NAJWYŻSZA IZBA KONTROLI
Delegatura w Białymstoku

LBI.410.023.05.2017
P/17/062

WYSTĄPIENIE POKONTROLNE

NAJWYŻSZA IZBA KONTROLI
Delegatura w Białymstoku
ul. Akademicka 4, 15-267 Białystok
T +48 85 874 81 00, F +48 85 874 81 33
lbi@nik.gov.pl

I. Dane identyfikacyjne kontroli

Numer i tytuł kontroli	P/17/062 – Bezpieczeństwo elektronicznych zasobów informacyjnych w jednostkach samorządu terytorialnego w województwie podlaskim[1]
Jednostka przeprowadzająca kontrolę	Najwyższa Izba Kontroli Delegatura w Białymstoku
Kontroler	Wojciech Zambrzycki – starszy inspektor kontroli państwowej, upoważnienie do kontroli nr LBI/155/2017 z 8 listopada 2017 r. (dowód: akta kontroli str. 1-2)
Jednostka kontrolowana	Gminny Ośrodek Pomocy Społecznej w Sztabinie, ul. Augustowska 45/1, 16-310 Sztabin (dalej: *GOPS* lub *Ośrodek*)
Kierownik jednostki kontrolowanej	Dorota Barbara Salik – Kierownik[2] (dowód: akta kontroli str. 3)

II. Ocena kontrolowanej działalności

Ocena ogólna

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

Uzasadnienie oceny ogólnej

Na powyższą ocenę wpłynęły m.in. następujące nieprawidłowości:

- użytkownicy czterech z ośmiu komputerów pracowali na nich na uprawnieniach administratora, co znacznie podwyższało niebezpieczeństwo niekontrolowanej utraty danych z tych urządzeń,
- nie był przeprowadzany okresowy audyt bezpieczeństwa informacji i analiza ryzyka utraty integralności, dostępności lub poufności informacji, stosownie do wymogów z § 20 ust. 2 pkt 3 i 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[4],
- rejestry zdarzeń (tzw. logi) nie były zabezpieczone przed usunięciem, modyfikacją lub utratą,
- polityka bezpieczeństwa informacji i instrukcja zarządzania systemami informatycznymi były niekompletne i nieaktualizowane od 2009 roku oraz nie była opracowana całościowa polityka bezpieczeństwa informacji,
- do rejestru prowadzonego przez Generalnego Inspektora Ochrony Danych Osobowych nie został zgłoszony zbiór klientów GOPS korzystających ze świadczeń wychowawczych,
- nie gromadzono bieżących informacji w zakresie inwentaryzacji sprzętu i oprogramowania służącego do przetwarzania informacji obejmujących ich rodzaj i konfigurację.

---

1 Kontrolą objęto lata 2016 – 2017 (do 15 grudnia).
2 Funkcję pełni od 28 kwietnia 2008 r.
3 Najwyższa Izba Kontroli stosuje 3-stopniową skalę ocen: pozytywna, pozytywna mimo stwierdzonych nieprawidłowości, negatywna.
4 Dz. U. z 2017 r. poz. 2247. Rozporządzenie zwane dalej: *rozporządzeniem KRI*.

363

III. Opis ustalonego stanu faktycznego

1. Rozwiązania dotyczące dostępu do poszczególnych systemów informatycznych i usług sieciowych zabezpieczające przed nieuprawnionym dostępem, przejęciem lub zniszczeniem zasobów informacyjnych

Opis stanu faktycznego

1.1. Do gromadzenia i przetwarzania danych w Ośrodku używano osiem programów dziedzinowych, edytorów tekstu, a także prowadzona była papierowa wersja dokumentacji zawierająca dane osobowe. (dowód: akta kontroli str. 243-245)

Na wyposażeniu Ośrodka znajdowało się osiem komputerów (siedem stacjonarnych i jeden laptop) oraz notebook (nieużytkowany). Na każdym komputerze utworzone było konto użytkownika (pracownika GOPS) oraz konto administratora (informatyka). Każdy z komputerów posiadał dostęp do Internetu. Ustawienie niektórych monitorów pozwalało klientom GOPS na wgląd w treść wyświetlanych informacji, co przedstawiono w dalszej części wystąpienia w sekcji *Ustalone nieprawidłowości.*

(dowód: akta kontroli str. 5-15, 308-310)

1.2. Kierownik GOPS w maju 2017 roku przeprowadziła analizę ryzyka utraty integralności, dostępności lub poufności informacji (wcześniej takich analiz nie przeprowadzała). Obowiązek przeprowadzania takich analiz wynika z § 20 ust. 2 pkt 3 rozporządzenia KRI. Analiza wykazała, że w Ośrodku istniało średnie ryzyko utraty bezpieczeństwa danych osobowych (32% prawdopodobieństwo utraty bezpieczeństwa danych osobowych).

(dowód: akta kontroli str. 155-181, 351)

W analizie nie wskazano konkretnych wniosków do wykonania w związku z jej wynikiem. Kierownik wyjaśniła, że po wykonaniu analizy, aby zmniejszyć ryzyko, wyłączyła sieć Wi-Fi i przebudowana została sieć wewnętrzna – położono nowe kable sieciowe i kable elektryczne, które były już wyeksploatowane, co pozwoliło na wprowadzenie nowych rozwiązań technicznych w sieci Ośrodka. (dowód: akta kontroli str. 352-356)

1.3. Pracownicy zaangażowani w proces przetwarzania informacji posiadali uprawnienia do użytkowanych programów w stopniu adekwatnym do realizowanych zadań i obowiązków. Zakresy obowiązków nie zmieniały się w okresie objętym kontrolą, w tym sensie, że pracowników nie delegowano do innych zadań (co wiązać się mogło z zaprzestaniem korzystania z użytkowanych wcześniej aplikacji), co najwyżej dodawano kolejne zadania. W zakresach obowiązków nie było jednak wskazane do jakiego typu oprogramowania pracownik ma dostęp. Kierownik Ośrodka wyjaśniła, że nie widziała powodu, dla którego należałoby wpisać takie informacje w zakresach obowiązków. Uprawnienia do konkretnych programów informatyk udzielał na polecenie Kierownik Ośrodka. Kontrola przetwarzania informacji gromadzonych w GOPS jest bardzo istotna z uwagi na gromadzenie w nim danych wrażliwych, o których mowa w art. 27 ustawy z dnia 29 sierpnia 1997 roku o ochronie danych osobowych[5], podlegających szczególnej ochronie i ograniczeniom w dostępie do nich. (dowód: akta kontroli str. 93-153, 351-356)

Każdy z pracowników posiadał własny login i hasło do stanowiska komputerowego i użytkowanego oprogramowania. Hasła spełniały wymogi określone dla wysokiego poziomu bezpieczeństwa, o którym mowa w punkcie XIV części C, w związku z punktem VIII części B załącznika do rozporządzenia Ministra Spraw Wewnętrznych i Administracji z dnia 29 kwietnia 2004 r. w sprawie dokumentacji przetwarzania danych osobowych oraz warunków technicznych i organizacyjnych, jakim powinny odpowiadać urządzenia i systemy informatyczne służące do przetwarzania danych osobowych[6], chociaż wewnętrzne regulacje o tym nie mówiły. Nie stwierdzono, aby użytkowano jedno konto przez kilku użytkowników. Czterech (z ośmiu) pracowników posiadało uprawnienia administratora swoich komputerów. Według informatyka Urzędu Gminy Sztabin, zajmującego się obsługą komputerów GOPS, wynikało to z potrzeby prawidłowego funkcjonowania aplikacji.

(dowód: akta kontroli str. 5-16, 308-310)

---

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

[6] Dz. U. Nr 100 poz. 1024. Rozporządzenie zwane dalej: *rozporządzeniem MSWiA*.

1.4. Nie był prowadzony papierowy ani elektroniczny rejestr dostępu do programów użytkowanych do przetwarzania danych osobowych. Biegły z dziedziny informatyki stwierdził, że gromadzone były informacje o ruchu sieciowym wychodzącym i przychodzącym do sieci Ośrodka, w tym wszelkich zagrożeniach bezpieczeństwa. Informacje o logach[7] były przetwarzane automatycznie do postaci pozwalającej na ułatwioną ich analizę. Logi nie były składowane centralnie ani też nie była wykonywana ich kopia zapasowa – znajdowały się bezpośrednio na monitorowanych urządzeniach. Nie były też zabezpieczone przed modyfikacją (o czym będzie mowa w dalszej części wystąpienia, w sekcji *Ustalone nieprawidłowości*), poza logami gromadzonymi w urządzeniu wielofunkcyjnej zapory sieciowej UTM (dostęp posiadał tylko administrator systemu), które były przesyłane automatycznie na komputer zdalny administratora.

Dedykowane narzędzia informatyczne były stosowane do badania stanu usług sieciowych, instalacji aktualizacji, instalacji oprogramowania na komputerach, badania statystyki wykorzystywania oprogramowania i użycia urządzeń USB.

(dowód: akta kontroli str. 324-327)

1.5. Biegły, powołany przez Najwyższą Izbę Kontroli, stwierdził, że urządzenia sieciowe chronione były przed nieautoryzowanym fizycznym dostępem poprzez umieszczenie ich w zamkniętej na klucz szafie. Dostęp do urządzenia wielofunkcyjnej zapory sieciowej UTM chroniony był hasłem. W Ośrodku nie było sieci Wi-Fi. (dowód: akta kontroli str. 324-327)

1.6. Wewnętrzne regulacje nie wskazywały, czy do sieci Ośrodka można podłączać zewnętrzny sprzęt (laptopy, telefony, tablety). Według biegłego, konfiguracja sieciowa uniemożliwiała podłączenie się do infrastruktury GOPS za pomocą sprzętu niestanowiącego własności pracodawcy oraz korzystania z jej zasobów. Informacje o podłączeniu do komputerów nośników pamięci (np. pendrive lub dysk przenośny) były monitorowane przez aplikację Desktop Central[8]. (dowód: akta kontroli str. 324-327)

1.7. Nie wystąpiły przypadki wykrycia nieautoryzowanych działań związanych z przetwarzaniem informacji, np. penetracji systemu informatycznego przez nieuprawnioną osobę. (dowód: akta kontroli str. 306-307)

1.8. Według biegłego, w GOPS nie przewidziano zdalnego dostępu do zasobów sieci lokalnej przez pracowników, nie mówiły też o tym wewnętrzne regulacje. Do zarządzania siecią administrator używał szyfrowanego tunelu połączonego z siecią Urzędu Gminy Sztabin. (dowód: akta kontroli str. 324-327)

1.9. W umowie serwisowej dotyczącej oprogramowania kadrowo-płacowego zawarta została gwarancja zachowania poufności oraz opisane zostały warunki, jakie musi spełniać wykonawca (Centrum Informatyki ZETO). Oprogramowanie do bieżącej pracy pracowników socjalnych było przekazane GOPS przez Urząd Wojewódzki w 1997 roku. Ośrodek nie był stroną tej umowy. (dowód: akta kontroli str. 276-281, 287-290, 328-345)

1.10. Każdy z komputerów wchodzących w skład sieci lokalnej, jak stwierdził biegły, był zabezpieczony oprogramowaniem antywirusowym. Badane komputery posiadały aktualne wersje aplikacji zabezpieczających. Dostęp do sieci lokalnej kontrolowany był przez profesjonalny firewall sprzętowy połączony z funkcją IPS[9]. Kontrola działania i bezpieczeństwo komputerów realizowana była przez aplikację Desktop Central, która pozwalała na analizę logów pochodzących z różnych źródeł. Biegły uznał, że właściwe było zabezpieczenie dostępu do sieci i bezpieczeństwo urządzeń pracujących w sieci.

(dowód: akta kontroli str. 324-327)

---

[7] Log (inaczej: dziennik, plik dziennika, rejestr zdarzeń) – chronologiczny zapis zawierający informację o zdarzeniach i działaniach dotyczących systemu informatycznego, systemu komputerowego czy komputera. Log tworzony jest automatycznie przez dany program komputerowy, a sama czynność zapisywania do logu nazywana jest też logowaniem – nie należy mylić tego określenia z logowaniem w celu wykonania uwierzytelnienia. https://pl.wikipedia.org/wiki/Log_(informatyka)

[8] Desktop Central to zintegrowane oprogramowanie do zdalnego centralnego zarządzania stacjami roboczymi – serwer aplikacji posadowiony jest na terenie Urzędu Gminy Sztabin, a komunikacja odbywa się poprzez zestawiony VPN. Desktop Central pozwala na automatyzację między innymi takich działań jak instalacja poprawek, dystrybucja oprogramowania, zarządzanie zasobami IT, zarządzanie licencjami oprogramowania, monitorowanie statystyk wykorzystywania oprogramowania czy zarządzanie wykorzystywaniem urządzeń USB.

[9] Intrusion Prevention System – ochrona przed włamaniami.

365

1.11. Ośrodek nie był stroną umowy z dostawcą usług pocztowych – umowę zawarł Urząd Gminy Sztabin i korzystał z adresu pocztowego @sztabin.ug.gov.pl. Taką domenę pocztową udostępnił GOPS. Na siedmiu (z ośmiu) komputerach dostęp do służbowej skrzynki e-mailowej zapewniony był poprzez oprogramowanie Mozilla Thunderbird. Jeden z pracowników nie miał adresu e-mailowego. (dowód: akta kontroli str. 5-15, 312-315)

1.12. Według Instrukcji zarządzania systemem informatycznym[10], kopie zapasowe powinny być tworzone w cyklach miesięcznych i zapisywane na dyskietkach, płytach CD lub DVD (§ 9). Dane z każdego komputera były poddawane procesowi tworzenia kopii zapasowych, z większą częstotliwością niż to wynikało z wewnętrznych uregulowań oraz z zastosowaniem nowocześniejszych form przechowywania. W przypadku pięciu z nich (gdzie użytkowano oprogramowanie zawierające dane osobowe) raz w tygodniu wykonywany był obraz systemu na dysk sieciowy. Wskazane przez użytkowników foldery na ich komputerach backupowane były na bieżąco w tle. Komputer głównej księgowej, poza powyższymi rozwiązaniami, miał wykonywaną dodatkową kopię na macierz dyskową. Dwa komputery Kierownik Ośrodka, na których nie było zainstalowanego oprogramowania z danymi osobowymi, miały wykonywaną kopię zapasową wytworzonych dokumentów (działanie w tle). Kopie były przechowywane w siedzibie GOPS (o czym będzie mowa w dalszej części wystąpienia, w sekcji *Ustalone nieprawidłowości)* i testowane raz na kwartał – wewnętrzne procedury nie określały częstotliwości testowania. Wystąpiła konieczność odtworzenia zbioru danych z kopii zapasowej i według informatyka Urzędu Gminy Sztabin – wszystkie dane zostały przywrócone. Zbędne kopie bezpieczeństwa były niszczone przez ich nadpisanie przez kolejne.
(dowód: akta kontroli str. 5-15, 308-310, 324-327)

1.13. Jak ustalił biegły, pracownicy GOPS mieli możliwość ściągania aplikacji i plików wykonalnych oraz instalowania ich na komputerach. Dodatkowo na trzech komputerach, które współdzieliły swoje zasoby w sieci i na komputerze głównej księgowej, pracownicy – z racji pracy na koncie administratora – posiadali pełne uprawnienia do zarządzania swoim komputerem, co przedstawiono w dalszej części wystąpienia, w sekcji *Ustalone nieprawidłowości.* W pozostałych czterech przypadkach uprawnienia użytkowników na to nie pozwalały. Nie prowadzono ewidencji zainstalowanego oprogramowania, co szerzej omówiono w punkcie 3.2. (dowód: akta kontroli str. 324-327)

1.14. Wszystkie zbadane przez biegłego komputery posiadały aktualne wersje systemów operacyjnych. Aktualizacje były wykonywane zgodnie z harmonogramem, domyślnie ustawionym przez dostawcę systemu operacyjnego. (dowód: akta kontroli str. 324-327)

1.15. Płatności drogą elektroniczną wykonywane były za pomocą dedykowanej aplikacji, udostępnionej przez bank. Użytkownik komputera, na którym wykonywane były takie operacje, miał uprawnienia administratora. Nie określono w wewnętrznych przepisach sposobu dokonywania płatności drogą elektroniczną. Główna księgowa GOPS wyjaśniła, że realizując płatności drogą elektroniczną, po wybraniu z bazy danych klienta sprawdza poprawność konta bankowego z dowodem księgowym, a następnie raz jeszcze sprawdza te dane przed wysłaniem przelewu. Po wykonaniu płatności sprawdzana była też historia przelewów zrealizowanych. (dowód: akta kontroli str. 5-15, 246-275, 304)

Ustalone nieprawidłowości

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

1. Kierownik GOPS nie przeprowadzała okresowych analiz ryzyka utraty integralności, dostępności lub poufności informacji. Pierwsza taka analiza wykonana została w maju 2017 roku. Konieczność przeprowadzania takich analiz wynika z § 20 ust. 2 pkt 3 rozporządzenia KRI i obowiązuje od 31 maja 2012 r. Wprawdzie przytoczony przepis nie określa częstotliwości przeprowadzania tych analiz, jednak nastąpiło aż pięcioletnie zaniechanie ich wykonania. Tymczasem zagrożenia utraty integralności, dostępności lub

[10] Pełna nazwa: Instrukcja określająca sposób zarządzania systemem informatycznym służącym do przetwarzania danych osobowych w Gminnym Ośrodku Pomocy Społecznej w Sztabinie.

poufności informacji – przy ciągle rozwijającej się technologii, w tym również nowych zagrożeniach bezpieczeństwa danych – mogą pojawiać się bardzo często.
(dowód: akta kontroli str. 155-181, 351)

Kierownik GOPS wyjaśniła, że miała świadomość potrzeby wykonania tej analizy, ale nie wiedziała jak ma to zrobić. Gdy zaczęła poszukiwać podpowiedzi w Internecie, znalazła odpowiedni formularz do jej przeprowadzenia. Stało się to dopiero w maju 2017 roku, gdyż wcześniej miała wiele innych spraw zawodowych i tę analizę odkładała na później.
(dowód: akta kontroli str. 352-356)

2. Monitory dwóch (z ośmiu) komputerów pracowników Ośrodka były ustawione w sposób umożliwiający osobom postronnym odczytanie wyświetlanych danych osobowych klientów Ośrodka. Było to działanie nierzetelne, które nie zapewniało właściwej ochrony przetwarzanych danych osobowych oraz niezgodne z art. 36 ust. 1 ustawy o ochronie danych osobowych. Jednocześnie trzy kolejne monitory wprawdzie były ustawione równoległe lub pod małym kątem do kierunku padania wzroku klientów GOPS, jednak dla pełnego zabezpieczenia wyświetlanych danych należałoby rozważyć montaż filtrów maskujących pokazywaną treść. (dowód: akta kontroli str. 5-15)

   Kierownik Ośrodka wyjaśniła, że była niekonsekwentna w egzekwowaniu od pracowników obowiązków zachowania właściwej ochrony danych. Pracownicy dla własnej wygody ustawili swoje biurka w taki sposób, że było widać informacje wyświetlane na monitorze.
(dowód: akta kontroli str. 352-356)

   W trakcie kontroli NIK zostało zmienione ustawienie biurek w taki sposób, że dane wyświetlane na dwóch wspomnianych monitorach nie były już widoczne dla klientów GOPS, a do trzech kolejnych zamontowano filtry maskujące.
(dowód: akta kontroli str. 348-350)

3. Elektroniczne zasoby informacyjne GOPS, według opinii biegłego informatyka, nie były wystarczająco chronione przed nieuprawnionym dostępem, przejęciem lub zniszczeniem danych.
   - Użytkownicy czterech (z ośmiu) komputerów pracowali w systemie operacyjnym z uprawnieniami administratora, co według biegłego informatyka znacznie podwyższało niebezpieczeństwo niekontrolowanej utraty danych z tych urządzań. Według biegłego należałoby rozważyć przeorganizowanie systemu, które pozwoliłoby na uniknięcie konieczności pracy czterech komputerów na koncie administratora. Stosownie do § 20 ust. 2 pkt 4 rozporządzenia KRI, 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.
   - Kopie zapasowe dwóch (z ośmiu) komputerów przechowywane były w tym samym pomieszczeniu co backupowane urządzenia. Było to niezgodne 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 baza danych i jej kopia zapasowa.
   - Logi z poszczególnych komputerów nie były zabezpieczone przed usunięciem lub utratą i były analizowane incydentalnie, w sposób ręczny. 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.
(dowód: akta kontroli str. 5-15, 324-327)

   Kierownik Ośrodka wyjaśniła, że odnośnie uprawnień administratora na czterech komputerach – informatyk musiał przyznać takie uprawnienia, aby właściwie działały programy dziedzinowe. Dodała, że podejmowane były próby innego rozwiązania

367

technicznego, ale nie wiadomo czy będą skuteczne. Odnośnie kopii bezpieczeństwa wyjaśniła, że po zakupieniu nowoczesnego urządzenia magazynującego dane odstąpiono od składowania kopii na płytach CD/DVD w innym budynku, bo było to niewygodne, ale podejmowane są działania aby wdrożyć inną procedurę tworzenia i składowania kopii bezpieczeństwa. (dowód: akta kontroli str. 352-356)

Ocena cząstkowa

Najwyższa Izba Kontroli ocenia negatywnie 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 osobowych

Opis stanu faktycznego

2.1. Do Generalnego Inspektora Ochrony Danych Osobowych (dalej: *GIODO*) zostały zgłoszone następujące zbiory danych:

- opieka społeczna – zasiłki – zgłoszony 7 lipca 1999 r.,
- świadczenia rodzinne – dodatki mieszkaniowe – zgłoszony 7 lipca 1999 r.,
- świadczenia rodzinne – stypendia – zgłoszony 22 kwietnia 2010 r.,
- świadczenia rodzinne – alimentacyjne – zgłoszony 22 kwietnia 2010 r.,
- świadczenia rodzinne – zgłoszony 20 sierpnia 2010 r.,
- przeciwdziałanie przemocy w rodzinie – zgłoszony 25 lipca 2011 r.

Zgłoszeń dokonywał pracownik Urzędu Gminy Sztabin. We wszystkich zgłoszeniach jako administratora danych wskazano Gminę Sztabin wraz z jej numerem REGON i adresem. Pięć zgłoszeń zawierało wszystkie wymagane elementy, w jednym zaś wskazano, że dane mogą być udostępniane innym podmiotom niż uprawnione do tego na podstawie przepisów prawa, bez wskazania tych podmiotów. O zgłaszaniu zbiorów GIODO i nieaktualizowaniu danych w zbiorach będzie mowa w dalszej części wystąpienia, w sekcji *Ustalone nieprawidłowości.* (dowód: akta kontroli str. 17-34, 351)

Według danych przedstawionych przez Kierownik Ośrodka (nie był prowadzony oddzielny rejestr), w GOPS prowadzone były następujące zbiory danych osobowych:

- świadczenia rodzinne,
- fundusz alimentacyjny,
- świadczenia wychowawcze,
- pomoc społeczna,
- dodatki mieszkaniowe,
- pomoc materialna o charakterze socjalnych (stypendia szkolne),
- przeciwdziałanie przemocy w rodzinie,
- Karta Dużej Rodziny – dostęp do bazy Gminy Sztabin,
- SEPI – dostęp do bazy Powiatowego Urzędu Pracy w Augustowie,
- empatia – dostęp do bazy MRPiPS. (dowód: akta kontroli str. 297-302)

2.2. Kierownik GOPS nie wyznaczyła administratora bezpieczeństwa informacji (dalej: *ABI*) – nie przewidywała tego Polityka bezpieczeństwa informacji (szerzej omówiona w punkcie 2.10.). Kierownik wyjaśniła, że nie miała odpowiedniej kadry, aby któregoś z pracowników powołać na stanowisko ABI. Dodała, że w październiku 2017 roku jedna z osób przeszła szkolenie na ABI i być może ona zostanie powołana na to stanowisko. W budżecie Ośrodka nie miała też środków finansowych na wynajęcie firmy zewnętrznej do pełnienia takich obowiązków. (dowód: akta kontroli str. 351-356)

2.3. W związku z niewyznaczeniem ABI, to na Kierownik Ośrodka, będącej administratorem danych osobowych (dalej: *ADO*), spoczywał obowiązek opracowania i aktualizowania dokumentacji opisującej przetwarzanie danych oraz środków technicznych i organizacyjnych, zapewniających ochronę przetwarzanych danych osobowych. Dokumentacja taka została opracowana i weszła w życie 1 kwietnia 2009 r., jako Zarządzenie Nr 12B/2009 Kierownika Gminnego Ośrodka Pomocy Społecznej w Sztabinie z dnia 1 kwietnia 2009 roku w sprawie wprowadzenia do użytkowania polityki

bezpieczeństwa informacji i instrukcji służących do przetwarzania danych osobowych w Gminnym Ośrodku Pomocy Społecznej w Sztabinie[11]. Szczegółowo zostanie to omówione w punkcie 2.10. wystąpienia. (dowód: akta kontroli str. 35-56)

Kierownik Ośrodka wyjaśniła, że przed przystąpieniem do pracy (zatrudnieniem) pracownik zapoznawał się z ustawą o ochronie danych osobowych, z dokumentami organizacyjnymi Ośrodka (polityka bezpieczeństwa informacji, regulamin organizacyjny, statut, instrukcje) a następnie podpisywał oświadczenie że zna te dokumenty i zobowiązuje się do ich stosowania. Pracownicy GOPS, którzy byli zatrudnieni przed objęciem stanowiska przez Kierownik Ośrodka – zapoznali się zarządzeniem w sprawie polityki bezpieczeństwa informacji i zostali zobligowani do zapoznawania się z ustawą o ochronie danych osobowych, gdy były w niej jakieś zmiany. Kierownik GOPS wywiązała się zatem z zadań określonych w art. 36a ust. 2 pkt 1 ustawy o ochronie danych osobowych – przypisanych ABI (z wyłączeniem sprawozdań). (dowód: akta kontroli str. 352-356)

2.4. Kierownik GOPS, stosownie do art. 39 ust. 1 ustawy o ochronie danych osobowych, prowadziła ewidencję osób upoważnionych do przetwarzania danych osobowych. Zawierała ona dane od 1 kwietnia 2009 r, a zatem od wydania zarządzenia w sprawie polityki bezpieczeństwa i instrukcji. W ewidencji tej zawarte zostały numery nadanych upoważnień wraz z ich datą, imieniem i nazwiskiem upoważnionego pracownika, zakresem upoważnienia (zawsze było to *„przetwarzanie danych osobowych klientów GOPS"*) oraz datą ustania upoważnienia, a zatem elementy określone w pkt 1 – 2 ww. normy prawnej. W ewidencji nie odnotowywano identyfikatora użytkownika systemów informatycznych, co przedstawiono w dalszej części wystąpienia, w sekcji *Ustalone nieprawidłowości.*
(dowód: akta kontroli str. 76)

Każdy z pracowników GOPS posiadał upoważnienie do przetwarzania danych osobowych klientów GOPS, odpowiadające zakresowi obowiązków i danymi, które przetwarzał. Nadała je Kierownik GOPS. Upoważnienia posiadali również pracownicy nieetatowi, np. asystent rodziny i pracownik zatrudniony na umowę zlecenie do obsługi programu Rodzina 500+.
(dowód: akta kontroli str. 3, 77-89)

W GOPS funkcjonował Regulamin ochrony danych osobowych. Stanowił on załącznik nr 6 do zarządzenia w sprawie polityki bezpieczeństwa i instrukcji. Regulamin ten określał zasady postępowania przy przetwarzaniu danych osobowych i prawa osób fizycznych, których dane osobowe przetwarzano, w tym w § 6 – obowiązki administratora danych dotyczące zapewnienia kontroli nad przetwarzanymi danymi.
(dowód: akta kontroli str. 48-53)

2.5. W okresie objętym kontrolą obowiązywała instrukcja w sprawie zabezpieczenia dokumentów zawierających dane osobowe, która wydana została przez Kierownik GOPS. Stanowiła ona załącznik nr 2 do zarządzenia w sprawie polityki bezpieczeństwa i instrukcji. Określała ona, że dokumenty zawierające dane osobowe mogą być przechowywane w wyznaczonych pomieszczeniach, zamykanych na czas nieobecności pracowników. Dokumenty nie mogą być pozostawiane niezabezpieczone, a obecność pracowników GOPS po godzinach pracy jest możliwa tylko za zgodą kierownika. Instrukcja ta nie była aktualizowana od czasu jej wprowadzenia w kwietniu 2009 roku.
(dowód: akta kontroli str. 38-39)

2.6. Pomimo, że Kierownik GOPS formalnie nie powołała administratora systemów informatycznych (obowiązku takiego nie nakładała Polityka bezpieczeństwa informacji ani Instrukcja zarządzania systemami informatycznymi, które szerzej omówiono w punkcie 2.10.), to jego zadania wykonywał informatyk Urzędu Gminy Sztabin[12]. Obsługę informatyczną Ośrodka miał wpisaną w zakresie obowiązków. Informatyk posiadał upoważnienie do przetwarzania danych osobowych klientów GOPS – wydane przez Kierownik Ośrodka oraz posiadał konto administratora w systemie operacyjnym każdego z użytkowanych komputerów GOPS. (dowód: akta kontroli str. 5-15, 88-89, 154)

---

[11] Zarządzenie zwane w dalszej części wystąpienia: *zarządzeniem w sprawie polityki bezpieczeństwa i instrukcji.*
[12] Referent ds. informatyzacji i pozamilitarnych ogniw obronnych oraz ochrony danych osobowych w Urzędzie Gminy Sztabin.

569

2.7. W okresie objętym kontrolą, Kierownik GOPS nie prowadziła corocznych audytów wewnętrznych z bezpieczeństwa informacji, co opisano w dalszej części wystąpienia, w sekcji *Ustalone nieprawidłowości*. Po rozpoczęciu kontroli NIK audyt taki przeprowadził informatyk Urzędu Gminy Sztabin. Wśród uchybień wskazał, że istniała rozbieżność pomiędzy stanem faktycznym a treścią instrukcji zarządzania systemami informatycznymi, odnośnie wykonywania kopii zapasowych (rozwiązania proceduralne były nieaktualne) oraz, że kopie zapasowe przechowywane były w tym samym miejscu co przebywający pracownicy. (dowód: akta kontroli str. 182-193, 351)

2.8. W latach 2016 – 2017 szkolenie z bezpieczeństwa informacji odbyła Kierownik GOPS (dla ADO) i jedna z pracownic (dla ABI). Miały one miejsce 27 października 2017 r. i związane były ze zmianą przepisów o ochronie danych osobowych, która ma wejść w życie 25 maja 2018 r. Wcześniej Kierownik odbyła (22 maja 2017 r.) kurs pt. Ochrona danych osobowych. Pozostali pracownicy nie byli szkoleni w okresie objętym kontrolą w temacie bezpieczeństwa informacji, co przedstawiono w dalszej części wystąpienia, w sekcji *Ustalone nieprawidłowości*. (dowód: akta kontroli str. 194-196, 305, 351-356)

Kierownik GOPS wyjaśniła, że w 2018 roku planuje kierować sukcesywnie pozostałych pracowników na szkolenia z tej tematyki. (dowód: akta kontroli str. 352-356)

2.9. W latach 2016 – 2017[13] GOPS nie był objęty kontrolą dotyczącą zapewnienia bezpieczeństwa elektronicznych zasobów informacyjnych i nie wpływały do niego skargi w tym zakresie. (dowód: akta kontroli str. 4)

2.10. Kierownik GOPS 1 kwietnia 2009 r. wydała zarządzenie w sprawie polityki bezpieczeństwa i instrukcji. Składało się ono z poniżej omówionych dokumentów.

Polityka bezpieczeństwa przetwarzanych danych osobowych (dalej: *PBI*, załącznik nr 1 do zarządzenia) nie zawierała większości elementów wskazanych w rozporządzeniu MSWiA. Instrukcja zarządzania systemem informatycznym służącym do przetwarzania danych osobowych (załącznik nr 3) nie uwzględniała zmian technologicznych lub była nieprecyzyjna, co opisano w dalszej części wystąpienia, w sekcji *Ustalone nieprawidłowości*.

Wprawdzie PBI nie zawierała określenia środków technicznych i organizacyjnych niezbędnych dla zapewnienia poufności, integralności i rozliczalności przetwarzanych danych, to opracowane były inne dokumenty regulujące te kwestie:

- regulamin ochrony danych osobowych (załącznik nr 6 do zarządzenia w sprawie polityki bezpieczeństwa i instrukcji, opisany w punkcie 2.4),
- instrukcja postępowania w sytuacji naruszenia ochrony danych osobowych (załącznik nr 4 do zarządzenia w sprawie polityki bezpieczeństwa i instrukcji),
- instrukcja w sprawie zabezpieczenia dokumentów zawierających dane osobowe (załącznik nr 2 do zarządzenia w sprawie polityki bezpieczeństwa i instrukcji),
- instrukcja w sprawie określenia procedury postępowania z kluczami oraz zabezpieczenia pomieszczeń w lokalach Gminnego Ośrodka Pomocy Społecznej w Sztabinie (załącznik nr 2 do regulaminu organizacyjnego Ośrodka),

Ponadto każdy z pracowników GOPS podpisywał dokument pt. *zasady regulujące korzystanie z oprogramowania w Gminnym Ośrodku Pomocy Społecznej w Sztabinie*.
(dowód: akta kontroli str.35-56, 72-73)

W żadnym z ww. dokumentów nie określono poziomu bezpieczeństwa przetwarzania danych osobowych w systemach informatycznych GOPS, mimo takiego wymogu określonego w § 6 ust. 1 rozporządzenia w sprawie dokumentacji oraz warunków technicznych, 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. Przyjęte rozwiązania opisane w PBI i w Instrukcji zarządzania systemem informatycznym dotyczyły wyłącznie ochrony danych osobowych, co opisano poniżej, w sekcji *Ustalone nieprawidłowości*. (dowód: akta kontroli str. 351)

---

[13] Do 15 grudnia 2017 r.

Ustalone nieprawidłowości

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

1. Kierownik GOPS nie zaktualizowała zbiorów danych osobowych zarejestrowanych w GIODO (przed objęciem przez nią stanowiska) przez pracownika Urzędu Gminy Sztabin. Dotyczyło to dwóch zbiorów: opieka społeczna – zasiłki i świadczenia rodzinne – dodatki mieszkaniowe, które zgłoszono 7 lipca 1999 r. Zmiany wymagały informacje dotyczące administratora danych osobowych, którym wskazano Gminę Sztabin, a nie GOPS, wraz z poprawnym adresem i numerem REGON.

   Jednocześnie Kierownik Ośrodka nie zgłaszała GIODO kolejnych zbiorów (świadczenia rodzinne – stypendia i świadczenia rodzinne – alimentacyjne, zgłoszono 22 kwietnia 2010 r., świadczenia rodzinne – 20 sierpnia 2010 r., przeciwdziałanie przemocy w rodzinie – 25 lipca 2011 r.). Zbiory zgłaszał pracownik Urzędu Gminy Sztabin, wskazując Gminę Sztabin, a nie GOPS, jako administratora danych.
   (dowód: akta kontroli str. 17-34, 351)

   Obowiązek zgłoszenia zbiorów danych do rejestracji GIODO wynika z art. 40 ustawy o ochronie danych osobowych, a ich zmian z art. 41 ust. 2 tej ustawy.

   Kierownik GOPS wyjaśniła, że takie rozwiązanie było wypracowane zanim została kierownikiem, że fizycznie zbiory te rejestrował pracownik Urzędu Gminy Sztabin – robił to dla Urzędu i dla jednostek organizacyjnych Gminy. Przekazywała mu informacje, jakie zbiory należy rejestrować i takie były rejestrowane. Najwyraźniej uznał, że skoro Ośrodek nie ma osobowości prawnej, to rejestrował zbiory i wskazywał, że administratorem danych jest Gmina Sztabin. Nie przekazywała mu szczegółów odnośnie rejestrowanego zbioru, w tym kto jest administratorem danych osobowych – sądziła, że wie jak to robić. (dowód: akta kontroli str. 352-356)

2. Kierownik GOPS nie zaktualizowała w rejestrze GIODO zakresu danych gromadzonych w ramach danego zbioru. W Ośrodku gromadzono dane, których przetwarzanie nie zostało wskazane w zgłoszeniach rejestracji tych zbiorów do GIODO, ale dane te były niezbędne do realizacji zadań GOPS. Dotyczyło to wymienionych poniżej zbiorów i danych.
   - W zbiorze opieka społeczna – zasiłki, poza zgłoszonymi danymi gromadzono: numer NIP, obywatelstwo, stan cywilny, sytuację ekonomiczną, mieszkaniową, płeć, nazwisko rodowe, dane opiekuna prawnego / kuratora, kwalifikacje zawodowe, stopień pokrewieństwa, numer telefonu.
   - W zbiorze świadczenia rodzinne – dodatki mieszkaniowe, poza zgłoszonymi danymi gromadzono: numer PESEL, datę urodzenia, NIP, miejsce pracy, stopień pokrewieństwa, tytuł prawny do lokalu, dane o niepełnosprawności i dochodach.
   - W zbiorze świadczenia rodzinne – stypendia, poza zgłoszonymi danymi gromadzono: numer PESEL, datę urodzenia, numer telefonu, stan cywilny, stopień pokrewieństwa, dochody, pozycję na rynku pracy, dane o alimentach i niepełnosprawności.
   - W zbiorze świadczenia rodzinne – alimentacyjne, poza zgłoszonymi danymi gromadzono: dane o obywatelstwie, stanie cywilnym, statusie na rynku pracy, płci, dacie i miejscu urodzenia, dochodach, ubezpieczeniu zdrowotnym, numerze konta bankowego.
   - W zbiorze danych świadczenia rodzinne, poza zgłoszonymi danymi gromadzono: numer PESEL, NIP, serię i numer dowodu osobistego, obywatelstwo, stan cywilny orzeczenia o niepełnosprawności, zobowiązania alimentacyjne, status na rynku pracy, płeć, datę urodzenia, miejsce urodzenia, dochody, ubezpieczenie zdrowotne, numer konta bankowego.
   - W zbiorze przeciwdziałanie przemocy w rodzinie, poza zgłoszonymi danymi gromadzono: stan cywilny, źródło utrzymania, dane o sytuacji ekonomicznej, mieszkaniowej i rodzinnej.

571

Obowiązek dokonywania zmian w zgłoszonych zbiorach wynikał z art. 41 ust. 2 ustawy o ochronie danych osobowych. (dowód: akta kontroli str. 297-303)

Kierownik GOPS wyjaśniła, że zbierane są niezbędne dane, chociaż nie zostały one wskazane w rejestrze GIODO. Zakres zbieranych danych wynikał z informacji, które zostały podane przez klientów Ośrodka we wnioskach o przyznanie świadczeń, w trakcie wywiadu środowiskowego lub które zostały przekazane przez inne instytucje. Gdy pracownik Urzędu Gminy Sztabin zgłaszał te zbiory, to wybierał z listy dostępnych danych – które z nich będą przez Ośrodek gromadzone i zrobił to nieprecyzyjnie.
(dowód: akta kontroli str. 352-356)

3. Kierownik GOPS nie zgłosiła do rejestracji GIODO zbioru danych osobowych (prowadzonego od 1 kwietnia 2016 r. tj. od dnia wejścia w życie ustawy z dnia 11 lutego 2016 r. o pomocy państwa w wychowywaniu dzieci[14]), zawierającego klientów Ośrodka korzystających ze świadczeń wychowawczych (program Rodzina 500+). Obowiązek takiego zgłoszenia wynikał z art. 40 ustawy o ochronie danych osobowych.
(dowód: akta kontroli str. 351)

   Kierownik GOPS wyjaśniła, że gdy ruszał program Rodzina 500+ była na zwolnieniu lekarskim i nie mogła zgłosić zbioru przed rozpoczęciem tego programu, natomiast po powrocie do pracy nie pamiętała, że należy ten zbiór zgłosić.
(dowód: akta kontroli str. 352-356)

4. W prowadzonej przez Kierownik GOPS ewidencji osób upoważnionych do przetwarzania danych osobowych:
   - Nie były podane identyfikatory użytkowników siedmiu pracowników Ośrodka, którzy przetwarzali dane w dwóch systemach informatycznych (dotyczyło to pracowników etatowych poza Kierownik GOPS, która nie korzystała z systemów informatycznych). Obowiązek wskazania w ewidencji identyfikatorów użytkowników wynika z art. 39 ust. 1 pkt 3 ustawy o ochronie danych osobowych. Ponadto w zakresach obowiązków pracowników nie wskazano do jakich systemów informatycznych mają dostęp poszczególni pracownicy. (dowód: akta kontroli str. 5-15, 76, 93-153)
   - Nie był uwzględniony informatyk Urzędu Gminy Sztabin, realizujący część swoich obowiązków służbowych w Ośrodku, mimo że miał upoważnienie do przetwarzania danych osobowych klientów GOPS. (dowód: akta kontroli str. 76, 88-89)

   Kierownik GOPS wyjaśniła, że nie wiedziała, że w ewidencji należy zawrzeć identyfikator użytkownika. Nie widziała też powodu, aby w zakresach obowiązków pracowników wpisać do jakich programów mają dostęp. W kwestii ujęcia w ewidencji informatyka Urzędu Gminy Sztabin dodała, że w ewidencji wpisała osoby, których zatrudnienie wynikało ze stosunku pracy lub innych umów. Informatyk nie jest pracownikiem Ośrodka, wykonuje tylko pewne obowiązki, jako informatyk Urzędu Gminy Sztabin, wynikające z zakresu czynności, dlatego nie ma go w ewidencji.
(dowód: akta kontroli str. 352-356)

5. Jedynie dwóch z ośmiu pracowników Ośrodka przeszkolono z zagrożeń bezpieczeństwa informacji. 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.
(dowód: akta kontroli str. 194-196, 305, 351)

   Kierownik GOPS wyjaśniła, że nie sądziła, że należy przeszkolić wszystkich pracowników. (dowód: akta kontroli str. 352-356)

6. PBI nie zawierała czterech z pięciu elementów wskazanych w § 4 rozporządzenia MSWiA, tj.:
   - wykazu zbiorów danych osobowych wraz ze wskazaniem programów zastosowanych do przetwarzania tych zbiorów (§ 4 pkt 2 rozporządzenia),

[14] Dz. U. z 2017 r. poz. 1851, ze zm.

- opisu struktury zbiorów danych wskazujący zawartość poszczególnych pól informacyjnych i powiązania między nimi – nie była opracowana taka struktura (§ 4 pkt 3 rozporządzenia),
- sposobu przepływu danych pomiędzy poszczególnymi systemami (§ 4 pkt 4 rozporządzenia),
- wykazu budynków, pomieszczeń lub części pomieszczeń, tworzących obszar, w którym przetwarzane są dane osobowe (§ 4 pkt 1 rozporządzenia) – w polityce mowa była tylko o ogólnych zasadach postępowania; wykaz budynków (nieaktualny) został zaś wskazany w instrukcji zarządzania systemami informatycznymi,
- po otrzymaniu przenośnego sprzętu do obsługi klientów GOPS poza siedzibą, w PBI nie zostały dodane zapisy odnoszące się do zasad korzystania z tego narzędzia.

(dowód: akta kontroli str. 36-37, 74-75)

Kierownik GOPS wyjaśniła, że PBI nie zawierała różnych danych, gdyż nie wiedziała, że musi ona je zawierać. Odnośnie niezaktualizowania PBI o zapisy dotyczące użytkowania notebooka poza siedzibą GOPS dodała, że Ośrodek ma możliwość wyboru – czy będzie sporządzał wywiad środowiskowy w formie papierowej czy elektronicznej. Stosujemy formę papierową. Nikt nie korzysta z tego notebooka. Jeśli zdecydujemy się go używać poza Ośrodkiem, wówczas stworzone zostaną zasady jego użytkowania w terenie. Obecnie nie są potrzebne. (dowód: akta kontroli str. 352-356)

NIK zwraca jednak uwagę, że w założeniach projektu Emp@tia notebook miał służyć wyłącznie do pracy poza GOPS. W sytuacji, gdy pracownik Ośrodka chciałby go użyć na zewnątrz albo gdyby wynikła taka konieczność – należałoby stworzyć odpowiednio wcześniej zasady użytkowania tego sprzętu. Takie mechanizmy powinny być przygotowane z wyprzedzeniem, aby pracownicy GOPS mieli czas na zapoznanie się z nimi.

7. Instrukcja zarządzania systemami informatycznymi:
   a) nie zawierała sposobu realizacji wymogu zapisu danych o odbiorcach danych osobowych – jeśli zostały udostępnione na zewnątrz, tj. elementu wskazanego w § 5 pkt 7 rozporządzenia MSWiA;
   b) zapisy instrukcji były zbyt ogólne lub nieaktualne i nie regulowały zastosowania nowoczesnych środków technicznych:
      - nie zostało w niej wskazane, jaki poziom bezpieczeństwa został przyjęty w GOPS (§ 5 pkt 2 rozporządzenia),
      - nie ustalono procedur rozpoczęcia i zawieszenia pracy (§ 5 pkt 3 rozporządzenia), a jedynie procedurę zakończenia pracy,
      - wskazano, że kopie bezpieczeństwa systemów wykonywane są w cyklu miesięcznym i zapisywane na dyskietki, płyty CD i DVD, chociaż stosowane rozwiązanie, opisane w pkt. 1.12 jest nowocześniejsze, backup odbywał się codziennie dla plików dokumentów oraz raz w tygodniu obraz systemów, z zastosowaniem dysku sieciowego i zapisu w chmurze (§ 5 pkt 4 rozporządzenia),
      - nie opisano w szczegółach sposobu zabezpieczenia systemu informatycznego przed działalnością oprogramowania, którego celem jest uzyskanie nieuprawnionego dostępu do systemu informatycznego (§ 5 pkt 6 rozporządzenia),
      - nie opisano szczegółowych procedur wykonywania przeglądów systemów (§ 5 pkt 8 rozporządzenia). (dowód: akta kontroli str. 38-39, 74-75)

   Kierownik GOPS wyjaśniła, że Instrukcja Zarządzania Systemami Informatycznymi nie zawierała różnych danych albo precyzyjnych informacji, gdyż nie wiedziała, że muszą one być w niej zawarte. (dowód: akta kontroli str. 352-356)

8. Kierownik GOPS nie prowadziła corocznych audytów wewnętrznych z bezpieczeństwa informacji. Obowiązek taki wynikał z § 20 ust. 2 pkt 14 rozporządzenia KRI. Audyt został przygotowany w trakcie kontroli NIK. Kierownik wyjaśniła, że nie potrafiła wykonać

373

samodzielnie takiego audytu. Nie miała też środków finansowych na zlecenie audytu na zewnątrz. Informatyk z Urzędu Gminy Sztabin miał dużo obowiązków we wszystkich jednostkach organizacyjnych Gminy, więc nie zlecała mu takiego audytu. Dopiero podczas kontroli stwierdzili wspólnie, że należy go jednak wykonać.
(dowód: akta kontroli str. 351-356)

9. W Ośrodku nie wprowadzono regulacji składających się na politykę bezpieczeństwa informacji, o której mowa w § 2 pkt 15, spełniającej wymogi § 20 ust. 1 rozporządzenia KRI, a rozwiązania opisane w PBI i w Instrukcji zarządzania systemem informatycznym dotyczyły jedynie ochrony danych osobowych. Kierownik GOPS wyjaśniła, że nie wiedziała, że musi taki dokument opracować. (dowód: akta kontroli str. 351-356)

Ocena cząstkowa

Najwyższa Izba Kontroli ocenia pozytywnie, mimo stwierdzonych nieprawidłowości, opracowanie dokumentacji i procedur dotyczących ochrony danych osobowych w GOPS.

3. Sposób przechowywania zasobów informacyjnych oraz ich zabezpieczenia

Opis stanu faktycznego

3.1. W PBI określono środki ochrony służące zapewnieniu poufności, integralności i rozliczalności danych. Przyjęte rozwiązania w sposób ogólny określały środki ochrony fizycznej, wskazując m.in., że: (1) dokumenty i systemy informatyczne służące do przetwarzania danych osobowych mogą być przechowywane wyłącznie w przeznaczonych do tego pomieszczeniach, (2) wyznaczone pomieszczenia muszą gwarantować prawidłową ich ochronę i zabezpieczenie przed wglądem osób nieupoważnionych, (3) pomieszczenia te po zakończeniu pracy powinny być skontrolowane przez ostatniego opuszczającego je pracownika, czy nie zostały niezabezpieczone dokumenty, (4) przebywanie w tych pomieszczeniach poza godzinami pracy możliwe jest tylko za zgodą Kierownika, a osoby nieupoważnione mogą przebywać w tych pomieszczeniach wyłącznie w obecności osób uprawnionych do przetwarzania danych osobowych. (dowód: akta kontroli str. 36-37)

Budynek, w którym mieści się Ośrodek był jednopiętrowy (dwupoziomowy). Na parterze znajdowała się przychodnia medyczna, a pomieszczenia GOPS na pierwszym piętrze. Na tym samym poziomie znajdowało się prywatne mieszkanie, wynajmowane jednej z rodzin przez Wójta z zasobów Gminy Sztabin. Według stanu na dzień kontroli, mieszkanie miało zostać opuszczone do 1 marca 2018 r., a pomieszczenia przekazane GOPS w celu realizacji zadań statutowych. (dowód: akta kontroli str. 197-201)

Nie została zapewniona ochrona pomieszczeń, sprzętów, infrastruktury przed bezpośrednim działaniem czynników fizycznych i zdarzeń losowych, co opisano w dalszej części wystąpienia, w sekcji *Ustalone nieprawidłowości.*

Załącznikiem nr 2 do Regulaminu Organizacyjnego GOPS była *Instrukcja w sprawie określenia procedury postępowania z kluczami oraz zabezpieczenia pomieszczeń w lokalach Gminnego Ośrodka Pomocy Społecznej w Sztabinie*, zwana dalej *polityką kluczy*. Według niej:

- klucze do poszczególnych pokojów były w posiadaniu pracowników – prowadzony był rejestr udostępnionych kluczy,
- kluczy do pokojów nie można było przekazywać innym osobom, a pomieszczenia służbowe, w których chwilowo nie przebywał żaden pracownik powinny być zamknięte na klucz,
- klucze do biurek stanowiskowych, szaf biurowych oraz sejfu były w posiadaniu pracowników, którzy ponoszą pełną odpowiedzialność za ich należyte zabezpieczenie.

Klucze do drzwi wejściowych do części budynku zajmowanych przez GOPS były w posiadaniu Kierownik Ośrodka oraz czterech innych pracowników. Powierzenie tych kluczy również było udokumentowane. Klucze do biurek, szaf z dokumentami klientów faktycznie przechowywane były w sejfie, w pokoju Kierownik Ośrodka.
(dowód: akta kontroli str. 197-199, 226-236)

3.2. Kierownik Ośrodka nie prowadziła rejestru zasobów informatycznych, czyli inwentaryzacji sprzętu i oprogramowania służącego do przetwarzania informacji, obejmującej rodzaj i konfigurację. Problem opisano w dalszej części wystąpienia, w sekcji *Ustalone nieprawidłowości.* (dowód: akta kontroli str. 351)

3.3. W okresie objętym kontrolą nie dokonywano likwidacji sprzętu komputerowego i nie zlecano bieżących napraw na zewnątrz – przeprowadzał je informatyk Urzędu Gminy Sztabin. W sejfie w pokoju Kierownik GOPS przechowywanych było dziewięć dysków z komputerów zlikwidowanych we wcześniejszych latach – do likwidacji były przekazywane komputery bez dysków. (dowód: akta kontroli str. 197-199, 237-242, 351)

3.4. Niszczenie dokumentów papierowych odbywało się na trzech niszczarkach. Miały one również funkcję niszczenia płyt CD/DVD. Kwestia ta nie była uregulowana w PBI. (dowód: akta kontroli str. 5)

3.5. W Ośrodku nie były opracowane wewnętrzne regulacje dotyczące korzystania ze sprzętu informatycznego poza GOPS. Była o tym mowa w sekcji *Ustalone nieprawidłowości,* w punkcie 2 wystąpienia. Ośrodek otrzymał z Ministerstwa Pracy i Polityki Społecznej (obecnie Ministerstwo Rodziny Pracy i Polityki Społecznej) notebook z projektu Emp@tia do pracy w terenie. Na dzień kontroli nie był on wykorzystywany. (dowód: akta kontroli str. 5, 35-56, 351)

3.6. Sprzątanie pomieszczeń było powierzone osobie zatrudnionej na umowę zlecenie. Posiadała ona wydaną 3 lipca 2017 r. przez kierownik GOPS zgodę na przebywanie w obszarze przetwarzania danych osobowych. Wcześniej takiej zgody nie posiadała, chociaż usługi świadczyła od 2 marca 2015 r. Według § 4 ust. 2 polityki kluczy – sprzątanie gabinetu Kierownik Ośrodka, pokoju księgowej oraz składnicy akt może odbywać się wyłącznie w godzinach pracy GOPS, w obecności pracownika i tak było wykonywane. (dowód: akta kontroli str. 90-92, 226-228)

3.7. Nie zostały opracowane szczegółowe procedury wykonywania przeglądów i konserwacji systemów i nośników informacji. Instrukcja określająca sposób zarządzania systemem informatycznym służącym do przetwarzania danych osobowych w GOPS (stanowiąca załącznik nr 3 do zarządzenia w sprawie polityki bezpieczeństwa i instrukcji) w § 11 ogólnie określała, że: *konserwacje i przeglądy odbywają się przy wyłączonych komputerach tak, aby zgromadzone dane nie zostały zniszczone lub odczytane przez niepowołane osoby*. Była już o tym mowa w punkcie 2.10 wystąpienia oraz w opisie nieprawidłowości w obszarze 2. (dowód: akta kontroli str. 40-43)

3.8. Każdy z komputerów stacjonarnych GOPS był wyposażony w bezprzewodowy zasilacz awaryjny (urządzenie UPS), podtrzymujący energię na wypadek braku zasilania. Umożliwiało to zapisanie danych w użytkowanych programach i poprawne wyłączenie programów i sprzętu w przypadku przerw w zasilaniu. GOPS nie posiadał własnego agregatu prądotwórczego. (dowód: akta kontroli str. 5)

3.9. Kierownik GOPS wyjaśniła, że nie zdarzyło się w okresie objętym kontrolą, aby utracono dane w wyniku kradzieży nośnika, przekazania go nieuprawnionej osobie, przypadkowego skasowania lub zniszczenia. (dowód: akta kontroli str. 352-356)

Ustalone nieprawidłowości

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

1. Budynek GOPS oraz dane klientów nie były właściwie zabezpieczone. Pięć z 16 (31%) szaf, w których przechowywane były dane osobowe klientów Ośrodka w formie papierowej, nie posiadało zamków. Było to działanie niezapewniające należytej ochrony gromadzonych dokumentów, zawierających również dane wrażliwe oraz niezgodne z art. 36 ust. 1 ustawy o ochronie danych osobowych. Brakujące zamki wstawiono w trakcie kontroli NIK.

   NIK zwraca też uwagę, że na stan zabezpieczeń budynku i pomieszczeń GOPS wpływało współdzielenie piętra budynku z prywatnym mieszkaniem – co ograniczało np. możliwość zamknięcia całej klatki schodowej w godzinach wieczornych oraz w weekendy. Poza tym,

375

dla lepszej ochrony danych, klucze do pokojów powinny być składowane w skrzynce na klucze. Zdaniem NIK, mechanizmy kontrolne łagodzą potencjalne ryzyko uszkodzenia urządzeń, a tym samym minimalizują przerwy w działaniu.
(dowód: akta kontroli str. 197-201)

Kierownik GOPS wyjaśniła, że trzy szafy wcześniej były użytkowane do innego celu i nie było potrzeby ich zamykania. W jednej z szaf rozsuwanych zamki były kiepskiej jakości i odpadły, a druga tego typu szafa była stosunkowo nowa i nie została wykonana z zamkami. Kierownik dodała, że planowała wstawić zamki w tych szafach przy okazji wykonania innych mebli biurowych w Ośrodku. Odnośnie stanu budynku, Kierownik wyjaśniła, że taki stan rzeczy zastała w 2008 roku, gdy została kierownikiem. Właścicielem budynku jest Gmina Sztabin i Kierownik GOPS nie ma wpływu na ten stan. Współdzielenie piętra z wynajmowanym mieszkaniem uniemożliwia zastosowanie alarmu. (dowód: akta kontroli str. 352-356)

2. Kierownik Ośrodka nie prowadziła rejestru zasobów informatycznych. Było to niezgodne z § 20 ust. 2 pkt 2 rozporządzenia KRI, zgodnie z którym zarządzanie bezpieczeństwem informacji odbywa się m.in. poprzez aktualną inwentaryzację sprzętu i oprogramowania służącego do przetwarzania informacji obejmującą ich rodzaj i konfigurację. Informacje te są niezbędne przy wprowadzaniu zmian w środowisku teleinformatycznym GOPS, ograniczając możliwość zaistnienia zakłóceń w pracy, które wynikłyby z błędnych decyzji i podejmowanych działań, wynikających z niewiedzy o aktualnej i kompleksowej wiedzy o stanie infrastruktury teleinformatycznej. (dowód: akta kontroli str. 351)

Kierownik Ośrodka wyjaśniła, że nie wiedziała o takim obowiązku, a poza tym nie potrafi zrobić takiego rejestru. (dowód: akta kontroli str. 352-356)

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 Ośrodka. (dowód: akta kontroli str. 5, 351)

Kierownik GOPS wyjaśniła, że nie uznała, że taki plan jest konieczny do opracowania. W przypadku długotrwałego braku zasilania można podłączyć agregat prądotwórczy, będący w posiadaniu Ochotniczej Straży Pożarnej. Agregaty takie Gmina zakupiła przed kilkoma laty i przekazała OSP. (dowód: akta kontroli str. 352-356)

Ocena cząstkowa

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

4. Zakres przetwarzanych danych osobowych

Opis stanu faktycznego

4.1. Zbiory danych osobowych wymienione w punkcie 2.1 prowadzone były zarówno w postaci papierowej jak i elektronicznej w oprogramowaniu dziedzinowym. Do GIODO, zgodnie z art. 43 ust. 1 ustawy o ochronie danych osobowych, nie zgłoszone zostały zbiory związane z zatrudnieniem (rejestr osób ubezpieczonych prowadzony w Płatniku a zatrudnienie – w programie Kadry i płace) oraz będące w posiadaniu GOPS wyłącznie do celu wystawienia faktury (rejestr VAT). (dowód: akta kontroli str. 5-15, 243-245, 297-302)

4.2. W okresie objętym kontrolą nie aktualizowano danych w rejestrze prowadzonym przez GIODO, co szerzej opisano w sekcji *Ustalone nieprawidłowości* obszaru nr 2.
(dowód: akta kontroli str. 351)

4.3. Zakres danych zbieranych przez GOPS wynikał z informacji, jakie podane zostały przez klientów Ośrodka we wnioskach o przyznanie świadczeń lub w trakcie wywiadu środowiskowego lub przekazane były przez inne instytucje. Nie stwierdzono przetwarzania danych zbędnych GOPS do realizacji swoich zadań. (dowód: akta kontroli str. 297-302)

W przypadku dwóch osób zatrudnionych w Ośrodku w okresie objętym kontrolą, jedna została zatrudniona na zastępstwo, a zatem bez ogłoszenia. W drugim przypadku w ogłoszeniu zawarte zostały informacje o konieczności wyrażenia zgody na przetwarzanie danych osobowych do przeprowadzenia procesu rekrutacji. (dowód: akta kontroli str. 347)

4.4. Ośrodek korzystał z zewnętrznych elektronicznych źródeł danych, których administratorami były zewnętrzne podmioty:

- Karta Dużej Rodziny[15] i baza danych projektu Emp@tia[16] – administrowane przez MRPiPS,
- system SEPI – administratorem był Powiatowy Urząd Pracy w Augustowie (dostęp do zbioru uzyskany na podstawie umowy z 26 stycznia 2010 r.). Pracownicy Urzędu Pracy nie mieli dostępu do danych GOPS.

Nie były ustalone szczegółowe wymagania dostępu do powyższych baz.

(dowód: akta kontroli str. 297-302)

Ustalone nieprawidłowości

W działalności kontrolowanej jednostki w przedstawionym wyżej zakresie nie stwierdzono nieprawidłowości.

Ocena cząstkowa

Najwyższa Izba Kontroli ocenia pozytywnie sposób przetwarzania zasobów informacyjnych, który był zgodny z zakresem działalności GOPS, a w odniesieniu do zbiorów zewnętrznych – spełniał wymogi związane z uzyskaniem do nich dostępu.

IV. Wnioski

Wnioski pokontrolne

Przedstawiając powyższe oceny i uwagi wynikające z ustaleń kontroli, Najwyższa Izba Kontroli, na podstawie art. 53 ust. 1 pkt 5 ustawy z dnia 23 grudnia 1994 r. o Najwyższej Izbie Kontroli[17], wnosi o:

1. Podjęcie działań w celu wyeliminowania nieprawidłowości wskazanych przez biegłego informatyka w zakresie ochrony elektronicznych zasobów informacyjnych.
2. Zaktualizowanie zbiorów danych osobowych zgłoszonych GIODO, poprzez wskazanie właściwego administratora tych danych oraz rozszerzenie zakresu gromadzonych informacji.
3. Zgłoszenie GIODO zbioru danych osobowych dotyczących klientów Ośrodka korzystających ze świadczeń wychowawczych.
4. Prowadzenie ewidencji osób upoważnionych do przetwarzania danych osobowych zgodnie z § 39 ust. 1 ustawy o ochronie danych osobowych oraz ujęcie w niej wszystkich osób upoważnionych do przetwarzania takich danych.
5. Zapewnienie szkoleń pracownikom Ośrodka zaangażowanym w proces przetwarzania informacji, stosownie do § 20 ust. 2 pkt 6 rozporządzenia KRI.
6. Zaktualizowanie Polityki Bezpieczeństwa Informacji i Instrukcji Zarządzania Systemami Informatycznymi, w tym uzupełnienie ich stosownie do wymogów § 20 ust. 1 rozporządzenia KRI oraz § 4 pkt 1 – 4, w § 5 pkt 2 – 7 i § 6 rozporządzenia MSWiA.
7. Prowadzenie corocznych audytów wewnętrznych z bezpieczeństwa informacji, przewidzianych w § 20 ust. 2 pkt 14 rozporządzenia KRI.
8. Wywiązanie się z obowiązku, o którym mowa w § 20 ust. 2 pkt. 2 rozporządzenia KRI, w zakresie utrzymywania aktualności inwentaryzacji sprzętu i oprogramowania służącego do przetwarzania informacji obejmującej ich rodzaj i konfigurację.

---

[15] Dostęp poprzez stronę internetową https://kdr.mpips.gov.pl/start/.
[16] Dostęp poprzez logowanie na stronie internetowej https://empatia.mpips.gov.pl/web/piu/dla-urzednikow.
[17] Dz. U. z 2017 r. poz. 524. Ustawa zwana dalej *ustawą o NIK*.

377

V. Pozostałe informacje i pouczenia

Prawo zgłoszenia zastrzeżeń

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

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

Obowiązek poinformowania NIK o sposobie wykorzystania uwag i wykonania wniosków

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

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

Białystok, 18 stycznia 2018 r.

Kontroler

Wojciech Zambrzycki
starszy inspektor kontroli państwowej

.....
podpis

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

.....
podpis