NAJWYŻSZA IZBA KONTROLI
Delegatura w Białymstoku

LBI.410.023.22.2017
P/17/062

00366618

WYSTĄPIENIE POKONTROLNE

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

I. Dane identyfikacyjne kontroli

Numer i tytuł kontroli	P/17/062 – Bezpieczeństwo elektronicznych zasobów informacyjnych w jednostkach samorządu terytorialnego w województwie podlaskim
Jednostka przeprowadzająca kontrolę	Najwyższa Izba Kontroli Delegatura w Białymstoku
Kontrolerzy	Adrian Gosk – specjalista kontroli państwowej, upoważnienie do kontroli nr LBI/2/2018 z 2 stycznia 2018 r. (dowód: akta kontroli str. 1-2)
Jednostka kontrolowana	Ośrodek Pomocy Społecznej w Ciechanowcu, ul. Adama Mickiewicza 1, 18-230 Ciechanowiec (zwany dalej: „Ośrodkiem" lub „OPS")
Kierownik jednostki kontrolowanej	Marzena Kryńska – dyrektor Ośrodka Pomocy Społecznej w Ciechanowcu[1] (dowód: akta kontroli str. 3)

II. Ocena kontrolowanej działalności[2]

Ocena ogólna

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

Uzasadnienie oceny ogólnej

Stwierdzono bowiem nieprawidłowości, polegające w szczególności na:

- umożliwieniu użytkownikom wszystkich 11 komputerów Ośrodka pełnego dostępu do panelu zarządzania tych urządzeń, w tym kontem administratora systemu operacyjnego,
- nieanalizowaniu i niezabezpieczeniu przed modyfikacją lub zniszczeniem logów systemów operacyjnych komputerów,
- niezabezpieczeniu przed uszkodzeniem lub zniszczeniem nośników zawierających kopie baz danych programów wykorzystywanych w OPS,
- udostępnianiu części zasobów informacyjnych (plików) Ośrodka dla pracowników innej jednostki, wbrew § 20 ust. 2 pkt 7 lit. c 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],
- zgłoszeniu z opóźnieniem Generalnemu Inspektorowi Ochrony Danych Osobowych[5] dwóch z 10 prowadzonych zbiorów danych osobowych, a w odniesieniu do kolejnych dwóch – niedokonaniu aktualizacji zgłoszeń,
- prowadzeniu ewidencji osób upoważnionych do przetwarzania danych osobowych niezawierającej informacji o wszystkich osobach, którym udzielono takiego upoważnienia oraz niewskazaniu w niej identyfikatorów w systemie informatycznym, mimo takiego wymogu określonego w art. 39 ust. 1 pkt 3 ustawy z dnia 29 sierpnia 1997 r. o ochronie danych osobowych[6],
- nieprowadzeniu corocznych audytów wewnętrznych z zakresu bezpieczeństwa,
- niegromadzeniu bieżących informacji w zakresie inwentaryzacji sprzętu i oprogramowania służącego do przetwarzania informacji, obejmujących ich rodzaj i konfigurację.

---

1 Od 29 sierpnia 2001 r.
2 Najwyższa Izba Kontroli stosuje 3-stopniową skalę ocen: pozytywna, pozytywna mimo stwierdzonych nieprawidłowości, negatywna.
3 Kontrolą objęty został okres od 1 stycznia 2016 r. do zakończenia czynności kontrolnych.
4 Dz. U. z 2017 r. poz. 2247. Rozporządzenie zwane dalej: „rozporządzeniem KRI".
5 Dalej: „GIODO".
6 Dz. U. 2016 r. poz. 922.

III. Opis ustalonego stanu faktycznego

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

Opis stanu faktycznego

1.1. W OPS do przetwarzania danych wykorzystywano trzy systemy informatyczne (aplikacje: „Pomost STD" „Świadczenia Rodzinne / Fundusz Alimentacyjny" i „Mała UniFirma") oraz program „Płatnik". Ponadto przetwarzano dane w dwóch serwisach udostępnionych OPS, tj. Karta Dużej Rodziny[7] oraz Samorządowa Elektroniczna Platforma Informacyjna[8]. Każdy z 11 komputerów posiadał dostęp do Internetu, co było zgodne z warunkami określonymi w dokumentacji tych systemów. Na wszystkich stacjach roboczych zainstalowana była także aplikacja pulpitu zdalnego TeamViewer, co szerzej opisano w dalszej części wystąpienia pokontrolnego, w sekcji „Ustalone nieprawidłowości".

(dowód: akta kontroli str. 4-14, 17, 22-28)

1.2. Realizując obowiązek, o którym mowa w § 20 ust. 2 pkt 3 rozporządzenia KRI, Dyrektor OPS, działając jako Administrator Danych Osobowych[9], w związku z opracowywaniem nowej dokumentacji bezpieczeństwa[10], przeprowadziła w grudniu 2016 roku analizę zagrożeń przetwarzania informacji, w tym danych występujących w systemach informatycznych Ośrodka. Wśród najważniejszych zagrożeń wymieniono m.in.: zaniedbania pracowników i pozostawienie sprzętu bez wylogowania się, niekontrolowaną obecność nieuprawnionych osób w obszarze przetwarzania danych oraz pokonanie zabezpieczeń informatycznych. Środki ochrony stanowić miały m.in.: zapoznanie pracowników z zasadami przetwarzania danych, stosowanie haseł i wykorzystywanie sprzętu przeznaczonego wyłącznie do tego celu. Poziom ryzyka naruszenia bezpieczeństwa danych określony został ówcześnie na poziomie „niskim", a zastosowane techniczne i organizacyjne środki ochrony uznano jako adekwatne do stwierdzonego poziomu ryzyka. Do dnia rozpoczęcia niniejszej kontroli w Ośrodku nie wykonywano innych analiz w tym zakresie, gdyż – jak wyjaśniła Dyrektor OPS – wyniki ww. analizy wydawały się nadal aktualne.

(dowód: akta kontroli str. 17, 74-75)

1.3. Wszystkich jedenastu pracowników OPS przetwarzających dane osobowe zaangażowano w ten proces w stopniu adekwatnym do realizowanych zadań, wynikających z ich zakresów obowiązków. Posiadali one wymagane upoważnienia Dyrektora OPS.

W okresie objętym kontrolą w Ośrodku na bieżąco zmieniano również uprawnienia użytkownikom, co potwierdziły imienne dokumenty nadane trzem nowo zatrudnionym pracownikom oraz odwołania upoważnień dla dwóch byłych pracowników OPS.

(dowód: akta kontroli str. 9, 95-113)

Każdy z pracowników zaangażowanych w przetwarzanie danych w systemach informatycznych OPS posiadał własny login i odpowiednio złożone hasło do systemów operacyjnych oraz dziedzinowych wykorzystywanych do przetwarzania danych osobowych. Mimo nadania profili z ograniczonymi uprawnieniami, wszystkich 11 użytkowników posiadało również pełny dostęp do panelu zarządzania komputera, w tym kontem administratora, co według powołanego w trakcie niniejszej kontroli biegłego z zakresu teleinformatyki oznaczało, że każdy użytkownik mógł dokonać zmiany hasła administratora, po czym zalogować się jako administrator i od tego momentu dysponować pełną kontrolą nad komputerem. Ponadto na wszystkich komputerach nie wprowadzono również mechanizmu wymuszania zmiany hasła systemowego co 30 dni, co szerzej opisano w dalszej części wystąpienia pokontrolnego, w sekcji „Ustalone nieprawidłowości".

(dowód: akta kontroli str. 4-14, 16-28)

---

[7] System informatyczny do obsługi KDR, znajdujący się na stronie internetowej Ministerstwa Rodziny, Pracy i Polityki Społecznej – kdr.mpips.gov.pl.

[8] Dostępnej na stronie internetowej: https://sepi.sygnity.pl. Dalej: „SEPI".

[9] Zwany dalej: „ADO".

[10] Dokumentacja bezpieczeństwa wprowadzona zarządzeniem Nr 7/2016 Dyrektora OPS z dnia 29 grudnia 2016 r. w sprawie wprowadzenia Polityki Bezpieczeństwa Informacji w Ośrodku, zawierającym Politykę Bezpieczeństwa Informacji (dalej „PBI") oraz Instrukcję zarządzania systemami informatycznymi służącymi do przetwarzania danych osobowych (dalej „Instrukcja Zarządzania").

1.4. W OPS nie monitorowano dostępu do informacji, mimo takiego wymogu zawartego w § 20 ust. 2 pkt 7 lit a rozporządzenia KRI, gdyż nie rejestrowano logów poszczególnych aplikacji, ruchu sieciowego, a także danych wychodzących z sieci lokalnej OPS do sieci publicznej – nie był prowadzony zbiorczy rejestr dostępu do systemu, a logi zapisywane na końcówkach klienckich nie były zabezpieczone przed modyfikacją i zniszczeniem, co szerzej opisano w dalszej części wystąpienia pokontrolnego, w sekcji „Ustalone nieprawidłowości". (dowód: akta kontroli str. 4-14, 16-28)

1.5. Ośrodek nie posiadał własnej serwerowni (korzystał z pomieszczenia Urzędu Miejskiego w Ciechanowcu), ani sieci bezprzewodowej. Sieć komputerowa OPS stanowiła element sieci ww. Urzędu, a część zasobów informacyjnych (plików) Ośrodka była udostępniana dla pracowników tej jednostki, co szerzej opisano w dalszej części wystąpienia, w sekcji „Ustalone nieprawidłowości". (dowód: akta kontroli str. 16-28)

1.6. W OPS nie wprowadzono regulacji umożliwiających wykorzystywanie przez pracowników sprzętu prywatnego do realizacji obowiązków służbowych, ale w praktyce poszczególni pracownicy w dowolnym momencie mieli możliwość podłączenia się za pomocą takich urządzeń (sieci lokalnej OPS nie wyposażono w filtr adresów MAC, umożliwiający kontrolę podłączanych do niej urządzeń). Dyrektor Ośrodka wyjaśniła m.in., że wszystkim pracownikom do celów służbowych powierzono niezbędny sprzęt służbowy, stąd nie było potrzeby bezpośredniego regulowania kwestii wykorzystywania urządzeń prywatnych. Jej zdaniem, pośrednio takie regulacje jednak występowały, gdyż w Instrukcji Zarządzania pracownikom zabroniono m.in. kopiowania programów i danych, samowolnego instalowania i używania oprogramowania, a także „przenoszenia sprzętu komputerowego", a zatem także „wnoszenia" sprzętu prywatnego. Według Dyrektor OPS do tej pory nie było takich zdarzeń w Ośrodku. (dowód: akta kontroli str. 16-28, 68-87)

1.7. Dokumentacja dotycząca zabezpieczenia danych w Ośrodku nie zawierała raportów potwierdzających wystąpienie przypadków naruszenia bezpieczeństwa danych osobowych. Zgodnie z wyjaśnieniami Dyrektora OPS, w latach 2016 – 2018 w Ośrodku nie odnotowano przypadków naruszenia bezpieczeństwa systemu informatycznego lub utraty integralności, dostępności lub poufności informacji. Nie wystąpiła również konieczność przywrócenia danych z wykonanych kopii bezpieczeństwa. (dowód: akta kontroli str. 18, 68-87)

1.8. Obowiązująca Instrukcja Zarządzania określała procedury postępowania z komputerami przenośnymi (przewidziano m.in. zachowanie szczególnej ostrożności przy transporcie, przechowywaniu i użytkowaniu poza siedzibą OPS), a w okresie objętym kontrolą na stanie Ośrodka poza 11 użytkowanymi komputerami stacjonarnymi, znajdowały się dwa terminale (minilaptopy), umożliwiające pracę mobilną. Sprzęt ten otrzymano w grudniu 2013 roku w ramach projektu Emp@tia – „Platforma komunikacyjna obszaru zabezpieczenia społecznego"[11], jednak do dnia rozpoczęcia niniejszej kontroli obu nie wykorzystywano w bieżącej pracy. Według Dyrektor OPS, urządzeń tych nie zapotrzebowywano, a bezpośrednio po przekazaniu Ministerstwo nie stworzyło również warunków prawno-organizacyjnych do ich bieżącego użytkowania. Dyrektor wyjaśniła, że pracownicy obawiają się ich utraty / zniszczenia w trakcie pracy w terenie i nie jest to narzędzie wpływające na przyspieszenie wykonywanych czynności. Z wyjaśnień Dyrektor OPS wynika, iż ostateczne uruchomienie tych urządzeń po kończącej się fazie testów powinno nastąpić do końca I kwartału br. (dowód: akta kontroli str. 4-14,18, 85-87, 185-188)

1.9. Ośrodek w latach 2016 – 2018 posiadał umowy serwisowe z firmą zajmującą się administracją systemami Pomost STD i Świadczenia Rodzinne / Fundusz Alimentacyjny, oraz z producentem oprogramowania Mała UniFirma. W obu umowach podmioty zewnętrzne w związku z realizacją tych usług zobowiązały się do zachowania poufności i przestrzegania przepisów o ochronie danych osobowych. Ponadto OPS współpracował z informatykiem Urzędu Miejskiego w Ciechanowcu (osoba ta posiadała upoważnienie Dyrektora OPS do przetwarzania danych osobowych), jednak zakres tej współpracy nie został formalnie określony, gdyż – jak wyjaśniła Dyrektor – obejmowała ona wyłącznie doraźną (okazjonalną) pomoc w przypadku drobnych problemów technicznych, na przykład

[11] Na podstawie umowy użyczenia Nr 73/20/EMP/2013, zawartej 23 grudnia 2013 r. pomiędzy Ministerstwem Pracy i Polityki Społecznej a OPS.

potrzeby zrestartowania serwera. W okresie objętym kontrolą Ośrodek nie korzystał z usług naprawy komputerów. (dowód: akta kontroli str. 16-21, 110, 143-158, 174-182)

1.10. Wszystkie 11 komputerów OPS wyposażono w centralnie instalowane oprogramowanie antywirusowe, którego aktualizacja odbywała się automatycznie (posiadano aktualne wersje aplikacji zabezpieczających). W opinii powołanego w trakcie niniejszej kontroli biegłego z zakresu teleinformatyki, dostęp do sieci lokalnej kontrolowany był przez firewall zainstalowany na routerze CISCO, co było zgodne z pkt III 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[12]. (dowód: akta kontroli str. 4-14, 22-28)

1.11. Ośrodek korzystał z domeny internetowej i poczty elektronicznej wykupionej przez Urząd Miejski w Ciechanowcu w podmiocie zewnętrznym. Zgodnie z regulaminem świadczenia tych usług podmiot zewnętrzny zobowiązał się w ramach ich świadczenia do przestrzegania przepisów prawa, w tym o ochronie danych osobowych i o świadczeniu usług drogą elektroniczną. Ponadto w regulaminie potwierdzono, że przy przesyłaniu danych stosowano odpowiednie zabezpieczenia kryptograficzne. Dyrektor Ośrodka wyjaśniła, iż wspólny zakup tych usług przez ww. Urząd i OPS pozwalał ograniczyć wydatki budżetowe, a monitorowaniem prawidłowości ich świadczenia zajmował się nieodpłatnie informatyk Urzędu. Dodała, że dotychczas nie był jej zgłaszany jakikolwiek problem związany ze spamem, zatem w jej ocenie dotychczasowe zabezpieczenia w tym zakresie były skuteczne. (dowód: akta kontroli str. 16-21, 114-142)

1.12. Regulacje wewnętrzne, tj. PBI i Instrukcja Zarządzania, nie określały sposobu i częstotliwości tworzenia kopii bezpieczeństwa danych znajdujących się w systemach OPS. W trakcie niniejszej kontroli stwierdzono, iż kopie zapasowe tworzone były w sposób automatyczny (codziennie) w systemach Pomost STD i Świadczenia Rodzinne / Fundusz Alimentacyjny. Kopie te zapisywane były na jednej z partycji dysku twardego serwera i przechowywane były co najmniej przez 30 dni. Ponadto Główna Księgowa OPS okresowo archiwizowała dane z programów Mała UniFirma i Płatnik na nośnik typu pendrive. Nośnik ten przechowywany był w zamykanej na klucz szafie, znajdującej się w tym samym pomieszczeniu co komputer, z którego dane były archiwizowane, co szerzej opisano w dalszej części wystąpienia pokontrolnego, w sekcji „Ustalone nieprawidłowości".
(dowód: akta kontroli str. 4-14, 16-28, 68-87)

1.13. Na każdym z 11 poddanych oględzinom komputerów zainstalowane było wyłącznie dopuszczone oprogramowanie służbowe, jednak – według biegłego z zakresu teleinformatyki – pracownicy (mimo nadania profili z ograniczonymi uprawnieniami, posiadali pełny dostęp do panelu zarządzania komputera, w tym kontem administratora) posiadali również techniczną możliwość instalowania danych do tego nieprzeznaczonych i zainfekowania komputerów złośliwym oprogramowaniem. Dziewięć (z 11) komputerów posiadało aktualne systemy operacyjne, natomiast dwa działały z wykorzystaniem systemów nieposiadających wsparcia producenta, co szerzej opisano w dalszej części wystąpienia pokontrolnego, w sekcji „Uwagi dotyczące badanej działalności".
(dowód: akta kontroli str. 4-14, 22-28)

1.14. W Ośrodku, zgodnie z § 20 ust. 2 pkt 12 lit. a rozporządzenia KRI, zadbano o aktualizację systemów operacyjnych (poza dwoma przypadkami opisanymi w pkt 1.13. wystąpienia) i aplikacji bezpieczeństwa, które były wykonywane zgodnie z harmonogramami ustalonymi przez ich producentów. (dowód: akta kontroli str. 4-14, 22-28)

1.15. W Ośrodku nie wprowadzono wewnętrznych regulacji dotyczących wykonywania płatności (przelewów) drogą elektroniczną, gdyż – jak wyjaśniła Dyrektor OPS – wszystkie przelewy wykonywane były drogą tradycyjną, a siedziba obsługującego Ośrodek banku znajduje się w bezpośrednim sąsiedztwie. (dowód: akta kontroli str. 19)

---

[12] Dz. U. Nr 100, poz. 1024. Rozporządzenie zwane dalej „rozporządzeniem w sprawie dokumentacji przetwarzania danych osobowych".

Ustalone nieprawidłowości

W działalności kontrolowanej jednostki w przedstawionym wyżej zakresie stwierdzono następujące nieprawidłowości:

1. Użytkownikom wszystkich 11 komputerów, mimo nadania profili z ograniczonymi uprawnieniami, umożliwiono pełny dostęp do panelu zarządzania komputera, w tym kontem administratora systemu operacyjnego tych urządzeń, chociaż – zgodnie z zakresami obowiązków – nie realizowali oni zadań w zakresie administrowania systemami. W wyniku tego, jak ustalił biegły, dysponowali oni możliwością ściągania aplikacji i plików wykonalnych oraz instalowania ich na stacjach komputerowych, do których mieli dostęp. Było to sprzeczne z przepisem § 20 ust. 2 pkt 4 rozporządzenia KRI, zgodnie z którym kierownictwo podmiotu publicznego jest obowiązane do podejmowania działań zapewniających, aby osoby zaangażowane w proces przetwarzania informacji posiadały stosowne uprawnienia i uczestniczyły w tym procesie w stopniu adekwatnym do realizowanych zadań oraz obowiązków, mających na celu zapewnienie bezpieczeństwa informacji. Dyrektor OPS wyjaśniła, że wynikało to z braku zatrudnionego na stałe informatyka. Najwyższa Izba Kontroli zwraca uwagę, że przyznanie wszystkim pracownikom takich uprawnień, przy jednoczesnym braku odpowiednio wykwalifikowanej kadry do realizacji wszystkich zadań związanych z ochroną danych, stwarza ryzyko obniżenia skuteczności ochrony danych przetwarzanych w OPS. (dowód: akta kontroli str. 4-14, 16-28)
2. W OPS nie zabezpieczano należycie danych przetwarzanych w systemach informatycznych, mimo wprowadzenia wysokiego poziomu bezpieczeństwa przetwarzania danych, wymaganego cz. C pkt XII załącznika do rozporządzenia w sprawie dokumentacji przetwarzania danych osobowych oraz postanowieniami pkt 1.2. i 7 Instrukcji Zarządzania. Na żadnym z 11 użytkowanych w Ośrodku komputerów nie wprowadzono mechanizmu obowiązkowej okresowej zmiany hasła. Było to niezgodne z cz. A pkt IV powołanego załącznika do rozporządzenia, wymagającego zmiany hasła nie rzadziej niż co 30 dni oraz z pkt 1.2 i 6.1. Instrukcji Zarządzania, przewidujących odpowiednią złożoność hasła i jego okresową zmianę. Według Dyrektora OPS aktualne ustawienia uprawnień poszczególnych użytkowników i mechanizmy zabezpieczające dostosowane były do uwarunkowań oraz możliwości wynikających z braku zatrudnienia na stałe informatyka, a ze strony pracowników nie było naruszeń. (dowód: akta kontroli str. 4-14, 16, 22-28, 85-87)
3. Nie analizowano i nie zabezpieczono przed modyfikacją lub zniszczeniem logów systemów operacyjnych komputerów wykorzystywanych w OPS, a także nie nadzorowano prac serwisowych realizowanych z wykorzystaniem aplikacji pulpitu zdalnego TeamViewer, zainstalowanej na wszystkich 11 komputerach. Tymczasem 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. Ponadto w opinii powołanego w trakcie niniejszej kontroli biegłego z zakresu teleinformatyki, w przypadku powstania w Ośrodku ewentualnych nadużyć znalezienie ich źródła lub sprawcy może być utrudnione. Niewykorzystanie narzędzi do automatycznej analizy logów powoduje, że administrator, z racji braku wiedzy o pojawiających się anomalnych stanach systemu, nie może szybko zareagować na pojawiające się ewentualne zagrożenie bezpieczeństwa, a serwisant łączący się za pośrednictwem aplikacji TeamViewer miał dostęp do wszystkich zasobów, do których dostęp w momencie połączenia posiadał dany użytkownik, przy tego typu rozwiązaniu nie było pewności, kto faktycznie znajdował się po drugiej stronie połączenia (weryfikacja odbywała się wyłącznie na podstawie rozmowy telefonicznej), a po przeprowadzonych pracach i ewentualnych błędach serwisanta nie pozostawał ślad w ewidencji. Dyrektor OPS wyjaśniła, że czynności tych nie wykonywano, ponieważ nie było osoby, która taki monitoring mogłaby na bieżąco prowadzić, a to ściśle związane było z brakiem środków na jej zatrudnienie.
(dowód: akta kontroli str. 4-14, 16-28)

4. Sieć komputerowa OPS stanowiła element sieci Urzędu Miejskiego w Ciechanowcu, a część zasobów informacyjnych (plików) Ośrodka była udostępniana dla pracowników ww. jednostki. Obowiązek zapewnienia środków uniemożliwiających nieautoryzowany dostęp na poziomie systemów operacyjnych, usług sieciowych i aplikacji wynika z § 20 ust. 2 pkt 7 lit. c rozporządzenia KRI, zgodnie z którym jest on jednym z elementów zarządzania bezpieczeństwem informacji, zmierzającym do zapewnienia ochrony przetwarzanych informacji przed kradzieżą, nieuprawnionym dostępem, uszkodzeniami lub zakłóceniami. Dyrektor OPS wyjaśniła, że po skonsultowaniu tego faktu z informatykiem Urzędu Miejskiego i serwisantem oprogramowania dziedzinowego nie jest w stanie określić przyczyn i przybliżonego roku uruchomienia tego mechanizmu. Dodała, że nikt nie zwracał do tej pory na to uwagi, ale zostaną uruchomione odpowiednie mechanizmy zabezpieczające w tym zakresie. Według Dyrektor Ośrodka najważniejsze dane osobowe zawarte chociażby w decyzjach czy wywiadach środowiskowych nie były udostępniane, ponieważ nie były opracowywane w edytorze tekstu tylko w programach dziedzinowych, które wymagały logowania, a więc nie były dostępne dla pracowników Urzędu. (dowód: akta kontroli str. 4-14, 16-28)

5. Nośniki kopii zapasowych baz danych przechowywano w Ośrodku w tych samych pomieszczeniach, co urządzenia z których dane były archiwizowane (w serwerowni archiwizowano dane z programów Pomost STD i Świadczenia Rodzinne / Fundusz Alimentacyjny, a w pomieszczeniu Głównej księgowej OPS – dane z programów Płatnik i Mała UniFirma). Było to niezgodne z przepisem pkt IV ust. 4 lit. a załącznika do rozporządzenia w sprawie dokumentacji przetwarzania danych osobowych, zgodnie z którym kopie zapasowe przechowuje się w miejscach zabezpieczających je przed uszkodzeniem lub zniszczeniem. Zdaniem NIK, przechowywanie tych kopii w miejscu skąd pochodzą dane stwarza duże ryzyko ich utraty, np. w przypadku wystąpienia pożaru, w wyniku którego zniszczeniu może ulec zarówno baza danych, jak i jej kopia zapasowa. Dyrektor OPS wyjaśniła, że nie posiada odpowiedniego przygotowania informatycznego, a współpracujący serwisant nie zasugerował potrzeby przechowywania kopii bezpieczeństwa na nośnikach zewnętrznych poza wymienionymi pomieszczeniami. (dowód: akta kontroli str. 4-14, 16-28)

Uwagi dotyczące badanej działalności

Najwyższa Izba Kontroli zwraca także uwagę, że na dwóch komputerach użytkowników systemów służących do przetwarzania danych osobowych były zainstalowane systemy operacyjne Windows XP, dla których producent zakończył wsparcie techniczne. W opinii powołanego w trakcie niniejszej kontroli biegłego z zakresu teleinformatyki, wykorzystywanie systemów w wersji XP jest działaniem nieprofesjonalnym. Producent zaniechał wsparcia tego oprogramowania co oznacza, że nie jest zobowiązany do opracowywania aktualizacji zabezpieczeń systemu i niewątpliwie podnosi to ryzyko naruszenia bezpieczeństwa. (dowód: akta kontroli str. 4-14, 16-28)

Ocena cząstkowa

Najwyższa Izba Kontroli ocenia negatywnie skuteczność przyjętych w OPS 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. Dane osobowe w OPS przetwarzane były w dziesięciu zbiorach danych, z których siedem prowadzono w wersji elektronicznej i papierowej, a trzy wyłącznie w wersji papierowej. Wszystkie ww. zbiory zgłoszono do GIODO, przy czym zbiór „Karta Dużej Rodziny" i „Dodatki energetyczne" zostały zgłoszone do rejestracji ze znacznym opóźnieniem, co szerzej opisano w dalszej części wystąpienia pokontrolnego, w sekcji „Ustalone nieprawidłowości". W okresie objętym kontrolą OPS nie aktualizował danych rejestracyjnych zbiorów zgłoszonych do GIODO, mimo że wystąpiła taka potrzeba (szerzej opisana w pkt 4.3) oraz nie występował o ich wykreślenie. Nie wystąpiły również przypadki odmowy rejestracji zbioru. (dowód: akta kontroli str. 4-14)

Analiza wszystkich trzech zgłoszeń OPS rejestracji zbiorów do GIODO w okresie objętym kontrolą wykazała, że zawierały one wymagane elementy, określone w art. 41 ust. 1 ustawy o ochronie danych osobowych. (dowód: akta kontroli str. 31-46)

2.2. PBI i Instrukcja Zarządzania przewidywały możliwość powołania przez Dyrektora OPS Administratora Bezpieczeństwa Informacji („ABI"). ADO nie skorzystała jednak z tej możliwości, przewidzianej wart. 36a ust. 1 ustawy o ochronie danych osobowych, gdyż – jak wyjaśniła – nie miała kogo wyznaczyć na to stanowisko spośród pracowników.
(dowód: akta kontroli str. 16-21, 68-87)

2.3. W myśl przepisu art. 36b ustawy o ochronie danych osobowych w przypadku niewyznaczenia ABI, zadania określone w art. 36a ust 2 pkt 1 tej ustawy, z wyłączeniem obowiązku sporządzania sprawozdania, realizuje ADO. Dyrektor OPS wywiązała się jedynie z obowiązku zapoznania osób upoważnionych do przetwarzania danych osobowych z przepisami o ich ochronie. Nie realizowała natomiast pozostałych zadań, określonych w art. 36a ust 2 pkt 1 ustawy o ochronie danych osobowych, co szerzej opisano w dalszej części wystąpienia pokontrolnego, w sekcji „Ustalone nieprawidłowości".
(dowód: akta kontroli str. 16-21)

2.4. W OPS, stosownie do art. 39 ust. 1 ustawy o ochronie danych osobowych, prowadzono ewidencją osób upoważnionych do przetwarzania danych osobowych. Zawierała ona elementy określone w art. 39 ust 1 pkt 1-2 ww. ustawy, tj.: imię i nazwisko osoby upoważnionej, datę nadania i ustania upoważnienia do przetwarzania danych osobowych. W ewidencji nie zawarto natomiast identyfikatora, co szerzej opisano w dalszej części wystąpienia pokontrolnego, w sekcji „Ustalone nieprawidłowości". W ewidencji tej ujęto wszystkich pracowników Ośrodka oraz dwie osoby współpracujące z OPS (serwisanta i informatyka Urzędu Miejskiego). Nie ujęto w niej natomiast informacji o dziewięciu pracownikach Powiatowego Urzędu Pracy w Wysokiem Mazowieckiem[13], którym udzielono upoważnienia do przetwarzania danych osobowych (pochodzących z OPS), co szerzej opisano w dalszej części wystąpienia pokontrolnego, w sekcji „Ustalone nieprawidłowości".
(dowód: akta kontroli str. 9, 16-21, 88-90, 113, 164)

Jedenastu pracowników OPS posiadających dostęp do zbiorów danych osobowych, posiadało ten dostęp w zakresie wynikającym z zakresów obowiązków oraz upoważnień do przetwarzania danych. (dowód: akta kontroli str. 9, 88-90)

2.5. W OPS nie wydawano innych wewnętrznych aktów prawnych, procedur, instrukcji lub poleceń dotyczących sposobu gromadzenia i przetwarzania zasobów informacyjnych niż dokumentacja bezpieczeństwa opisana w pkt 2.10. niniejszego wystąpienia pokontrolnego. (dowód: akta kontroli str. 20, 68-87)

2.6. Regulacje wewnętrzne Ośrodka nie przewidywały zadań realizowanych przez Administratora Systemów Informatycznych – w okresie objętym kontrolą nie powołano osoby do pełnienia tej funkcji. (dowód: akta kontroli str. 16-21, 68-87)

2.7. W okresie objętym kontrolą w OPS nie przeprowadzano corocznych audytów wewnętrznych z zakresu bezpieczeństwa informacji, wynikających z § 20 ust. 2 pkt. 14 rozporządzenia KRI, co szerzej opisano w dalszej części wystąpienia pokontrolnego, w sekcji „Ustalone nieprawidłowości". (dowód: akta kontroli str. 16-21)

2.8. Do dnia rozpoczęcia niniejszej kontroli NIK pracownicy OPS nie uczestniczyli w szkoleniach dotyczących zagadnień związanych z ochroną danych osobowych oraz bezpieczeństwem informacji, co szerzej opisano w dalszej części wystąpienia pokontrolnego, w sekcji „Ustalone nieprawidłowości. (dowód: akta kontroli str. 9, 16-21, 195)

2.9. W latach 2016 – 2018 (do zakończenia kontroli) w Ośrodku nie było zewnętrznych kontroli w zakresie bezpieczeństwa danych oraz nie wpływały skargi dotyczące przypadków związanych z ujawnieniem danych osobowych lub naruszeniem przepisów związanych z ich ochroną. (dowód: akta kontroli str. 15)

[13] Dalej: „PUP".

2.10. Do 29 grudnia 2016 r. w OPS obowiązywała dokumentacja bezpieczeństwa przyjęta zarządzeniem Dyrektora Ośrodka z 15 września 2008 r.[14], zastąpiona aktualnie obowiązującymi PBI i Instrukcją Zarządzania, które nie zawierały jednak elementów wymaganych § 4 pkt 2 – 4 i § 5 pkt 4 – 5 rozporządzenia w sprawie dokumentacji oraz warunków technicznych, co szerzej opisano w dalszej części wystąpienia pokontrolnego, w sekcji „Ustalone nieprawidłowości". (dowód: akta kontroli str. 51-87)

Ustalone nieprawidłowości

W działalności kontrolowanej jednostki w przedstawionym wyżej zakresie stwierdzono następujące nieprawidłowości:

1. Zgłoszenie do rejestracji w GIODO dwóch zbiorów danych osobowych nastąpiło ze znacznym opóźnieniem. Zbiór „Karta Dużej Rodziny" zgłoszono w styczniu 2016 roku, zbiór „Dodatki energetyczne" – w styczniu 2018 roku, podczas gdy pierwsze dokumenty (wnioski) gromadzone w tych zbiorach wpłynęły do OPS odpowiednio w czerwcu i w styczniu 2014 roku. Działanie takie naruszało wymogi art. 40 i 46 ustawy o ochronie danych osobowych, zgodnie z którymi przetwarzanie danych w zbiorze można rozpocząć po zgłoszeniu go do GIODO. Dyrektor OPS wyjaśniła, że w obu przypadkach był to jej błąd wynikający z natłoku innych obowiązków.
(dowód: akta kontroli str. 11, 16-21, 31-41)

2. ADO nie realizował zadań określonych w art. 36a ust 2 pkt 1 ustawy o ochronie danych osobowych, tj. dokonywania sprawdzeń zgodności przetwarzania danych osobowych z przepisami o ochronie danych osobowych oraz nadzorowania opracowania i aktualizowania dokumentacji, o której mowa w art. 36 ust. 2 tej ustawy. Dyrektor OPS wyjaśniła, że wskazane zadania nie były realizowane z uwagi na obciążenie innymi obowiązkami, a także nieprzygotowanie w zakresie zabezpieczenia ochrony danych osobowych oraz opracowywania i wprowadzania dokumentacji dotyczącej zabezpieczenia systemów informatycznych. (dowód: akta kontroli str. 16-21, 51-87)

3. W ewidencji osób upoważnionych do przetwarzania danych osobowych, wbrew wymogom art. 39 ust. 1 pkt 3 ustawy o ochronie danych osobowych, nie wskazano identyfikatora w systemie informatycznym i nie ujęto informacji o dziewięciu pracownikach PUP, którym udzielono upoważnienia do przetwarzania danych osobowych. Dyrektor OPS wyjaśniła, że zarówno brak identyfikatorów wszystkich pracowników, jak i dwóch współpracowników ujętych w tej ewidencji wynikał z przeoczenia. Jeśli chodzi o brak w ewidencji dziewięciu pracowników PUP w Wysokiem Mazowieckiem to nie wiedziała, że osoby te również należy ujmować w tej ewidencji, skoro były imiennie wyszczególnione na odrębnej liście (stanowiącej integralną część porozumienia z PUP). (dowód: akta kontroli str. 16-21, 88-90, 164)

4. W okresie objętym kontrolą (od 1 stycznia 2016 r. do 8 lutego 2018 r.) w Ośrodku nie przeprowadzano okresowych (nie rzadziej niż raz na rok) audytów wewnętrznych z zakresu bezpieczeństwa informacji, mimo wymogu wynikającego z § 20 ust. 2 pkt. 14 rozporządzenia KRI. Dyrektor OPS wyjaśniła: *„nie posiadaliśmy wystarczających środków finansowych na zapewnienie tego wymogu"*. (dowód: akta kontroli str. 16-21)

5. Od 1 stycznia 2016 r. do dnia rozpoczęcia niniejszej kontroli pracownicy OPS nie uczestniczyli w szkoleniach z ochrony danych osobowych i 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. Dyrektor OPS wyjaśniła to brakiem środków na umożliwienie podnoszenia kwalifikacji pracowników we wszystkich obszarach działalności i skupianiem się z tego powodu na szkoleniach w szeroko rozumianym obszarze pomocy społecznej. Dodała, że serwisanci zewnętrzni w ramach bieżącej obsługi zajmowali się również drobnymi przeszkoleniami z pogranicza informatyki i bezpieczeństwa danych, ale ze względu na niewielkie zatrudnienie i rzadkie wizyty czynności te nie były dokumentowane. Wyjaśniła też,

[14] Zarządzenie Nr 3/2008 Dyrektora OPS z dnia 15 września 2008 r. w sprawie dokumentacji opisującej sposób przetwarzania danych oraz środki techniczne i organizacyjne zapewniające ochronę przetwarzanych danych osobowych.

że w związku ze zbliżającą się istotną zmianą przepisów, w styczniu 2018 roku odbyła jednodniowe szkolenie w tym zakresie i omówiła z pracownikami najważniejsze zagadnienia, które poruszano na szkoleniu. Uważa zatem, że personel Ośrodka posiada wystarczającą wiedzę w tym zakresie. (dowód: akta kontroli str. 9, 16-21, 195)

6. Aktualnie obowiązujące PBI oraz Instrukcja Zarządzania nie zawierały elementów określonych w § 4 pkt 2 – 4 oraz § 5 pkt 4 – 5 rozporządzenia w sprawie dokumentacji przetwarzania danych osobowych, tj. m.in.: wykaz zbiorów danych osobowych nie obejmował wskazania programów zastosowanych do przetwarzania tych danych, brakowało opisu struktury zbiorów danych wskazującego zawartość poszczególnych pól informacyjnych i powiązania między nimi, a także określenia sposobu przepływu danych pomiędzy poszczególnymi systemami, procedur tworzenia kopii zapasowych zbiorów danych oraz programów i narzędzi programowych służących do ich przetwarzania; a także nie określono sposobu, miejsca i okresu przechowywania elektronicznych nośników informacji zawierających dane osobowe. Dyrektor OPS wyjaśniła, że brak tych elementów wynikał z niedopatrzenia. (dowód: akta kontroli str. 16-21, 68-87)

Ocena cząstkowa

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

3. Sposób przechowywania oraz zabezpieczenia danych

Opis stanu faktycznego

3.1. W Ośrodku nie wprowadzono systemu kontroli dostępu, monitoringu, systemu alarmowego i systemu przeciwpożarowego. Nie stosowano również zabezpieczeń okien (krat, rolet lub folii antywłamaniowej). W obowiązującej dokumentacji bezpieczeństwa określono natomiast, że pomieszczenia, w których znajdują się przetwarzane zbiory danych osobowych pozostają zawsze pod nadzorem pracownika upoważnionego do ich przetwarzania, a opuszczenie pomieszczenia musi być poprzedzone zamknięciem zbioru danych w szafie na klucz (dłuższa nieobecność powinna wiązać się z zamknięciem pomieszczenia). Przeprowadzone w trakcie niniejszej kontroli oględziny pomieszczeń Ośrodka nie wykazały jakichkolwiek bezpośrednich zagrożeń ze strony czynników fizycznych (OPS dysponował m.in. zamkami w pomieszczeniach i w szafkach na dokumenty, niszczarkami, gaśnicami, a na wykorzystywanych korytarzach Urzędu Miejskiego w Ciechanowcu znajdował się monitoring i czujki alarmowe). W OPS nie opracowano tzw. „polityki kluczy". W praktyce klucze umieszczano w przeznaczonej do tego skrzynce. (dowód: akta kontroli str. 4-14, 68-87, 114-116)

3.2. W OPS nie gromadzono bieżących informacji w zakresie inwentaryzacji sprzętu i oprogramowania służącego do przetwarzania informacji obejmujących ich rodzaj i konfigurację, co szerzej opisano w dalszej części wystąpienia pokontrolnego, w sekcji „Ustalone nieprawidłowości". (dowód: akta kontroli str. 18)

3.3. W latach 2016 – 2018 w Ośrodku nie likwidowano sprzętu komputerowego, będącego nośnikiem danych oraz nie wystąpiły przypadki, w których naprawa takiego sprzętu była realizowana przez podmioty zewnętrzne. (dowód: akta kontroli str. 16-21)

3.4. Niszczenie dokumentów zawierających dane osobowe prowadzone było w czterech niszczarkach, znajdujących się w obszarze przetwarzania danych osobowych. Przyjęte rozwiązania były zgodne z regulacjami określonym w PBI.
(dowód: akta kontroli str. 4-5, 16-21, 68-87)

3.5. W Instrukcji Zarządzania określono ogólne zasady dotyczące użytkowania komputerów przenośnych, ale do zakończenia niniejszej kontroli NIK nie wykorzystywano tych urządzeń – co omówiono szerzej w pkt 1.8. niniejszego wystąpienia pokontrolnego.
(dowód: akta kontroli str. 4-14, 18, 87)

3.6. W OPS nie wprowadzono regulacji wewnętrznych w zakresie sprzątania pomieszczeń, w których przetwarzano dane osobowe, a w latach 2016 – 2018 Ośrodek nie zatrudniał personelu sprzątającego. Jak wyjaśniła Dyrektor OPS, podstawowe utrzymanie porządku i czystości spoczywało na każdym zatrudnionym pracowniku, natomiast dodatkowe nieodpłatne usługi sprzątania pomieszczeń, w których przetwarzano dane osobowe wykonywały panie zatrudnione w Urzędzie Miejskim poza godzinami pracy (przy zamkniętych szafkach i wyłączonych komputerach). Według Dyrektor OPS wszystkie

te osoby w posiadanych zakresach czynności potwierdziły świadomość odpowiedzialności karnej za ewentualne naruszenie tajemnicy państwowej, służbowej, przepisów o ochronie informacji niejawnych oraz o ochronie danych osobowych.
(dowód: akta kontroli str. 16-21, 68-87, 114-116)

3.7. Obowiązująca w OPS Instrukcja Zarządzania określała procedury dotyczące przeglądów i konserwacji systemów oraz sprzętu do przetwarzania danych osobowych i realizowana była przez zewnętrzne podmioty serwisujące, co szerzej opisano w pkt 1.9. niniejszego wystąpienia pokontrolnego. (dowód: akta kontroli str. 16-21, 85-87, 143-182)

3.8. Ośrodek nie posiadał wewnętrznych regulacji dotyczących rozwiązań na wypadek wystąpienia sytuacji nadzwyczajnych, np. długotrwałego braku zasilania. Nie opracowano także procedur przywracania systemów po awarii oraz planu ciągłości działania umożliwiającego kontynuację wykonywania zadań publicznych, co szerzej opisano w dalszej części wystąpienia pokontrolnego, w sekcji „Uwagi dotyczące badanej działalności". OPS nie posiadał agregatu prądotwórczego umożliwiającego podtrzymywanie zasilania urządzeń komputerowych w razie długotrwałej utraty zasilania, natomiast możliwość kilkunastominutowej pracy w przypadku braku energii elektrycznej zapewniały urządzenia typu UPS, w które wyposażone były wszystkie wykorzystywane komputery stacjonarne. Dyrektor Ośrodka wyjaśniła, że OPS funkcjonuje w takich, a nie innych realiach finansowych i nie stać go na zakup agregatu prądotwórczego, którego nie posiada również Urząd Miejski. Podważyła też racjonalność takiego zakupu ze względu na sporadyczne przypadki zaniku napięcia (z reguły obejmujące okres, w którym podtrzymanie zasilania zapewniały UPS-y). Dodała, że jest niezwykle trudno opracować procedury dotyczące sytuacji nadzwyczajnych, bowiem – jak sama nazwa wskazuje – są one wyjątkowe i w zasadzie nieprzewidywalne. (dowód: akta kontroli str. 4-5, 16-21, 68-87)

3.9. Jak wyjaśniła Dyrektor OPS, w okresie objętym kontrolą w Ośrodku nie wystąpiły przypadki fizycznej utraty danych. Nie stosowano również procedury postępowania w przypadku naruszenia ochrony danych osobowych, określonej w §§ 27 – 32 PBI.
(dowód: akta kontroli str. 15-21, 76-77)

Ustalone nieprawidłowości

W działalności kontrolowanej jednostki w przedstawionym wyżej zakresie stwierdzono nieprawidłowość, polegającą na niegromadzeniu w OPS bieżących informacji w zakresie inwentaryzacji sprzętu i oprogramowania służącego do przetwarzania informacji obejmujących ich rodzaj i konfigurację. Obowiązek gromadzenia tych danych wynika § 20 ust. 2 pkt 2 rozporządzenia KRI. Dyrektor OPS wyjaśniła, że powodem było niezatrudnianie na stałe informatyka. Niewielka liczba sprzętu komputerowego i posiadanego oprogramowania umożliwiała jednak – według Dyrektora Ośrodka – w każdej chwili sprawne zebranie brakujących informacji. (dowód: akta kontroli str. 16-21)

Uwagi dotyczące badanej działalności

Najwyższa Izba Kontroli zwraca uwagę, na potrzebę opracowania w OPS 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 Ośrodka. 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 OPS.

Ocena cząstkowa

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

4. Przetwarzanie zasobów informacyjnych zgodnych z zakresem działalności jednostki kontrolowanej

Opis stanu faktycznego

4.1. W OPS wszystkie dziesięć zbiorów danych, w których przetwarzane były dane osobowe prowadzono w wersji papierowej, a siedem z nich także w formie elektronicznej. Wszystkie prowadzone zbiory zostały ujęte w wykazie zbiorów danych osobowych, stanowiącym element PBI. (dowód: akta kontroli str. 11, 68-84, 192-193)

4.2. W okresie objętym kontrolą Ośrodek nie aktualizował danych w rejestrze prowadzonym przez GIODO w odniesieniu do zbiorów, które były zarejestrowane.

(dowód: akta kontroli str. 11, 189-190)

4.3. W ośmiu (spośród 10) zbiorach zgłoszonych GIODO i prowadzonych przez Ośrodek zakres przetwarzanych danych był zgodny ze zgłoszeniem. W przypadku dwóch zbiorów („Karta Dużej Rodziny" i „Świadczenia z Pomocy Społecznej") nie wskazano faktu przetwarzania niektórych danych osobowych, co szerzej opisano w dalszej części wystąpienia pokontrolnego, w sekcji „Ustalone nieprawidłowości".

Analiza wszystkich dziesięciu zbiorów danych prowadzonych w OPS wykazała, że dane w nich gromadzone były wykorzystywane (niezbędne) do realizacji zadań, dla których zbiory były prowadzone. (dowód: akta kontroli str. 11, 16-21, 31-36, 47-50, 194)

W okresie objętym kontrolą w Ośrodku prowadzono postępowania dotyczące naboru kandydatów do pracy, a w ogłoszeniach wskazywano informacje wymagane art. 24 ust. 1 ustawy o ochronie danych osobowych. (dowód: akta kontroli str. 196-197)

4.4. Dyrektor OPS była administratorem zbiorów danych, do których dostęp posiadali pracownicy Ośrodka, z wyjątkiem elektronicznej wersji zbiorów: Karta Dużej Rodziny, SEPI oraz bazy danych programu Emp@tia. Dyrektor Ośrodka prowadziła postępowania z zakresu przyznawania Kart Dużej Rodziny na podstawie pisemnego upoważnienia Burmistrza Ciechanowca z czerwca 2014 roku. Natomiast dane osobowe w SEPI przetwarzano w oparciu o postanowienia porozumienia w sprawie korzystania z Samorządowej Elektronicznej Platformy Informacyjnej, zawartej 15 listopada 2013 r. pomiędzy Dyrektorem OPS i dyrektorem PUP. Uzyskanie dostępu do ww. zbiorów nie wymagało spełnienia przez Ośrodek specjalnych warunków takich, jak np. stworzenie wydzielonego łącza internetowego czy też budowy określonej struktury sieci.

(dowód: akta kontroli str. 10, 91-94, 159-165, 183-188)

Ustalone nieprawidłowości

W działalności kontrolowanej jednostki w przedstawionym wyżej zakresie stwierdzono nieprawidłowość, polegającą na niezaktualizowaniu zgłoszenia rejestracyjnego do GIODO dotyczącego zbioru „Karta Dużej Rodziny", w którym przetwarzano także niezgłoszone dane (nr PESEL oraz serię i nr dowodu osobistego) oraz zbioru „Świadczenia z Pomocy Społecznej" w związku z powierzeniem innemu podmiotowi (PUP) przetwarzania danych w tym zbiorze. Stanowiło to naruszenie przepisu art. 41 ust. 1 pkt 2 i ust. 2 ustawy o ochronie danych osobowych, zgodnie z którym w terminie 30 dni od dokonania zmiany ADO ma obowiązek zgłosić GIODO zmianę zakresu gromadzonych danych w zbiorze. Dyrektor OPS wyjaśniła, że potrzeba przetwarzania obu ww. danych w zbiorze „Karta Dużej Rodziny" wynika wprost z przepisów przedmiotowej ustawy i dlatego przetwarzano te dane, a przeoczonej wcześniej zmiany nie zgłoszono do GIODO, ponieważ do chwili obecnej nie uzyskano jeszcze potwierdzenia zarejestrowania tego zbioru, na mocy zgłoszenia ze stycznia 2016 roku. Jeśli chodzi o uwagi do zbioru „Świadczenia z Pomocy Społecznej", to Dyrektor przyznała, że nie była świadoma takiego obowiązku.

(dowód: akta kontroli str. 11, 16-21, 31-36, 47-50, 159-165)

Ocena cząstkowa

Najwyższa Izba Kontroli ocenia pozytywnie mimo stwierdzonej nieprawidłowości sposób przetwarzania zasobów informacyjnych, który był zgodny z zakresem działalności OPS, 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[15], wnosi o:

1. Nadanie użytkownikom korzystającym ze służbowych komputerów uprawnień odpowiadającym zakresom ich obowiązków.

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

2. Wprowadzenie mechanizmu wymuszenia okresowej zmiany haseł dostępu do urządzeń wykorzystywanych do przetwarzania danych osobowych.
3. Wywiązywanie się z obowiązków określonych w art. 36a ust 2 pkt 1 ustawy o ochronie danych osobowych.
4. Analizowanie i zabezpieczenie przed modyfikacją lub zniszczeniem logów systemów operacyjnych komputerów wykorzystywanych w OPS.
5. Należyte zabezpieczenie danych przetwarzanych w systemach informatycznych, a w szczególności udostępnianie zasobów informacyjnych Ośrodka wyłącznie osobom upoważnionym i przechowywanie kopii zapasowych baz danych systemów dziedzinowych w miejscach gwarantujących zabezpieczenie ich przed uszkodzeniem.
6. Zaktualizowanie danych rejestracyjnych zbiorów „Karta Dużej Rodziny" i „Świadczenia z Pomocy Społecznej" w GIODO.
7. Ujęcie w prowadzonej ewidencji wszystkich osób upoważnionych do przetwarzania danych osobowych i wszystkich elementów określonych w art. 39 ust. 1 pkt 3 ustawy o ochronie danych osobowych.
8. Wywiązywanie się z obowiązków wynikających z § 20 ust. 2 pkt. 2 i 14 rozporządzenia KRI, dotyczących utrzymywania aktualności inwentaryzacji sprzętu i oprogramowania służącego do przetwarzania informacji obejmującej ich rodzaj i konfigurację oraz przeprowadzania corocznych audytów wewnętrznych z zakresu bezpieczeństwa informacji.
9. Zapewnienie szkoleń, o których mowa w § 20 ust. 2 pkt 6 rozporządzenia KRI, dla wszystkich pracowników zaangażowanym w proces przetwarzania informacji.
10. Aktualizację PBI i Instrukcji Zarządzania, w tym uzupełnienie ich stosownie do wymogów § 20 ust. 1 rozporządzenia KRI oraz § 4 pkt 2 – 4 i § 5 pkt 4 – 5 rozporządzenia w sprawie dokumentacji przetwarzania danych osobowych.

V. Pozostałe informacje i pouczenia

Prawo zgłoszenia zastrzeżeń

Wystąpienie pokontrolne zostało sporządzone w dwóch egzemplarzach; jeden dla kierownika 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 12 lutego 2018 r.

Kontroler
Adrian Gosk
specjalista kontroli państwowej
podpis

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