawartej ze spółką Orange Polska S.A., zaś do służbowej poczty elektronicznej (na wszystkich stanowiskach komputerowych) – w ramach Systemu Wrota Podlasia[20] (GOPS korzystał także z modułu Cyfrowy Urząd, Biuletynu Informacji Publicznej, Systemu usług hostingowych www oraz Centrum Certyfikacji Województwa Podlaskiego). W regulaminie korzystania z Systemu wskazano, że do obowiązków Lidera (Województwo Podlaskie) należy: [1] utworzenie konta i nadanie odpowiednich uprawnień administratorowi lokalnemu, [2] zapewnienie ochrony antywirusowej oraz antyspamowej, [3] tworzenie kopii bezpieczeństwa poczty elektronicznej. (dowód: akta kontroli str. 223-246)

1.12. Zasady tworzenia kopii bezpieczeństwa oraz usuwania informacji zostały określone w *Instrukcji zarządzania systemami informatycznymi*, zgodnie z którą: [1] archiwizacja zasobów i wykonywanie kopii zapasowych odbywa się wg. planu podlegającego bieżącej aktualizacji, [2] kasowanie informacji na zewnętrznych nośnikach danych (pendrive) oraz nośnikach zainstalowanych w komponentach informatycznych (utylizowanych, przekazywanych do naprawy lub użytkowania podmiotowi zewnętrznemu) odbywa się przy pomocy specjalistycznego oprogramowania, poprzez fizyczne niszczenie (pocięcie, spalenie) nośników lub przy użyciu demagnetyzacji, [3] utylizację odnotowuje się w protokole zniszczenia. (dowód: akta kontroli str. 74-75, 83-84)

Dopiero w trakcie kontroli NIK, tj. 27 listopada 2017 r., sporządzono w GOPS kopię baz danych gromadzonych w systemach dziedzinowych na nośniku zewnętrznym (płyta CD).
(dowód: akta kontroli str. 283)

Informatyk udzielający wsparcia technicznego w Ośrodku, wyjaśnił: *„W okresie od 1.06.2017 r. do 28.11.2017 r. były tworzone kopie bezpieczeństwa zbiorów danych przetwarzanych w GOPS (...) na osobnej partycji dysku twardego, a same stacje (w tym też dyski) są nowe, wobec czego nie wystąpiła konieczność tworzenia kopii zapasowych na nośnikach zewnętrznych (...) Kopie bezpieczeństwa wykonywane są w sposób zautomatyzowany (raz w tygodniu), natomiast ich testowanie dokonywane jest w sposób manualny. Informacje o wykonywanych testach spójności kopii zapasowych są odnotowywane w dzienniku administratora".* (dowód: akta kontroli str. 205)

Kierownik GOPS wyjaśniła: *„W okresie od 1 stycznia 2016 r. do 31 maja 2017 r. były tworzone kopie bezpieczeństwa zbiorów danych przetwarzanych w GOPS, ale nie były one tworzone na nośnikach zewnętrznych, ponieważ kopie zapisywano na odrębnej partycji dysku twardego. Taki zapis kopii bezpieczeństwa uznano za wystarczający. Przewidziane są środki na zakup w 2018 roku sprzętu pozwalającego na automatyczne tworzenie kopii zapasowych na nośnikach zewnętrznych".* (dowód: akta kontroli str. 207)

W okresie objętym kontrolą w GOPS nie wystąpiła konieczność odtworzenia zbioru danych ze sporządzonej kopii bezpieczeństwa. Nie dokonywano także niszczenia kopii.
(dowód: akta kontroli str. 205, 207)

1.13. Pracownicy GOPS dysponowali możliwością ściągania aplikacji i plików wykonalnych, bez uprawnień do ich instalacji (uprawnienia do konfiguracji systemu posiadał jedynie administrator). Programy zainstalowane na poszczególnych stacjach komputerowych ujęto w ewidencji prowadzonej przez ASI. Na jednym z urządzeń zainstalowany był system operacyjny nieposiadający wsparcia technicznego producenta, co szerzej opisano w dalszej części wystąpienia pokontrolnego, w sekcji *„Uwagi dotyczące badanej działalności"*.
(dowód: akta kontroli str. 5, 200-202)

1.14. Wszystkie użytkowane w Ośrodku komputery stacjonarne posiadały aktualne wersje oprogramowania (aktualizacje były wykonywane zgodnie z harmonogramem domyślnie ustawionym przez dostawcę). (dowód: akta kontroli str. 202)

---

[20] System elektronicznej komunikacji i świadczenia elektronicznych usług administracji samorządowej w Województwie Podlaskim (wdrażany na podstawie umowy zawartej 30 grudnia 2015 r. pomiędzy Województwem Podlaskim i Gminą Narewka).

1.15. W GOPS wprowadzono procedurę dokonywania płatności[21], zgodnie z którą przelewy dokonywane były przez użytkowników posiadających stosowne uprawnienia, za pośrednictwem aplikacji dostarczonej przez bank. Zgodnie z załącznikiem[22] do umowy o świadczenie usług bankowości elektronicznej („eCorpoNet"), zawartej 4 września 2014 r. z Bankiem Spółdzielczym w Brańsku, dyspozycje przelewów zatwierdzane były przez kierownika GOPS, księgowego i skarbnika gminy (stosownie do uchwały Rady Gminy Narewka z 23 lutego 2016 r. obsługę finansową GOPS powierzono Urzędowi Gminy w Narewce). (dowód: akta kontroli str. 247-249)

Ustalone nieprawidłowości

W działalności GOPS w przedstawionym wyżej zakresie stwierdzono niżej wymienione nieprawidłowości.

1. Mimo wymogów określonych w § 20 ust. 2 pkt 10 rozporządzenia KRI, w umowie serwisowej sprzętu obowiązującej od 1 lipca 2015 r. do 30 czerwca 2016 r. nie zawarto zapisów gwarantujących odpowiedni poziom bezpieczeństwa informacji i ochrony danych. Kierownik GOPS wyjaśniła: „*Umowa z firmą NanoCom została zawarta zgodnie ze wzorcem przedstawionym przez usługodawcę. Mój stan wiedzy na dzień jej podpisania nie pozwalał na jednoznaczne określenie zapisów gwarantujących odpowiedni poziom bezpieczeństwa informacji i ochrony danych. Od dnia wygaśnięcia umowy, tj. dnia 30.06.2016 r. kwestiami związanymi z serwisowaniem sprzętu komputerowego zajmowałam się osobiście przy pomocy pracowników GOPS. Mój stan wiedzy okazał się niewystarczający, w związku z czym powzięłam decyzję o nawiązaniu współpracy z informatykiem Urzędu Gminy Narewka. W dniu 01.06.2017 r. informatykowi zostało wydane upoważnienie do przetwarzania danych osobowych w ramach prowadzonego wsparcia technicznego z Urzędu Gminy Narewka*". (dowód: akta kontroli str. 218-220, 318)

2. Logi gromadzone domyślnie w rejestrze zdarzeń systemu operacyjnego zainstalowanego w komputerach wykorzystywanych w GOPS nie były automatycznie analizowane ani chronione przed utratą integralności. Nie objęto ich procesem tworzenia kopii danych (backupu), co powodowało, że ich trwałość uzależniona była od ustawień producenta systemu i stwarzało zagrożenie skasowania lub nadpisania. Nie wprowadzono także harmonogramu tworzenia tych logów i nie gromadzono ich centralnie na serwerze Ośrodka. 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 ich kradzieżą, nieuprawnionym dostępem, uszkodzeniami lub zakłóceniami. Informatyk pełniący funkcję ASI i udzielający wsparcia technicznego w GOPS wyjaśnił: „*Logi gromadzone domyślnie w rejestrze zdarzeń systemu operacyjnego zainstalowanego w komputerach wykorzystywanych w GOPS nie były analizowane automatycznie, ponieważ koszt zakupu wyspecjalizowanego oprogramowania waha się w granicach 3 – 4 tys. USD, który to przekracza możliwości finansowe Ośrodka. Niezależnie, ze względu na niewielką ilość komputerów będących w użytkowaniu GOPS, zautomatyzowanie tego procesu było nieuzasadnione. Logi nie zostały objęte procesem tworzenia kopii zapasowych, ponieważ każdorazowa kopia takich logów zajmuje dużo miejsca na dyskach komputerów i zapisywanie ich mogłoby doprowadzić do wyczerpania przestrzeni dyskowej. Należy zaznaczyć, że rozwiązanie powyższego problemu zostało zaplanowane na rok 2018, na kiedy to jest planowany zakup urządzania do wykonywania backupu (...) Funkcję serwera pełni komputer Pani Kierownik, który ze względu na ograniczoną przestrzeń dyskową uniemożliwia wykorzystywanie go jako miejsce przechowywania logów systemów operacyjnych. Ze względu na brak wykonywania kopii logów, nie został utworzony harmonogram ich wykonywania*". (dowód: akta kontroli str. 201, 251)

3. Wbrew wymogom określonym w § 20 ust. 2 pkt. 7 lit. c rozporządzenia KRI, nie zapewniono pełnej kontroli administratora nad dostępem do zasobów sieciowych GOPS przez podmiot serwisujący, bowiem – jak wynika z opinii uczestniczącego w kontroli

[21] Weszła w życie 17 stycznia 2017 r.
[22] Załącznik z 11 lipca 2016 r.

biegłego z zakresu bezpieczeństwa systemów informatycznych – narzędzie przeznaczone do zdalnego kontrolowania systemu poprzez Internet nie wymagało od podłączanego użytkownika pełnej autoryzacji. Korzystano z autoryzacji użytkownika udostępniającego pulpit, dotyczącej jedynie nawiązania połączenia (kanału), a nie dostępu do komputera. Informatyk pełniący funkcję ASI i udzielający wsparcia technicznego w GOPS wyjaśnił: *„Na żadnym z komputerów będących w użytkowaniu GOPS Narewka nie jest zainstalowane oprogramowanie TeamViewier. Na komputerze Pani Kierownik jest wykorzystywany jedynie moduł klienta, który umożliwia zdalne sterowanie komputerem. Połączenie z tym komputerem, za pomocą wspomnianego modułu klienta, jest możliwe po podaniu jednorazowego hasła, które jest generowane przy uruchomieniu aplikacji klienckiej. Aplikacja nie jest uruchamiana automatycznie przy włączeniu systemu operacyjnego, wymaga uruchomienia przez użytkownika. Niezależnie warto zaznaczyć, iż użytkownik w trakcie połączenia nieustannie nadzoruje proces zdalnego połączenia i w każdym momencie może to połączenie zakończyć. W związku z czym cały proces jest dodatkowo nadzorowany przez użytkownika"*.

(dowód: akta kontroli str. 203, 251)

4. Urządzenia sieciowe w GOPS (router i switch) nie zostały zabezpieczone przed fizyczną ingerencją osób do tego nieupoważnionych (znajdowały się za biurkiem w jednym pomieszczeń, nie zaś w zabezpieczonej szafie), co stanowiło naruszenie cz. A pkt IV ust. 4 lit. a załącznika do rozporządzenia w sprawie dokumentacji oraz warunków technicznych. Kierownik Ośrodka wyjaśniła: *„Zastosowane zabezpieczenia w postaci umiejscowienia urządzenia w miejscu o utrudnionym dostępie dla osób postronnych oraz stosowanie polityki haseł, zebranie oświadczeń o zachowaniu w poufności, jak i stosowanie polityki kluczy (zamykanie pomieszczenia pod nieobecność), zostały uznane przeze mnie jako adekwatne do poziomu zagrożeń wiążących się z użytkowaniem routera i switcha we wskazanej lokalizacji."*

(dowód: akta kontroli str. 200, 318)

Uwagi dotyczące badanej działalności

Najwyższa Izba Kontroli zwraca uwagę, że:

1. W Ośrodku wykorzystywano jeden komputer (na którym przetwarzano dane w programach TT-Pomoc i TT-500+), z zainstalowanym systemem operacyjnym Windows XP, mimo że z dniem 8 kwietnia 2014 r. producent oprogramowania zakończył udzielanie wsparcia technicznego dla tego systemu. Kierownik GOPS wyjaśniła: *„W Ośrodku wykorzystywano komputer z zainstalowanym systemem operacyjnym Windows XP, ponieważ brak było środków finansowych na zakup nowego komputera. W budżecie na rok 2018 zostały zabezpieczone środki na zakup komputera z oprogramowaniem wspieranym przez producenta"*.

(dowód: akta kontroli str. 5, 200, 318)

2. Do dnia kontroli NIK, tj. do 12 grudnia 2017 r., nie cofnięto upoważnienia do przetwarzania danych osobowych byłemu pracownikowi GOPS, mimo że stosunek pracy z tą osobą ustał 30 czerwca 2016 r. Kierownik Ośrodka wyjaśniła: *„Upoważnienie do przetwarzania danych osobowych nie zostało przeze mnie cofnięte w wyniku przeoczenia. Jednak uprawnienia dostępowe tej osoby (login i hasło) do systemów obsługiwanych w GOPS zostały wygaszone z dniem rozwiązania stosunku pracy, tj. 30 czerwca 2016 r."* (dowód: akta kontroli str. 3, 143, 252)

Ocena cząstkowa

Najwyższa Izba Kontroli ocenia pozytywnie, mimo stwierdzonych nieprawidłowości, skuteczność przyjętych w 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. W GOPS, wg. stanu na 16 listopada 2017 r., prowadzono dziewięć zbiorów danych osobowych, z których pięć zgłoszono do GIODO, tj.: „Program Rodzina 500 plus", „Zespół interdyscyplinarny"[23], „Rejestr świadczeniobiorców", „Karta Dużej Rodziny", „Pomoc

[23] Przetwarzano w nim dane osób objętych realizacją zadań określonych w Gminnym Programie Przeciwdziałania Przemocy w Rodzinie.

społeczna". Dwa pierwsze z wymienionych zbiorów zgłoszono 23 marca i 22 lipca 2016 r. zaś kolejne trzy – 18 lipca 2017 r. (do dnia kontroli nie zostały one ujęte w rejestrze prowadzonym przez GIODO). W zgłoszeniach zawarto informacje wymagane w art. 41 ust. 1 ustawy o ochronie danych osobowych oraz zgodne z zakresem danych przetwarzanych w GOPS.

Nie stwierdzono przypadku odmowy rejestracji przez GIODO zgłaszanego zbioru danych, ani aktualizacji zbiorów już zgłoszonych. W okresie objętym kontrolą Ośrodek nie występował też do GIODO o wykreślenie z rejestru zbiorów danych osobowych.

Zbiory „Dane kadrowe", „Rejestr korespondencji", „Dane kontrahentów" i „Składnica akt" nie podlegały zgłoszeniu do GIODO, na podstawie art. 43 ust. 1 pkt 4 ustawy o ochronie danych osobowych. (dowód: akta kontroli str. 50, 253-255)

2.2. W Ośrodku 2 stycznia 2015 r.[24] został powołany Administrator Bezpieczeństwa Informacji[25], o którym mowa w art. 36a ust. 1 ustawy o ochronie danych osobowych. Funkcję tę powierzono pracownikowi Biura Bezpieczeństwa Informacji STS Elektronik w Białymstoku[26]. Wyznaczono mu zadania określone w art. 36a ust. 2 ustawy o ochronie danych osobowych, tj.: [1] zapewnienie przestrzegania przepisów o ochronie danych osobowych, w szczególności: sprawdzanie zgodności przetwarzania danych z przepisami o ochronie danych oraz opracowanie w tym zakresie sprawozdania dla administratora danych, nadzorowanie opracowania i aktualizowania dokumentacji opisującej sposób przetwarzania danych osobowych oraz przestrzeganie zasad w niej określonych, zapewnianie zapoznania osób upoważnionych do przetwarzania danych osobowych z przepisami o ochronie danych osobowych, [2] prowadzenie rejestru zbiorów danych przetwarzanych przez administratora danych. ABI powierzono również m.in.: [1] prowadzenie ewidencji osób upoważnionych do przetwarzania danych osobowych, [2] przeprowadzanie corocznych sprawdzeń wewnętrznych (audytów) z zakresu bezpieczeństwa informacji, [3] zorganizowanie dla pracowników GOPS szkolenia z zakresu ochrony danych osobowych i bezpieczeństwa informacji oraz zapoznanie ich z obowiązującą w tym zakresie dokumentacją. (dowód: akta kontroli str. 16, 22-23)

Kierownik Ośrodka, w terminie określonym w art. 46b ust. 1 ustawy o ochronie danych osobowych, zgłosiła[27] GIODO do rejestracji powołanie ABI. W zgłoszeniu zawarto wszystkie elementy wymagane w art. 46b ust. 2 ww. ustawy, tj. m.in.: oznaczenie administratora danych i adres jego siedziby (w tym numer identyfikacyjny REGON), imię, nazwisko, nr PESEL, nr dokumentu tożsamości ABI i adres do korespondencji, datę powołania, oświadczenie Kierownika Ośrodka o spełnianiu przez ABI warunków przewidzianych w art. 36a ust. 5 i 7 ustawy o ochronie danych osobowych. Do 16 listopada 2017 r. nie dokonywano zmian na tym stanowisku, a według stanu na dzień kontroli informacje zawarte w zgłoszeniu pokrywały się z danymi w rejestrze prowadzonym przez GIODO[28].
(dowód: akta kontroli str. 256)

2.3. W okresie objętym kontrolą ABI podejmował następujące działania wynikające z art. 36a ust. 2 ustawy o ochronie danych osobowych:

- w styczniu 2017 roku opracował: *„Instrukcję zarządzania systemami informatycznymi"*, *„Politykę bezpieczeństwa danych osobowych"* oraz *„Politykę bezpieczeństwa informacji"* w GOPS,
- opracował wykaz pomieszczeń tworzących obszar przetwarzania danych osobowych,
- sporządził wykaz zbiorów danych osobowych wraz ze wskazaniem programów zastosowanych do ich przetwarzania,
- wykonał opis struktury zbiorów danych ze wskazaniem zawartości poszczególnych pól informacyjnych,

---

[24] Zarządzeniem nr 1/2017 Kierownika Gminnego Ośrodka Pomocy Społecznej w Narewce z dnia 2 stycznia 2017 r. w sprawie powołania Administratora Bezpieczeństwa Informacji oraz powołania zastępców Administratora Bezpieczeństwa Informacji w Gminnym Ośrodku Pomocy Społecznej w Narewce.
[25] Dalej „ABI".
[26] Partner spółki Optimus S.A.
[27] Data wysłania zgłoszenia: 20 stycznia 2017 r.
[28] https://egiodo.giodo.gov.pl/search_ado.dhtml.

- prowadził ewidencję osób upoważnionych do przetwarzania danych osobowych,
- opracował i pobrał oświadczenia o zapoznaniu z przepisami o ochronie danych osobowych pracowników Ośrodka, upoważnionych do przetwarzania danych osobowych,
- prowadził rejestr użytkowników i uprawnień w systemie informatycznym,
- przeprowadził szkolenie mające na celu zapoznanie osób upoważnionych do przetwarzania danych osobowych z przepisami o ochronie danych osobowych,
- opracował plan sprawdzeń (sprawdzenie zgodności przetwarzania danych osobowych z przepisami o ich ochronie, zaplanowane na III – IV kwartał 2017 r., nie zostało przeprowadzone do dnia kontroli NIK; jak wynika z korespondencji mailowej prowadzonej pomiędzy ABI i ADO, termin sprawdzenia zaplanowano na 15 – 29 grudnia 2017 r.),
- prowadził rejestr zbiorów danych wraz z informacjami wymaganymi w art. art. 41 ust. 1 pkt 2 – 4a i 7 wymienionej ustawy (zawarto w nim siedem z dziewięciu zbiorów danych osobowych przetwarzanych w GOPS, tj. „Pomoc społeczna", „Rejestr świadczeniobiorców", „Program Rodzina 500 plus", „Karta Dużej Rodziny", „Przeciwdziałanie przemocy" („Zespół interdyscyplinarny"), „Rejestr korespondencji" i „Składnica akt". (dowód: akta kontroli str. 24-138, 256-279)

2.4. W GOPS prowadzono ewidencję osób upoważnionych do przetwarzania danych osobowych zawierającą 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, zakres upoważnienia oraz identyfikator. Według stanu na 16 listopada 2017 r. w ewidencji ujęto wszystkich (czterech) pracowników GOPS, z podaniem zbiorów i zakresów upoważnień odpowiadających treści upoważnienia do przetwarzania danych osobowych, udzielonego przez Kierownika Ośrodka[29]. Analiza zakresów obowiązków tych pracowników i wydanych dla nich upoważnień wykazała, że posiadali oni dostęp do zbiorów danych osobowych wynikający z zakresów obowiązków oraz upoważnienia do przetwarzania danych we wszystkich zbiorach, w których te dane przetwarzali. Nie ujęto w niej natomiast informacji o 10 pracownikach Powiatowego Urzędu Pracy w Hajnówce[30], którym udzielono upoważnienia do przetwarzania danych osobowych (pochodzących z GOPS), co szerzej opisano w dalszej części wystąpienia pokontrolnego, w sekcji *„Ustalone nieprawidłowości"*.
(dowód: akta kontroli str. 277-279)

Obowiązek zapewnienia przez ADO kontroli nad tym, jakie dane osobowe, kiedy i przez kogo zostały do zbioru wprowadzone oraz komu były przekazywane został – stosownie do art. 38 ustawy o ochronie danych osobowych – sformułowany w *Polityce bezpieczeństwa danych osobowych*. (dowód: akta kontroli str. 40)

2.5. W okresie objętym kontrolą w GOPS nie zaszły zmiany organizacyjne powodujące konieczność zaktualizowania regulacji wewnętrznych dotyczących sposobu gromadzenia i przetwarzania zasobów informacyjnych. W Ośrodku, poza *„Polityką bezpieczeństwa danych osobowych"* i *„Instrukcją zarządzania systemami informatycznymi"*, wprowadzono *„Polityką bezpieczeństwa informacji"* (dokument ten omówiono w punkcie 2.10 wystąpienia) oraz *Instrukcję postępowania w sytuacji naruszenia systemu ochrony danych osobowych i bezpieczeństwa informacji* (opisaną w punkcie 3.8.) (dowód: akta kontroli str. 99-122)

2.6. W GOPS nie powołano ASI, mimo że w *Instrukcji zarządzania systemami informatycznymi* wskazano, iż ASI powoływany jest przez ADO. Kierownik Ośrodka wyjaśniła, że obowiązki ASI *„wykonywane są przez informatyka zatrudnionego w Urzędzie Gminy Narewka. W związku ze strategią bezpieczeństwa informacji osoba ta została wyznaczona do sprawowania technicznej opieki nad informatycznymi zasobami wszystkich jednostek organizacyjnych Gminy"*. Informatyk ten posiadał upoważnienie do przetwarzania danych osobowych w systemach, do których miał dostęp oraz zobowiązał się do zachowania w tajemnicy tych danych i sposobów ich zabezpieczenia. Do zadań ASI

[29] W ewidencji ujęto również pracowników Urzędu Gminy w Narewce, którym udzielono upoważnienia do przetwarzania danych w zbiorze „Przeciwdziałanie przemocy w rodzinie" oraz zajmującym się obsługą kadrową i finansową Ośrodka.
[30] Dalej: „PUP w Hajnówce".

– zgodnie z *Instrukcją zarządzania systemami informatycznymi* – należało m.in.: [1] sprawowanie nadzoru nad funkcjonowaniem infrastruktury sieciowej, urządzeń informatycznych oraz oprogramowania, [2] zapewnienie poprawnej i bezpiecznej eksploatacji środków przetwarzania informacji, [3] zapewnienie bezpieczeństwa plików systemowych przed ich nieuprawnioną modyfikacją lub utratą, [4] kontrolowanie zgodności systemów teleinformatycznych z odpowiednimi normami i politykami bezpieczeństwa, [5] systematyczna aktualizacja programów antywirusowych.

(dowód: akta kontroli str. 63-64, 195-197, 280)

2.7. W GOPS nie wywiązano się z obowiązku prowadzenia corocznych audytów wewnętrznych z zakresu bezpieczeństwa informacji, określonego w § 20 ust. 2 pkt 14 rozporządzenia KRI (co zostało opisane w dalszej treści wystąpienia pokontrolnego, w sekcji *„Ustalone nieprawidłowości"*). W zatwierdzonym przez Kierownika Ośrodka 2 stycznia 2017 r. *„Planie wdrożenia procedur i dokumentacji z zakresu danych osobowych i bezpieczeństwa informacji w GOPS"*, przeprowadzenie audytu przewidziano na I kwartał 2018 roku. (dowód: akta kontroli str. 24)

2.8. W styczniu 2017 roku ABI przeprowadził wśród wszystkich pracowników GOPS, zaangażowanych w proces przetwarzania informacji, szkolenie z zakresu ochrony danych osobowych. Objęto nim następujące zagadnienia: [1] zbiory danych, [2] dopuszczalność ich przetwarzania, obowiązki informacyjne, zapewnienie poufności, zasady udostępniania oraz powierzania danych osobowych, [3] postępowanie z danymi osobowymi w wersji papierowej, [4] skutki naruszenia zasad bezpieczeństwa informacji (odpowiedzialność służbowa, cywilna i karna), [5] sposoby zabezpieczenia danych (fizyczne, organizacyjne, informatyczne), [6] zasady bezpiecznego użytkowania sprzętu IT, korzystania z oprogramowania, Internetu, poczty elektronicznej, ochrony antywirusowej, [7] stosowanie środków zapewniających bezpieczeństwo informacji, w tym urządzeń i oprogramowania minimalizującego ryzyko błędów ludzkich, [8] nadawanie upoważnień do przetwarzania danych osobowych, [9] polityka haseł, procedura rozpoczęcia, zawieszenia i zakończenia pracy, [10] bezpieczeństwo w systemach teleinformatycznych, zagrożenia bezpieczeństwa informacji i ich konsekwencje, w tym odpowiedzialność prawna. W GOPS nie przeprowadzano szkoleń związanych ze zmianą 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)[31]. Kierownik GOPS, wyjaśniła: *„W I kwartale 2018 r. ABI przewiduje dostosowanie istniejącego w GOPS systemu zarządzania bezpieczeństwem informacji do wymogów rozporządzenia Parlamentu Europejskiego i Rady UE 2016/679 z dnia 27 kwietnia 2016 r. Po zakończeniu procesu aktualizacji i zatwierdzeniu przez ADO zaproponowanych zmian, nastąpi proces implementacji, którego kluczowym elementem będzie przeszkolenie personelu GOPS w zakresie nowych zasad dotyczących bezpieczeństwa informacji i ochrony danych osobowych"*.

(dowód: akta kontroli str. 267-276, 280-281)

2.9. W latach 2016 – 2017 w GOPS nie były przeprowadzane kontrole dotyczące bezpieczeństwa danych osobowych. Nie odnotowano również skarg w tym zakresie.

(dowód: akta kontroli str. 282)

2.10. *Polityka bezpieczeństwa danych osobowych* oraz *Instrukcja zarządzania systemem informatycznym* zostały opracowane przez ABI i zatwierdzone przez Kierownika Ośrodka 17 stycznia 2017 r. Zawarto w nich elementy wymagane w §§ 4 i 5 rozporządzenia w sprawie dokumentacji oraz warunków technicznych, tj.:

– w *Polityce bezpieczeństwa danych osobowych*: [1] aktualny wykaz budynków, pomieszczeń tworzących obszar, w którym przetwarzano dane osobowe, [2] aktualny wykaz wszystkich zbiorów danych osobowych wraz ze wskazaniem programów zastosowanych do ich przetwarzania, [3] opis struktury zbiorów danych, ze wskazaniem zawartości poszczególnych pól informacyjnych i powiązań między nimi, [4] sposób

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

przepływu danych pomiędzy poszczególnymi systemami, [5] określenie środków technicznych i organizacyjnych niezbędnych dla zapewnienia poufności, integralności i rozliczalności przetwarzanych danych[32];

- w *Instrukcji zarządzania systemem informatycznym*: [1] procedury nadawania uprawnień do przetwarzania danych i rejestrowania tych uprawnień w systemach informatycznych oraz wskazanie osoby odpowiedzialnej za te czynności[33], [2] stosowane metody i środki uwierzytelnienia oraz procedury związane z ich zarządzaniem i użytkowaniem, [3] procedury rozpoczęcia, zawieszenia i zakończenia pracy przeznaczone dla użytkowników systemów; [4] procedury tworzenia kopii zapasowych zbiorów danych oraz programów i narzędzi programowych służących do ich przetwarzania, [5] sposób, miejsce i okres przechowywania elektronicznych nośników informacji zawierających dane osobowe oraz kopii zapasowych, [6] sposób zabezpieczenia systemu informatycznego przed działalnością wirusów komputerowych i nieuprawnionym dostępem, [7] procedury wykonywania przeglądów i konserwacji systemów oraz nośników informacji służących do przetwarzania danych.

(dowód: akta kontroli str. 27-90)

W *Instrukcji zarządzania systemami informatycznymi* zawarto postanowienia świadczące o przyjęciu wysokiego poziomu bezpieczeństwa przetwarzania danych osobowych i odpowiadające wymogom rozporządzenia w sprawie dokumentacji oraz warunków technicznych (m.in. w zakresie polityki haseł, ochrony kryptograficznej oraz fizycznych i logicznych zabezpieczeń systemu informatycznego służącego do przetwarzania danych przed nieuprawnionym dostępem). (dowód: akta kontroli str. 60-79)

W Ośrodku opracowano *Politykę bezpieczeństwa informacji*. Stosownie do wymogów § 2 pkt 15 w związku z § 20 ust. 1 rozporządzenia KRI, określono w niej sposoby postępowania w zakresie doboru środków, metod i standardów wykorzystywanych do ustanowienia, wdrożenia, eksploatacji, monitorowania i udoskonalania systemu informatycznego oraz procedur organizacyjnych zapewniających bezpieczeństwo informacji. W Polityce zawarto m.in.: [1] zakres odpowiedzialności ADO, ABI, ASI oraz pracowników GOPS, [2] proces zarządzania ryzykiem i aktywami (w tym arkusz analizy ryzyka i plan postępowania z ryzykiem), [3] zabezpieczenia organizacyjne, fizyczne i logiczne[34], [4] procedury systemowe (w tym zasady postępowania z informacjami w celu minimalizacji ryzyka kradzieży informacji i środków przetwarzania[35], procedurę postępowania w przypadku wystąpienia incydentu związanego z bezpieczeństwem informacji i procedurę dotyczącą corocznych audytów wewnętrznych z zakresu bezpieczeństwa informacji).

(dowód: akta kontroli str. 99-122)

Ustalone nieprawidłowości

W działalności GOPS w przedstawionym wyżej obszarze stwierdzono niżej wymienione nieprawidłowości.

1. Pomimo obowiązku wynikającego z § 20 ust. 2 pkt 14 rozporządzenia KRI, w Ośrodku nie przeprowadzano corocznych audytów wewnętrznych z zakresu bezpieczeństwa informacji. Kierownik Ośrodka wyjaśniła: *„Nie miałam świadomości o obowiązku przeprowadzania corocznych audytów wewnętrznych z zakresu bezpieczeństwa informacji (...) Mój stan wiedzy w tym zakresie był niewystarczający, dlatego w dniu 2.01.2017 r. podpisana została umowa z firmą, która zawodowo wykonuje usługi związane z ochroną danych osobowych i bezpieczeństwa informacji. Według przygotowanego planu wdrożenia przeprowadzenie audytu w zakresie bezpieczeństwa informacji na podstawie rozporządzenia KRI planuje się w I kw. 2018 roku"*.

(dowód: akta kontroli str. 318-319)

2. W ewidencji osób upoważnionych do przetwarzania danych osobowych, wbrew wymogom art. 39 ust. 1 ustawy o ochronie danych osobowych, nie ujęto informacji o 10 pracownikach PUP w Hajnówce, którym Kierownik Ośrodka udzieliła upoważnienia

[32] W zakresie zabezpieczeń sprzętowych infrastruktury informatycznej i telekomunikacyjnej oraz zabezpieczeń narzędzi programowych i baz danych odwołano się do *Instrukcji zarządzania systemami informatycznymi*.
[33] Szczegółową procedurę nadawania, zmiany zakresu i anulowania upoważnień do przetwarzania danych osobowych zawarto w *Polityce bezpieczeństwa danych osobowych*.
[34] Określone w *Instrukcji zarządzania systemami informatycznymi*.
[35] Opisane w *Instrukcji zarządzania systemami informatycznymi*.

do przetwarzania danych osobowych (pochodzących z GOPS) w systemie Samorządowej Elektronicznej Platformy Informacyjnej[36]. Kierownik Ośrodka wyjaśniła, że wynikało to z jej przeoczenia. (dowód: akta kontroli str. 277-279, 321)

Ocena cząstkowa

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

3. Sposób przechowywania oraz zabezpieczenia danych

Opis stanu faktycznego

3.1. Zgodnie z przyjętą w Ośrodku polityką bezpieczeństwa informacji, wszystkie pomieszczenia stanowiące obszar przetwarzania danych (zlokalizowane na parterze budynku) oraz szafy, w których gromadzono dane w wersji papierowej, zamykane były na klucz (zbiorczą skrzynkę do zamykania kluczy przechowywano w gabinecie kierownika GOPS). Ośrodek nie posiadał sejfu (sporządzoną w trakcie kontroli NIK kopię bezpieczeństwa danych na płycie CD umieszczono w pomieszczeniu pełniącym funkcję składnicy akt, w zamkniętej szafie i metalowej kasetce). (dowód: akta kontroli str. 283-284)

Budynek Ośrodka nie był wyposażony w system kontroli dostępu. Nie posiadał także systemu alarmowego lub przeciwwłamaniowego. Okna nie były zabezpieczone przed włamaniem. Ośrodek nie korzystał z ochrony fizycznej. Wejście do budynku GOPS monitorowane było za pośrednictwem kamer umieszczonych na sąsiednim budynku Urzędu Gminy. Na korytarzu Ośrodka zainstalowano gaśnicę z ważnym przegląd technicznym. (dowód: akta kontroli str. 283-284)

W styczniu 2017 roku w GOPS przyjęto do stosowania *„Instrukcję w sprawie określenia procedury postępowania z kluczami oraz zabezpieczania pomieszczeń biurowych"*, w której zawarto m.in. zasady: [1] dostępu do pomieszczeń służbowych przez pracowników i osobę sprzątającą, [2] zabezpieczenia sprzętu komputerowego oraz dokumentacji w trakcie pracy i po jej zakończeniu, [3] wykonywania pracy w godzinach ponadwymiarowych, [4] otwierania budynku w porze nocnej, w dni wolne od pracy oraz w sytuacjach nadzwyczajnych, [5] przechowywania i udostępniania kluczy zapasowych. (dowód: akta kontroli str. 285-289)

3.2. Stosownie do wymogów § 20 ust. 2 pkt 2 rozporządzenia KRI, w Ośrodku prowadzono wykaz wszystkich urządzeń wykorzystywanych do przetwarzania danych, zawierający informacje o rodzaju sprzętu, zainstalowanych systemach operacyjnych i programach, adresie IP oraz adresie karty sieciowej LAN. (dowód: akta kontroli str. 291)

3.3. W okresie objętym kontrolą w GOPS nie dokonywano likwidacji lub naprawy sprzętu będącego nośnikiem danych. (dowód: akta kontroli str. 205, 207)

3.4. Do niszczenia dokumentów zawierających dane osobowe wykorzystywano niszczarkę, znajdującą się w pomieszczeniu nr 1 (stanowiącym obszar przetwarzania danych). Rozwiązanie to było zgodne z zapisem w *Polityce bezpieczeństwa danych osobowych*, stanowiącym, że: *„użytkownicy zobowiązani są do niszczenia dokumentów i tymczasowych wydruków w niszczarkach, niezwłocznie po ustaniu celu ich przetwarzania"*. (dowód: akta kontroli str. 41, 283)

3.5. W *Instrukcji zarządzania systemami informatycznymi* Ośrodka określono zasady użytkowania urządzeń mobilnych (tabletów, smartfonów, komputerów przenośnych). Wskazano w niej m. in. że: [1] praca w systemie informatycznym GOPS, poza jego siedzibą, wymaga odpowiedniego zabezpieczenia zarówno przesyłanych informacji jak i zdalnej stacji roboczej (zgodę na takie wykorzystanie systemu informatycznego wydaje ADO na wniosek pracownika), [2] uwierzytelnienie zdalnego użytkownika następuje za pomocą nazwy i hasła, [3] wymiana informacji odbywa się w postaci zaszyfrowanej, z wykorzystaniem mechanizmów kryptograficznych, [4] urządzenia wykorzystywane do dostępu zdalnego muszą posiadać aktualne oprogramowanie antywirusowe, [5] każdy dostęp jest automatycznie rejestrowany (logowany), [6] zabronione jest wykorzystanie do pracy zdalnej komputerów niebędących własnością GOPS, ani dostępnych publicznie (np. znajdujących się w kawiarenkach internetowych). Ośrodek posiadał jedno urządzenie typu tablet (tzw. terminal mobilny) otrzymane w ramach realizacji programu Emp@tia. Kierownik

[36] Dalej: „SEPI".

Ośrodka wyjaśniła, że: *„otrzymany w ramach realizacji programu Emp@tia tablet został wykorzystany kilkukrotnie, natomiast nie jest wykorzystywany do codziennej pracy".*
(dowód: akta kontroli str. 76-77, 319)

3.6. W GOPS stosowana jest polityka *„czystych biurek"*, zgodnie z którą dane osobowe w wersji papierowej zabezpieczane są – przed kradzieżą lub wglądem osób nieupoważnionych – w szafach. Sprzątanie pomieszczeń, w których przetwarzane są te dane odbywa się w obecności osób upoważnionych lub po skończonej przez nie pracy. Regulacje wewnętrzne w tym zakresie zostały określone w *Instrukcji zarządzania systemami informatycznymi,* w której wskazano że: *„(...) Przedstawiciele podmiotów zewnętrznych dostęp do obszarów bezpiecznych uzyskują tylko wtedy, gdy jest to konieczne (prace konserwacyjne, sprzątanie), a prace wykonują w obecności osoby upoważnionej (...) Osoba odpowiedzialna za pomieszczenie jest zobowiązana zadbać, aby podczas wykonywania prac wszelkie zasoby informatyczne i urządzenia do ich przetwarzania były odpowiednio zabezpieczone i chronione przed dostępem (...)."* Osoba sprzątająca otrzymała pisemną zgodę od Kierownika MGOPS na przebywanie w pomieszczeniach Ośrodka, w których przetwarzane są dane osobowe.
(dowód: akta kontroli str. 41, 67, 290)

3.7. Procedura wykonywania przeglądów konserwacji systemów oraz nośników informacji służących do przetwarzania danych stanowi integralną część *Instrukcji zarządzania systemami informatycznymi* w GOPS. Wskazano w niej m.in., że: [1] przeglądy i konserwacje powinny być wykonywane w terminach określonych przez producentów systemu lub zgodnie z harmonogramem ASI, jednak nie rzadziej niż raz do roku, [2] wszelkie prace konserwacyjne i naprawy sprzętu oraz aktualizacje systemu informatycznego, wykonywane przez podmiot zewnętrzny, powinny się odbywać na zasadach określonych w umowie, z uwzględnieniem klauzuli dotyczącej ochrony danych, [3] czynności naprawcze wykonywane doraźnie przez osoby nieposiadające upoważnień do przetwarzania danych (np. specjalistów z zewnątrz) muszą być wykonywane pod nadzorem osób upoważnionych, [4] przed przekazaniem uszkodzonego sprzętu komputerowego z danymi osobowymi do naprawy poza GOPS należy wymontować nośniki z danymi, trwale usunąć dane z użyciem specjalistycznego oprogramowania, a w przypadku braku możliwości usunięcia danych – naprawa powinna być nadzorowana przez osobę upoważnioną do tych czynności przez ADO. W procedurze wskazano ponadto, że za terminowość przeprowadzenia przeglądów i konserwacji oraz ich prawidłowy przebieg odpowiada ASI, który prowadzi również dziennik administratora. W 2017 roku (do 22 listopada) w dzienniku odnotowano 10 wpisów dotyczących m.in.: okresowej konserwacji stacji komputerowych i aktualizacji wtyczki do podpisu elektronicznego (11[37] i 27 lipca), zmiany hasła w ustawieniach skanera (4 i 15 września), testu przywracania danych z kopii zapasowej (25 września). (dowód: akta kontroli str. 60-79, 89-90)

3.8. GOPS nie posiadał dodatkowego źródła zasilania na wypadek długotrwałych przerw w dostawie energii elektrycznej. Kierownik Ośrodka wyjaśniła, że: *„Urząd Gminy Narewka dysponuje agregatem prądotwórczym, który jest uruchamiany w razie dłuższych braków w dostawie prądu. Z agregatu korzystają Urząd oraz GOPS"*. Komputery stacjonarne, na których znajdują się bazy danych, podłączone są do układów podtrzymujących napięcie typu UPS (wykonywana praca w przypadku utraty zasilania lub awarii pozostaje zapisana w systemach dzięki funkcji autozapisu). Ośrodek posiadał *Plan ciągłości działania systemu informatycznego* oraz *Instrukcję postępowania w sytuacji naruszenia systemu ochrony danych osobowych o bezpieczeństwa informacji*[38]. W dokumentach tych zawarto m.in. opis typowych incydentów wpływających na bezpieczeństwo danych oraz działań zapewniających przywrócenie zdolności realizacji działalności statutowej GOPS (ze wskazaniem niezbędnych zasobów i osób odpowiedzialnych).
(dowód: akta kontroli str. 4-7, 91-98, 319)

[37] Data pierwszego wpisu w dzienniku.
[38] Obydwa dokumenty zostały opracowane przez ABI i zatwierdzone przez kierownika GOPS w dniu 17 stycznia 2017 r.

3.9. W okresie objętym kontrolą nie wystąpiły przypadki utraty danych w wyniku kradzieży nośnika, przekazania go nieuprawnionej osobie, przypadkowego skasowania lub zniszczenia w rezultacie wystąpienia sytuacji nadzwyczajnych (pożar, zalanie).
(dowód: akta kontroli str. 205, 207)

Ustalone nieprawidłowości

W działalności Ośrodka w przedstawionym wyżej obszarze nie stwierdzono nieprawidłowości.

Ocena cząstkowa

Najwyższa Izba Kontroli ocenia pozytywnie działania GOPS dotyczące przestrzegania przyjętych procedur w zakresie przechowywania i zabezpieczania danych.

4. Przetwarzanie zasobów informacyjnych zgodnych z zakresem działalności GOPS

Opis stanu faktycznego

4.1. Dane osobowe w GOPS przetwarzane były w dziewięciu zbiorach danych, z których siedem prowadzono zarówno w wersji elektronicznej jak i papierowej. Do prowadzenia zbiorów danych osobowych w wersji elektronicznej wykorzystywano następujące systemy informatyczne: „Płatnik", „eCorpoNet", „TT-Pomoc", TT-500+", „Emp@tia", „Centralna Aplikacja Statystyczna", „Poczta Polska", System Informatyczny do obsługi Karty Dużej Rodziny. Systemy te zostały ujęte załączniku nr B[39] do *Polityki bezpieczeństwa danych osobowych*. (dowód: akta kontroli str. 50, 294)

4.2. W okresie objętym kontrolą nie dokonywano aktualizacji danych w rejestrze prowadzonym przez GIODO. (dowód: akta kontroli str. 253-255)

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[40], ustawy z dnia 11 lutego 2016 r. o pomocy państwa w wychowywaniu dzieci[41], ustawy z dnia 29 lipca 2005 r. o przeciwdziałaniu przemocy w rodzinie[42], ustawy z dnia 5 grudnia 2014 r. o Karcie Dużej Rodziny[43] oraz w rozporządzeniach wykonawczych. W okresie objętym kontrolą nie przeprowadzano naboru do pracy w GOPS. (dowód: akta kontroli str. 295-301)

4.4. GOPS korzysta z elektronicznej wersji zbioru danych osobowych Karta Dużej Rodziny[44], do którego uzyskał dostęp w grudniu 2015 roku[45]. Ponadto, na postawie porozumienia[46] zawartego 6 września 2013 r. ze Starostą Hajnowskim reprezentowanym przez Dyrektora PUP w Hajnówce, Ośrodek uzyskał – za pośrednictwem platformy SEPI – dostęp do danych osobowych beneficjentów GOPS zarejestrowanych w PUP. Strony porozumienia zobowiązały się do zachowania w tajemnicy danych osobowych beneficjentów oraz ich zabezpieczenia zgodnie z zasadami określonymi w ustawie o ochronie danych osobowych. Pracownicy PUP zostali upoważnieni do przetwarzania tych danych przez Kierownika GOPS. Jak wyjaśniła Kierownik, w Ośrodku nie udostępniano i nie pobierano informacji za pośrednictwem platformy SEPI.
(dowód: akta kontroli str. 302-316, 319)

Ustalone nieprawidłowości

W działalności Ośrodka w przedstawionym wyżej obszarze nie stwierdzono nieprawidłowości.

Ocena cząstkowa

Najwyższa Izba Kontroli ocenia pozytywnie sposób przetwarzania zasobów informacyjnych, który był zgodny z zakresem działalności GOPS.

---

[39] Załącznik B – *Wykaz zbiorów danych osobowych.*
[40] Dz. U. z 2017 r. poz. 1769, ze zm.
[41] Dz. U. z 2017 r. poz. 1851, ze zm.
[42] Dz. U. z 2015 r. poz. 1390.
[43] Dz. U. z 2017 r. poz. 1832.
[44] System informatyczny do obsługi KDR, znajdujący się na stronie internetowej Ministerstwa Rodziny, Pracy i Polityki Społecznej – kdr.mpips.gov.pl.
[45] Na podstawie loginu i hasła otrzymanych z Ministerstwa Pracy i Polityki Społecznej za pośrednictwem Centrum Komputerowego ZETO w Łodzi.
[46] W sprawie wdrożenia i funkcjonowania dwukierunkowej wymiany danych dotyczących beneficjentów obszaru rynku pracy i pomocy społecznej na platformie komunikacyjnej.

III. Wnioski

Wnioski pokontrolne

Przedstawiając powyższe oceny i uwagi wynikające z ustaleń kontroli, Najwyższa Izba Kontroli, na podstawie art. 53 ust. 1 pkt 5 ustawy z dnia 23 grudnia 1994 r. o Najwyższej Izbie Kontroli[47], wnosi o:

1. Wywiązywanie się z obowiązków wynikających z § 20 ust. 2 pkt 14 rozporządzenia KRI, dotyczących prowadzenia audytów wewnętrznych z zakresu bezpieczeństwa informacji.
2. Odpowiednie zabezpieczenie urządzeń sieciowych przed dostępem osób nieuprawnionych.
3. Wprowadzenie rozwiązań zapewniających pełną kontrolę administratora nad dostępem do zasobów sieciowych GOPS ze strony podmiotu serwisującego.
4. Analizowanie i zabezpieczenie przed modyfikacją lub zniszczeniem logów systemów operacyjnych komputerów wykorzystywanych w Ośrodku.
5. Ujęcie w ewidencji wszystkich osób upoważnionych przez Kierownika GOPS do przetwarzania danych osobowych.

IV. 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 16 stycznia 2018 r.

Kontroler
Krzysztof Gołębiewski
główny specjalista kontroli państwowej

.....
podpis

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

.....
podpis

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