NAJWYŻSZA IZBA KONTROLI
Delegatura w Białymstoku

LBI.410.023.18.2017
P/17/062

02268217

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	Tomasz Ambrozik – doradca ekonomiczny, upoważnienie do kontroli nr LBI/175/2017 z 7 grudnia 2017 r. (dowód: akta kontroli str. 1-2)
Jednostka kontrolowana	Miejski Ośrodek Pomocy Społecznej w Supraślu, 16-030 Supraśl, ul. Józefa Piłsudskiego 17 (dalej „MOPS").
Kierownik jednostki kontrolowanej	Małgorzata Ostrowska – kierownik MOPS[1] (dowód: akta kontroli str. 3)

II. Ocena kontrolowanej działalności[2]

Ocena ogólna

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

Uzasadnienie oceny ogólnej

Ocenę tę uzasadniają stwierdzone nieprawidłowości, polegające w szczególności na:

- nadaniu użytkownikom wszystkich 22 komputerów uprawnień administratora systemu operacyjnego,
- nieanalizowaniu i niezabezpieczeniu przed modyfikacją lub zniszczeniem logów systemów operacyjnych komputerów wykorzystywanych do przetwarzania danych,
- nieprowadzeniu okresowych audytów wewnętrznych z zakresu bezpieczeństwa informacji, o których mowa w § 20 ust. 2 pkt 14 rozporządzeniu 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],
- niedokonaniu aktualizacji zgłoszenia rejestracyjnego do Generalnego Inspektora Ochrony Danych Osobowych[5] dotyczącego zbioru „Pomoc Społeczna", co było niezgodne z przepisem art. 41 ust. 2 ustawy z dnia 29 sierpnia 1997 r. o ochronie danych osobowych[6],
- niewskazaniu w ewidencji osób upoważnionych do przetwarzania danych osobowych zakresu upoważnienia, daty ustania upoważnienia oraz identyfikatora w systemie informatycznym, mimo takiego wymogu określonego w art. 39 ust. 1 pkt 2 i 3 ustawy o ochronie danych osobowych,
- niezapewnieniu szkoleń osobom zaangażowanym w proces przetwarzania informacji, mimo wymogu wynikającego z przepisu § 20 ust. 2 pkt 6 rozporządzenia KRI,
- nieprowadzeniu okresowych analiz ryzyka utraty integralności, dostępności lub poufności informacji, o których mowa w § 20 ust. 2 pkt 3 rozporządzenia KRI.

---

1 Od 1 czerwca 1990 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. Ustawa zwana dalej: „ustawą o ochronie danych osobowych".

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. System informatyczny MOPS zbudowany jest na profesjonalnym routerze marki CISCO. W sieci LAN działają dwa serwery Microsoft Windows Serwer. Na pierwszym z nich posadowiona jest aplikacja finansowo-księgowa, na kolejnym aplikacje dziedzinowe firmy Infor S.A., a na wydzielonej z jego zasobów maszynie wirtualnej – aplikacja księgowa Bestia (firmy Sputnik Software Sp. z o.o.). Na serwerze uruchomiony jest systemowy VPN, który wykorzystywany jest do łączenia z siecią LAN komputerów oddziału zamiejscowego w Zaściankach (cztery komputery).

Równolegle, bez podłączenia do sieci LAN, w MOPS działają dwa serwery: serwer elektronicznego obiegu dokumentów (EZD) oraz powiązany z nim „serwer komunikacyjny". Wymienione urządzenia wraz z urządzeniami sieciowymi zostały umieszczone w wydzielonej, klimatyzowanej serwerowni, dostępnej tylko uprawnionemu personelowi.

Zarządzanie siecią lokalną oparte jest na protokole DHCP ze statyczną adresacją IP, bez filtracji adresów MAC. Na serwerze został zestawiony systemowy VPN, który jest wykorzystany przez pracowników oddziału zamiejscowego i przez administratora do realizacji prac serwisowych na komputerach pracujących w sieci LAN. Na terenie MOPS nie działa sieć WIFI. (dowód: akta kontroli str. 13-15)

W MOPS do przetwarzania danych wykorzystywano sześć systemów informatycznych, (aplikacje: „Helios" i „Kalipso" – Pomoc społeczna, „Izyda" – Świadczenia Wychowawcze, „Amazis" – Świadczenia Rodzinne, „Nemezis" – Fundusz Alimentacyjny i „Cheops" – Dodatki Mieszkaniowe) oraz program „Płatnik". Ponadto przetwarzano dane w dwóch serwisach udostępnionych MOPS, tj. Karta Dużej Rodziny[7] oraz Samorządowa Elektroniczna Platforma Informacyjna[8]. Każdy z 22 komputerów posiadał dostęp do Internetu, co było zgodne z warunkami określonymi w dokumentacji tych systemów.
(dowód: akta kontroli str. 6-7)

1.2. W okresie objętym kontrolą w MOPS nie przeprowadzano okresowych analiz ryzyka utraty integralności, dostępności lub poufności informacji, co szerzej opisano w dalszej części wystąpienia pokontrolnego, w sekcji „Ustalone nieprawidłowości".
(dowód: akta kontroli str. 8-10)

1.3. Według stanu na 11 stycznia 2018 r., wszystkich 23 pracowników MOPS zaangażowanych było w proces przetwarzania danych osobowych w stopniu adekwatnym do realizowanych zadań, wynikających z ich zakresów obowiązków. Posiadali oni stosowne upoważnienia Kierownika MOPS – Administratora Danych Osobowych[9], do przetwarzania danych osobowych w zbiorach, do których mieli dostęp.

W okresie objętym kontrolą w MOPS nie zachodziły okoliczności (np.: zmiana zakresu obowiązków lub zwolnienie), które wymagałyby dokonywania zmiany uprawnień użytkowników w systemach wykorzystywanych do przetwarzania danych.
(dowód: akta kontroli str. 16-21)

Każdy z pracowników zaangażowanych w przetwarzanie danych w systemach informatycznych MOPS posiadał własny login i hasło do systemów dziedzinowych zainstalowanych na jednostkach komputerowych, które to systemy wykorzystywano do przetwarzania danych osobowych. Użytkownikom wszystkich 22 komputerów nadano jednak uprawnienia administratora systemu operacyjnego tych urządzeń, co szerzej opisano w dalszej części wystąpienia pokontrolnego, w sekcji „Ustalone nieprawidłowości".
(dowód: akta kontroli str. 11-15 i 30-41)

1.4. Ustalenia biegłego (powołanego przez NIK) wskazują, że w MOPS nie był prowadzony rejestr dostępu do systemów informatycznych wykorzystywanych do przetwarzania danych.

---

[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".

Na każdym z komputerów system operacyjny domyślnie gromadził logi systemowe dla danego urządzenia na własnym dysku lokalnym (rejestr zdarzeń systemu Windows). Logi te nie były zabezpieczane przed modyfikacją, nie były agregowane ani analizowane. Szerzej nieprawidłowości w zakresie monitorowania dostępu do systemu opisano w dalszej części wystąpienia pokontrolnego, w sekcji „Ustalone nieprawidłowości".

(dowód: akta kontroli str. 11-15)

1.5. Ustalenia biegłego wskazują, że środkiem zabezpieczającym przed nieautoryzowanym dostępem do wszystkich systemów operacyjnych komputerów było hasło użytkownika, przy czym nie aktywowano mechanizmu okresowego wymuszania jego zmiany. Aplikacje dziedzinowe wykorzystywane w MOPS posiadały wymuszenie zmiany hasła co 30 dni. W MOPS nie działała sieć WI-FI. Urządzenia sieciowe były zabezpieczone przed fizyczną ingerencją osób do tego nieupoważnionych z racji umieszczenia ich w przeznaczonym do tego pomieszczeniu – serwerowni. (dowód: akta kontroli str. 11-15)

1.6. W MOPS nie wprowadzono regulacji umożliwiających wykorzystanie przez pracowników prywatnego sprzętu komputerowego do pracy nad zadaniami powierzonymi w ramach obowiązków służbowych. Biegły stwierdził, że konfiguracja sieciowa umożliwia podłączenie do infrastruktury jednostki sprzętu (laptopy, telefony, tablety) niestanowiącego własności pracodawcy. Informacje o podłączeniu do komputerów nośników pamięci (np. pendrive lub dysk przenośny) były domyślnie zapisywane w logach systemu komputerowego. Router, na którym zbudowano sieci LAN, gromadził w logach informacje o urządzeniach, które były podłączane do sieci. (dowód: akta kontroli str. 11-15)

W trakcie oględzin stwierdzono, że do sieci MOSP nie były podłączone urządzenia nie będące jego własnością. (dowód: akta kontroli str. 151-152)

1.7. W okresie objętym kontrolą w MOPS nie ujawniono przypadków wykrycia nieautoryzowanych działań związanych z przetwarzaniem informacji. Nie wystąpiła również potrzeba przywrócenia danych z wykonanych kopii bezpieczeństwa.

(dowód: akta kontroli str. 28-29)

1.8. W MOPS nie wprowadzono regulacji wewnętrznych dotyczących bezpiecznej pracy przy przetwarzaniu mobilnym. Praca taka była możliwa na terminalu mobilnym przekazanym do Ośrodka[10] w ramach realizacji projektu Emp@tia – „Platforma komunikacyjna obszaru zabezpieczenia społecznego". Kierownik MOPS wyjaśniła, że: *„Do dnia dzisiejszego nie rozpoczęto pracy na terminalach mobilnych. W najbliższym czasie zostaną opracowane regulacje wewnętrzne związane z w/w zagadnieniem i pracownicy socjalni zaczną korzystać z terminali mobilnych"*.

Biegły stwierdził, że w MOPS przewidziano zdalny dostęp do zasobów sieci lokalnej przez pracowników i taki dostęp funkcjonował. Opierał się on o systemowy VPN, zestawiony na serwerze pracującym na środowisku Microsoft Windows Serwer 2012. Autoryzacja przy korzystaniu z VPN odbywała się przez podanie loginu i hasła użytkownika.

(dowód: akta kontroli str. 8-15, 30-41 i 134-135)

1.9. MOPS nie zawierał z podmiotami zewnętrznymi umów, których przedmiotem był serwis urządzeń komputerowych. Natomiast na dzień rozpoczęcia kontroli NIK miał zawarte dwie umowy serwisu oprogramowania. W każdej z tych umów zawarto regulacje zobowiązujące wykonawcę umowy do zachowania w tajemnicy i nieudostępniania danych osobowych przekazanych przez MOPS. (dowód: akta kontroli str. 8-10, 104-109 i 118-125)

1.10. Wszystkie komputery (22) wchodzące w skład sieci lokalnej były zabezpieczone dedykowanym do tego celu oprogramowaniem antywirusowym bądź systemowym narzędziem producenta systemu operacyjnego (cztery komputery z MS Windows 10). Biegły stwierdził, że badane komputery posiadały aktualne wersje aplikacji zabezpieczających. (dowód: akta kontroli str. 11-15)

1.11. W okresie objętym kontrolą MOPS nie zawierał umów dotyczących świadczenia usług poczty elektronicznej. Dwadzieścia dwa stanowiska komputerowe MOPS umożliwiały dostęp do poczty elektronicznej, w tym do głównej skrzynki email, znajdującej się

[10] Na podstawie umowy użyczenia Nr 12/20/EMP/2013 z 23 grudnia 2013 r.

na serwerze, udostępnionym przez firmę zewnętrzną (Merinosoft Sp. z o. o. w Białymstoku), na podstawie umowy zawartej w 1999 roku. (dowód: akta kontroli str. 8-10)

1.12. Zgodnie z postanowieniami Instrukcji zarządzania systemem informatycznym, w MOPS codziennie były wykonywane całościowe kopie bezpieczeństwa dwóch serwerów pracujących w LAN – codziennie nadpisywany był backup z dnia poprzedniego. Raz w tygodniu wykonywany był backup baz danych. Backupy zapisywano na urządzeniu klasy NAS, umieszczonym w serwerowni. Wspomniane urządzenie było na stałe wpięte do sieci. (dowód: akta kontroli str.11-15)

1.13. Biegły stwierdził, że pracownicy MOPS dysponują możliwością ściągania aplikacji i plików wykonalnych oraz posiadają uprawnienia do ich instalowania na stacjach komputerowych, do których mają dostęp. Każdy z użytkowników posiadał uprawnienia administratora systemu operacyjnego jednostek komputerowych, na których wykonywał obowiązki służbowe, co szerzej opisano w dalszej części wystąpienia pokontrolnego, w sekcji „Ustalone nieprawidłowości".

Na czterech (z 22) komputerach zainstalowany był system operacyjny nieposiadający wsparcia technicznego producenta, co szerzej opisano w dalszej części wystąpienia pokontrolnego, w sekcji „Uwagi dotyczące badanej działalności".

(dowód: akta kontroli str. 11-15 i 30-41)

1.14. Biegły stwierdził, że 18 z 22 komputerów posiadało aktualne wersje systemów operacyjnych[11]. Aktualizacje były wykonywane zgodnie z harmonogramem domyślnie ustawionym przez dostawcę systemu operacyjnego. Aktualne były również aplikacje dziedzinowe. Tryb ich aktualizacji wynikał również z domyślnych ustawień producenta.

(dowód: akta kontroli str. 11-15)

1.15. W MOPS regulacje dotyczące wykonywania płatności (przelewów) drogą elektroniczną zostały określone w załączniku Nr 6 (Instrukcja obiegu i kontroli dokumentów) do zarządzenia Nr 021.9.2016 Kierownika MOPS z 19 kwietnia 2016 r. Płatności realizowane były za pośrednictwem elektronicznego systemu zdalnej obsługi bankowej. Dane przekazywane między MOPS a bankiem były przesyłane łączem szyfrowanym. Realizacja zleconych przez MOPS przelewów była wykonywana przez upoważnionych pracowników, którzy posiadali klucze autoryzujące, zabezpieczone kodami PIN.

(dowód: akta kontroli str. 8-10 i 129-133)

Ustalone nieprawidłowości

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

1. Użytkownikom wszystkich 22 komputerów nadano uprawnienia administratora systemu operacyjnego tych urządzeń, mimo że zgodnie z ich zakresem 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, 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. Kierownik MOPS wyjaśniła, że: *„Użytkownicy komputerów posiadają uprawnienia administratora, aby mieć możliwość bieżącej aktualizacji programów dziedzinowych info-r (są to 22 komputery w 3 lokalizacjach, gdzie odległości od siedziby głównej Ośrodka wynosi ok. 15 km w jedną stronę). Aktualizacje te są ogłaszane na www producenta w nieprzewidywalnych terminach, często jest to kilka oddzielnych aktualizacji dziennie, co kilka godzin. Niewykonanie aktualizacji na stacji roboczej uniemożliwia pracę na danym komputerze. Ponieważ Ośrodek nie zatrudnia informatyka na etacie (nie ma takich możliwości finansowych) a jedynie na umowę zlecenia, co sprawiło, że aby zapewnić wykonanie wszystkich zadań w wyznaczonych terminach, udzielono pracownikom uprawnień administratorów, które*

[11] Z wyłączeniem czterech komputerów z zainstalowanym systemem operacyjnym Windows XP.

to uprawnienia służyły tylko i wyłącznie do ściągania aktualizacji programów dziedzinowych. Zrobiono to, aby zapewnić ciągłość wykonywania zadań obarczonych krótkim terminem realizacji i dużą presją organów nadrzędnych i środowisk korzystających ze świadczeń realizowanych przez MOPS".

Najwyższa Izba Kontroli zwraca jednak uwagę, że przyznanie wszystkim pracownikom uprawnień administratora systemu operacyjnego, przy jednoczesnym braku odpowiednio wykwalifikowanej kadry do realizacji wszystkich zadań związanych z ochroną danych, stwarza ryzyko obniżenia skuteczności ochrony danych przetwarzanych w MOPS. (dowód: akta kontroli str. 11- 15, 22-27 i 30-41)

2. W MOPS nie był prowadzony rejestr dostępu do systemów informatycznych. Każdy z komputerów domyślnie (rejestr zdarzeń systemu Windows) gromadził swoje logi systemowe na własnym dysku lokalnym. W opinii biegłego, logi te nie były zabezpieczane przed modyfikacją, nie były agregowane ani też automatycznie analizowane. W MOPS logi ruchu sieciowego gromadzono na routerze, ale nie były one analizowane. Nie zastosowano żadnych środków, które chroniłyby gromadzące się na komputerach logi przed utratą integralności lub skasowaniem, tj.: logi nie były objęte procesem tworzenia kopii danych (nie były backupowane) Ich trwałość zależała od ustawień producenta systemu, co stwarza zagrożenie, że mogą zostać skasowane lub nadpisane, uniemożliwiając odtworzenie tego co działo się z zasobami. Nie gromadzono ich centralnie na głównym serwerze jednostki, nie wprowadzono także harmonogramu tworzenia backupów logów. Zgodnie z przepisem § 20 ust. 2 pkt 7 lit. a rozporządzenia KRI, monitorowanie dostępu do informacji jest jednym z elementów zarządzania bezpieczeństwem informacji, zmierzającym do zapewnienia ochrony przetwarzanych informacji przed ich kradzieżą, nieuprawnionym dostępem, uszkodzeniami lub zakłóceniami. W wyjaśnieniu Kierownik MOPS stwierdziła, że: *„Logi systemowe na stacjach roboczych nie były zabezpieczane przed modyfikacją, nie były agregowane, automatycznie analizowane, ani backupowane, ponieważ uznano, że logi na stacjach roboczych nie wymagają dodatkowego zabezpieczania. Logi te są od dnia 11 stycznia 2018 r. backupowane i analizowane za pomocą programu Axence nVision".*
(dowód: akta kontroli str.11-15 i 22-27)

3. W okresie objętym kontrolą w MOPS nie przeprowadzano okresowych analiz ryzyka utraty integralności, dostępności lub poufności informacji, co stanowiło naruszenie przepisu § 20 ust. 2 pkt 3 rozporządzenia KRI. W wyjaśnieniu Kierownik MOPS podała: *„w natłoku wielu zadań i obowiązków przeoczono konieczność przeprowadzania takiej analizy".* (dowód: akta kontroli str. 8-10 i 22-27)

Uwagi dotyczące badanej działalności

Najwyższa Izba Kontroli zwraca uwagę, że w MOPS wykorzystywano cztery z 22 komputerów z zainstalowanym systemem operacyjnym Windows XP, mimo że z dniem 8 kwietnia 2014 r. producent oprogramowania zakończył udzielanie wsparcia technicznego dla tego systemu. W wyjaśnieniu Kierownik MOPS podała, że: *„Wymiana komputerów jest procesem w toku. Brak jest funduszy na jednorazową wymianę pozostałych pięciu stanowisk – wymiana systemu operacyjnego XP na 10 wiąże się z wymianą całej jednostki centralnej. W najbliższym czasie komputery te zostaną wymienione na komputery z Windows 10".* (dowód: akta kontroli str. 11-15, 22-27 i 30-41)

Ocena cząstkowa

Najwyższa Izba Kontroli ocenia negatywnie skuteczność przyjętych w MOPS 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. W MOPS prowadzono 10 zbiorów danych osobowych (wszystkie w wersji papierowej i w formie elektronicznej). Do GIODO zgłoszono wszystkie zbiory danych, w tym dwa („Program Rodzina 500 plus" i Wsparcie kobiet w ciąży i rodzin „Za życiem") w okresie objętym kontrolą. Analiza tych dwóch zgłoszeń wykazała, że zawarto w nich elementy wymagane przepisem art. 41 ust. 1 ustawy o ochronie danych osobowych. Zakres danych we wszystkich zarejestrowanych zbiorach odpowiadał zakresowi, w jakim były one przetwarzane. W 2017 roku MOPS dokonał aktualizacji zbiorów już zgłoszonych do GIODO. Nie dokonano natomiast aktualizacji zgłoszenia rejestracyjnego do GIODO dotyczącego

zbioru „Pomoc społeczna", w związku z powierzeniem innemu podmiotowi przetwarzania danych w tym zbiorze, co szerzej opisano w pkt 4.3. wystąpienia pokontrolnego. W okresie objętym kontrolą nie wystąpiły przypadki odmowy rejestracji przez GIODO zgłaszanych zbiorów danych. MOPS nie występował do GIODO o wykreślenie z rejestru zbiorów danych osobowych. (dowód: akta kontroli str. 6-10 i 136-150)

2.2. W okresie objętym kontrolą w MOPS nie skorzystano z możliwości powołania Administratora Bezpieczeństwa Informacji (dalej: „ABI"), o którym mowa w art. 36a ust. 1 ustawy o ochronie danych osobowych. Kierownik MOPS wyjaśniła: *„Nie wyznaczyłam Administratora Bezpieczeństwa Informacji, ponieważ nie było takiej potrzeby".*
(dowód: akta kontroli str. 8-10 i 22-27)

2.3. Stosownie do 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. W okresie objętym kontrolą ADO podejmował następujące działania wynikające z art. 36a ust. 2 ustawy o ochronie danych osobowych: [1] w kwietniu 2016 roku i w grudniu 2017 roku opracował Politykę bezpieczeństwa i Instrukcję zarządzania systemem informatycznym, [2] opracował wykaz pomieszczeń tworzących obszar przetwarzania danych osobowych, [3] sporządził wykaz zbiorów danych osobowych wraz ze wskazaniem programów zastosowanych do ich przetwarzania, [4] prowadził ewidencję osób upoważnionych do przetwarzania danych osobowych. [5] opracował i pobrał oświadczenia o zapoznaniu pracowników MOPS, upoważnionych do przetwarzania danych osobowych, z przepisami o ochronie danych osobowych. W dokumentacji MOPS nie ma dowodów potwierdzających wykonywanie przez ADO zadania polegającego na sprawdzeniu zgodności przetwarzania danych osobowych z przepisami o ich ochronie (art. 36a ust. 2 pkt 1 lit. a ustawy o ochronie danych osobowych). W wyjaśnieniu Kierownik MOPS stwierdziła, że: *„Prowadziłam bieżący stały nadzór i kontrolę zgodności przetwarzania danych osobowych przez podległych pracowników z przepisami o ochronie danych osobowych. Nie dokumentowałam swoich działań i czynności w tym zakresie, ponieważ były to działania ciągłe nie wymagające takiego dokumentowania".* (dowód: akta kontroli str. 16-21, 22-27, 42-91 i 154-160)

2.4. Zgodnie z przepisem art. 39 ust. 1 ustawy o ochronie danych osobowych, w MOPS prowadzono ewidencję osób upoważnionych do przetwarzania danych osobowych. Do 7 grudnia 2017 r. w ewidencji nie zawarto zakresu upoważnienia tych osób, daty ustania upoważnienia oraz identyfikatora w systemie informatycznym, co szerzej opisano w dalszej części wystąpienia pokontrolnego, w sekcji „Ustalone nieprawidłowości". Ewidencja od 8 grudnia 2017 r. spełnia wymagania przepisu art. 39 ust. 1 pkt 1 – 3 ustawy o ochronie danych osobowych. (dowód: akta kontroli str. 154-160)

Analiza zakresów obowiązków wszystkich 23 pracowników MOPS (ujętych w ewidencji) i wydanych dla nich upoważnień wykazała, że posiadali oni dostęp do zbiorów danych osobowych wynikający z zakresów obowiązków oraz upoważnienia do przetwarzania danych. (dowód: akta kontroli str. 16-21)

2.5. W MOPS od 8 grudnia 2017 r. obowiązują następujące akty administracyjne dotyczące gromadzenia i przetwarzania zasobów informacyjnych: Polityka bezpieczeństwa i Instrukcja zarządzania systemem informacyjnym, wprowadzone zarządzeniem Nr 021.6.2017 Kierownika MOPS z 8 grudnia 2017 r. Z tym dniem zostało uchylone uprzednio obowiązujące zarządzenie Nr 021.7.2016 Kierownika MOPS z 19 kwietnia 2016 r. w sprawie dokumentacji oraz warunków technicznych i organizacyjnych, jakim powinny odpowiadać urządzenia i systemy informatyczne służące do przetwarzania danych osobowych. (dowód: akta kontroli str. 42-90)

2.6. Kierownik MOPS, wykonując dyspozycje określone w Instrukcji zarządzania systemem informatycznym, od 12 stycznia 2016 r. umową zlecenia powierzyła osobie fizycznej wykonywanie zadań ASI. Kierownik MOPS upoważniła ASI do obsługi systemu informatycznego i urządzeń wchodzących w jego skład, służących przetwarzaniu danych osobowych. Do obowiązków ASI należało m.in.: [1] wykonywanie serwisu technicznego zestawów mikrokomputerowych posiadanych przez MOPS, [2] zapewnienie prawidłowego funkcjonowania serwerów i zabezpieczenie ich przed niepowołanym dostępem,

[3] administrowanie prawami dostępu do całości systemu, [4] zapewnienie prawidłowego funkcjonowania serwera dostępowego do Internetu, [5] usprawnienie działania istniejących systemów komputerowych i telefonicznych, [6] przeszkolenie pracowników MOPS w zakresie obsługi systemów komputerowych. (dowód: akta kontroli str. 161-172)

2.7. W MOPS nie wywiązano się z obowiązku prowadzenia corocznych audytów wewnętrznych z zakresu bezpieczeństwa informacji, wynikającego z przepisu § 20 ust. 2 pkt. 14 rozporządzenia KRI, co szerzej opisano w dalszej części wystąpienia pokontrolnego, w sekcji „Ustalone nieprawidłowości". (dowód: akta kontroli str. 8-10)

2.8. Do 31 grudnia 2017 r. nie przeszkolono 19 z 23 pracowników MOPS z zagadnień w zakresie ochrony danych osobowych oraz bezpieczeństwa informacji, co szerzej opisano w dalszej części wystąpienia pokontrolnego, w sekcji „Ustalone nieprawidłowości". (dowód: akta kontroli str. 8-10 i 22-27)

2.9. W okresie objętym kontrolą w MOPS nie były prowadzane kontrole w zakresie bezpieczeństwa danych osobowych. Nie wpłynęły również skargi dotyczące tej problematyki. (dowód: akta kontroli str. 8-10)

2.10. Zarządzeniem Nr 021.7.2016 Kierownika MOPS z 16 kwietnia 2016 r. wprowadzono do stosowania w MOPS Politykę bezpieczeństwa i Instrukcję zarządzania systemem informatycznym. Wymienione zarządzenie zostało uchylone z dniem 8 grudnia 2017 r. W tym dniu Kierownik MOPS wydała zarządzenie Nr 021.6.2017, które wprowadziło w życie aktualnie obowiązujące dokumenty określające sposób przetwarzania danych osobowych oraz warunków technicznych i organizacyjnych, jakim powinny odpowiadać urządzenia i systemy informatyczne służące do przetwarzania danych osobowych, tj.: Politykę bezpieczeństwa i Instrukcję zarządzania systemem informatycznym.

W styczniu 2017 roku MOPS przeniósł swoją siedzibę z ul Józefa Piłsudskiego 58 na ul. Józefa Piłsudskiego Nr 17 w Supraślu. Tak więc, w MOPS przez ponad 10 miesięcy od zmiany siedziby obowiązywały dokumenty (Polityka bezpieczeństwa i Instrukcji zarządzania systemem informatycznym), które w części były nieaktualne, co szerzej opisano w dalszej części wystąpienia pokontrolnego, w sekcji „Ustalone nieprawidłowości". (dowód: akta kontroli str. 42-90)

Natomiast aktualnie obowiązujące od 8 grudnia 2017 r. Polityka bezpieczeństwa i Instrukcja zarządzania systemem informatycznym spełniały wymagania określone w przepisach § 4 pkt 1 – 5 i § 5 pkt 1 – 8 rozporządzenia Ministra Spraw Wewnętrznych i Administracji z dnia 29 kwietnia 2004 r. w sprawie w dokumentacji przetwarzania danych osobowych oraz warunków technicznych i organizacyjnych, jakim powinny odpowiadać urządzenia i systemy informatyczne służące do przetwarzania danych osobowych[12].

W Instrukcji zarządzania systemem informatycznym określono poziom bezpieczeństwa przetwarzania danych osobowych w systemach informatycznych MOPS jako wysoki, co było zgodne z przepisem § 6 ust. 1 pkt 3 rozporządzenia w sprawie dokumentacji oraz warunków technicznych. (dowód: akta kontroli str. 42-66)

Regulacje składające się na politykę bezpieczeństwa informacji (Polityka bezpieczeństwa i Instrukcja zarządzania systemem informatycznym) odpowiadały wymogom przepisu § 2 pkt 15 w związku z § 20 ust. 1 rozporządzenia KRI. (dowód: akta kontroli str. 42-66)

Ustalone nieprawidłowości

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

1. Do 7 grudnia 2017 r. w ewidencji osób upoważnionych do przetwarzania danych osobowych, wbrew wymogom określonym w przepisie art. 39 ust. 1 pkt 2 i 3 ustawy o ochronie danych osobowych, nie wskazano zakresu upoważnienia tych osób, daty ustania upoważnienia oraz identyfikatora w systemie informatycznym. W wyjaśnieniu Kierownik MOPS stwierdziła, że: *„przeoczono wymóg zawarcia w ewidencji osób upoważnionych do przetwarzania danych osobowych zakresu upoważnienia, daty ustania upoważnienia oraz identyfikatora w systemie informatycznym. Zgodnie*

[12] Dz. U. Nr 100 poz. 1024. Rozporządzenie zwane dalej „rozporządzeniem w sprawie dokumentacji oraz warunków technicznych".

z obowiązującym obecnie Zarządzeniem Nr 021.6.2017 Kierownika Miejskiego Ośrodka Pomocy Społecznej w Supraślu z dnia 08 grudnia 2017r. w sprawie dokumentacji określającej sposób przetwarzania danych osobowych oraz warunków technicznych i organizacyjnych, jakim powinny odpowiadać urządzenia i systemy informatyczne służące do przetwarzania danych osobowych w Miejskim Ośrodku Pomocy Społecznej w Supraślu, od dnia 08 grudnia 2017r. ewidencja osób upoważnionych zawiera wszystkie niezbędne elementy wynikające z ustawy o ochronie danych osobowych".

(dowód: akta kontroli str. 22-27 i 154-160)

2. W MOPS nie przeprowadzano okresowych audytów wewnętrznych z zakresu bezpieczeństwa informacji, co stanowiło naruszenie przepisu § 20 ust. 2 pkt. 14 rozporządzenia KRI. W wyjaśnieniu Kierownik MOPS stwierdziła, że: *„w natłoku wielu zadań i obowiązków przeoczono konieczność dokonanie audytu. Jednakże na bieżąco stale monitorowano elementy z zakresu bezpieczeństwa informacji".*

(dowód: akta kontroli str. 8-10 i 22-27)

3. W MOPS przez ponad 10 miesięcy od zmiany siedziby (styczeń 2017 roku) obowiązywały dokumenty, wprowadzone w życie zarządzeniem Nr 021.7.2016 Kierownika MOPS z 16 kwietnia 2016 r., tj. Polityka bezpieczeństwa i Instrukcja zarządzania systemem informatycznym, które w części były nieaktualne. Na przykład w Polityce bezpieczeństwa nieaktualne były postanowienia dotyczące obszaru przetwarzania danych osobowych, czy też wykazu zbiorów danych osobowych. Nieaktualny był również wykaz budynków i pomieszczeń tworzących obszar, w którym były przetwarzane dane osobowe. Z kolei uregulowania Instrukcji zarządzania systemem informatycznym były nieaktualne w części dotyczącej nazwy sieci, do której są podłączone komputery. Było to sprzeczne z przepisem § 20 ust. 2 pkt 1 rozporządzenia KRI, zgodnie z którym zapewnia się aktualizację regulacji wewnętrznych w zakresie dotyczącym zmieniającego się otoczenia. Kierownik MOPS wyjaśniła, że: *„Polityka bezpieczeństwa przetwarzania danych osobowych i Instrukcja zarządzania systemem informatycznym służącym do przetwarzania danych osobowych zostały wprowadzone do stosowania w MOPS 8 grudnia 2017 r., to jest po upływie 10 miesięcy od zmiany siedziby, z powodu kumulacji zadań związanych ze zmianą siedziby oraz stale rosnącą ilością powierzanych do realizacji zadań. Mieliśmy stale obowiązujące Zarządzenie Nr 021.7.2016 Kierownika Miejskiego Ośrodka Pomocy Społecznej w Supraślu z dnia 19 kwietnia 2016 r. w sprawie dokumentacji określającej sposób przetwarzania danych osobowych oraz warunków technicznych i organizacyjnych, jakim powinny odpowiadać urządzenia i systemy informatyczne służące do przetwarzania danych osobowych w Miejskim Ośrodku Pomocy Społecznej w Supraślu. Mimo braku nowej polityki bezpieczeństwa, wszystkie systemy i dane klientów były chronione w najlepszy, możliwy do zrealizowania sposób".* (dowód: akta kontroli str. 42-90 i 22-27)

4. W MOPS, poza czterema pracownikami, którzy w latach 2014 – 2015 uczestniczyli w szkoleniach dotyczących problematyki ochrony danych osobowych, pozostałych 19 pracowników nie zostało przeszkolonych w zakresie ochrony danych oraz 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. Z wyjaśnienia Kierownika MOPS wynika, że w latach 2016 – 2017 pracownicy nie korzystali ze szkoleń dotyczących ochrony danych osobowych organizowanych przez podmioty zewnętrzne. Jednak w tego typu szkoleniach część z nich uczestniczyła w latach 2014 – 2015. I tak:
   - w 2014 roku trzech pracowników (w tym Kierownik MOPS) brało udział w szkoleniach o następującej tematyce: „Ochrona Danych Osobowych (pojęcia, obowiązki, uprawnienia oraz przegląd orzecznictwa GIODO i sądów administracyjnych)", „Przygotowanie jednostki organizacyjnej do kontroli GIODO z uwzględnieniem wybranych elementów audytu bezpieczeństwa informacji" oraz "Opracowanie polityki bezpieczeństwa informacji w jednostce organizacyjnej – wdrożenia, aktualizacja",

– w 2015 roku dwóch pracowników (w tym Kierownik MOPS) zostało przeszkolonych w tematach: „Realizacja zapisów ustawy o ochronie danych osobowych po nowelizacji" i „Ochrona danych osobowych, zmiany w statusie ABI, nowe spojrzenie na ADO, praktyczne wskazówki i zalecenia".

Ponadto w dniu 22 stycznia 2018 r. Kierownik MOPS weźmie udział w szkoleniu: „Zadania użytkowników, Inspektora ODO i Administratora Danych w świetle zmian RODO 2018".

W dalszej części wyjaśnienia Kierownik MOPS stwierdziła, że: *„Po każdym szkoleniu, w ramach szkoleń wewnętrznych, osoby przeszkolone przekazywały pozostałym pracownikom wiedzę zdobytą na szkoleniach tak, aby wszyscy pozostali pracownicy wiedzieli o zmieniających się przepisach, ale przede wszystkim o ich obowiązkach wynikających z ustawy o ochronie danych osobowych. Spotkania nie były protokołowane. W ramach spotkań z pracownikami omawiano między innymi zagadnienia z zakresu ochrony danych osobowych".*

(dowód: akta kontroli str. 8-10 i 22-27)

Ocena cząstkowa

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

3. Sposób przechowywania oraz zabezpieczenia danych

Opis stanu faktycznego

3.1. Zgodnie z postanowieniami Polityki bezpieczeństwa, obszarem przetwarzania danych osobowych w MOPS są pomieszczenia w budynku w Supraślu (ul. Józefa Piłsudskiego 17), pomieszczenia będące siedzibą pracowników socjalnych w Zaściankach (ul. Szosa Baranowicka 37) oraz pomieszczenia na I piętrze Filii Urzędu Miejskiego w Zaściankach (ul. Szosa Baranowicka 58/4). Przyjęte rozwiązania określały środki ochrony fizycznej, wskazując m.in., że: [1] pomieszczenia, które należą do obszaru przetwarzania danych wyposażone są w zamknięcia; [2] w czasie, gdy nie znajdują się w nich osoby upoważnione, pomieszczenia są zamykane w sposób uniemożliwiający wstęp osobom nieupoważnionym; [3] w obszarze, w którym są przetwarzane dane osobowe, osoby nieupoważnione mogą przebywać tylko za zgodą ADO lub w obecności osób upoważnionych; [4] budynek MOPS jest wyposażony w system alarmowy i monitorujący; [5] tymczasowe wydruki z danymi osobowymi po ustaniu ich przydatności są niszczone w niszczarkach; [6] dokumenty zawierające dane osobowe są przekazywane do archiwum zakładowego; [7] zbiory danych, przetwarzane przez MOPS znajdują się na stacjach dedykowanych (serwerach) bądź na stacjach roboczych podłączonych do sieci lokalnej LAN. Serwery znajdują się w wydzielonym pomieszczeniu z ograniczonym dostępem. (dowód: akta kontroli str. 42-66)

Oględziny pomieszczeń MOPS w Supraślu, w których przetwarzane były zbiory danych osobowych, wykazały, że: [1] przetwarzanie danych odbywało się w miejscach do tego wyznaczonych; [2] urządzenia (stacje komputerowe) znajdowały się w pomieszczeniach zabezpieczonych zamkami; [3] stacje komputerowe wykorzystywane do przetwarzania danych wyposażone były w zabezpieczenia na wypadek zaniku napięcia (UPS); [4] kopie zapasowe systemów dziedzinowych były przechowywane w serwerowni, a wejście do tego pomieszczenia było możliwe po wprowadzeniu kodu; [5] nie ustalono pisemnych zasad gospodarki kluczami do pomieszczeń i szaf, w których przechowywano zbiory danych; [6] klucze do szaf po zakończeniu pracy każdy pracownik zabezpieczał osobiście; [7] klucze do wejścia głównego MOPS były w posiadaniu Kierownika oraz wyznaczonych czterech pracowników; [8] drzwi do poszczególnych pomieszczeń MOPS posiadały możliwość zamknięcia na klucz; [9] w MOPS nie zainstalowano monitoringu wizyjnego. Był natomiast zainstalowany system przeciwpożarowy (w budynku parterowym był zamontowany hydrant oraz umieszczono dwie gaśnice, w tym jedną w serwerowni) i przeciwwłamaniowy; [10] wszystkie pomieszczenia znajdowały się na parterze, a okna nie posiadały zabezpieczeń antywłamaniowych i krat metalowych, przy czym okna w dwóch pomieszczeniach były wyposażone w funkcję zamknięcia na klucz; [11] papierowa część wszystkich 10 zbiorów danych osobowych przechowywana była w szafach zamykanych na klucz; [12] pomieszczenie archiwum znajdowało się na parterze, w Szkole Podstawowej w Supraślu. (dowód: akta kontroli str. 151-152)

3.2. W MOPS, stosownie do wymogów § 20 ust. 2 pkt 2 rozporządzenia KRI, prowadzono wykaz urządzeń wykorzystywanych do przetwarzania danych osobowych, który zawierał między innymi: informacje o rodzaju sprzętu, zainstalowanych systemach operacyjnych i programach, nazwę firmy, która opracowała dany system, datę zainstalowania systemu na komputerze, numer seryjny oraz komu dany sprzęt został przyporządkowany.
(dowód: akta kontroli str. 173-177)

3.3. W okresie objętym kontrolą w MOPS nie dokonywano likwidacji sprzętu komputerowego, będącego nośnikiem danych. Nie dokonywano również naprawy sprzętu przez podmioty zewnętrzne. (dowód: akta kontroli str. 8-10)

3.4. Do niszczenia dokumentów zawierających dane osobowe wykorzystywane były cztery niszczarki, które znajdowały się w pomieszczeniach nr 3, 7, 10 i 12, stanowiących obszar przetwarzania danych osobowych. Rozwiązanie to było zgodne z regulacjami określonym w Polityce bezpieczeństwa. (dowód: akta kontroli str. 151-152)

3.5. W Polityce bezpieczeństwa i w Instrukcji zarządzania systemem informatycznym nie określono procedur dotyczących użytkowania komputerów przenośnych. Na wyposażeniu MOPS były dwa laptopy (terminale mobilne) otrzymane z Ministerstwa Pracy i Polityki Społecznej w ramach projektu Emp@tia – „Platforma komunikacyjna obszaru zabezpieczenia społecznego", co zostało szerzej opisane w pkt 1.8. niniejszego wystąpienia pokontrolnego. (dowód: akta kontroli str. 8-10 i 30-41)

3.6. W MOPS nie wprowadzono procedur dotyczących sprzątania pomieszczeń, w których przetwarzano dane osobowe. Sama czynność odbywała się po godzinach pracy. Osoby sprzątające pomieszczenia MOPS zostały zobowiązane do przestrzegania danych ustawowo chronionych (dowód: akta kontroli str. 8-10 i 160)

3.7. Procedury wykonywania przeglądów i konserwacji systemów oraz nośników informacji służących do przetwarzania danych zostały ujęte w *„Instrukcji zarządzania systemami informatycznymi"* w MOPS. Wskazano w nich m.in., że: [1] przeglądy i konserwacje urządzeń wchodzących w skład systemu informatycznego powinny być wykonywane w terminach określonych przez producenta sprzętu, [2] jeśli producent nie przewidział dla danego urządzenia potrzeby dokonywania przeglądów eksploatacyjnych lub też nie określił ich częstotliwości, to o dokonaniu przeglądu oraz sposobie jego przeprowadzenia decyduje ASI, [3] nieprawidłowości ujawnione w trakcie przeglądów bądź konserwacji powinny być niezwłocznie usunięte, a ich przyczyny przeanalizowane. O fakcie ujawnienia nieprawidłowości należy powiadomić ADO. W procedurze wskazano również, że za terminowość przeprowadzenia przeglądów i konserwacji oraz ich prawidłowy przebieg odpowiada ASI. (dowód: akta kontroli str. 59-66)

3.8. W MOPS nie opracowano regulacji wewnętrznych dotyczących rozwiązań na wypadek wystąpienia sytuacji nadzwyczajnych, np. długotrwałego braku zasilania bądź przywracania systemów po awarii. Nie opracowano także planu ciągłości działania umożliwiającego kontynuację wykonywania zadań publicznych przez MOPS, co szerzej opisano poniżej, w sekcji „Uwagi dotyczące badanej działalności". Kierownik MOPS wyjaśniła, że: *„nie wiedzieliśmy o obowiązku opracowania takiej regulacji"*.

W sytuacji braku zasilania możliwość kilkunastominutowej pracy zapewniały urządzenia typu UPS, w które wyposażone były wszystkie komputery stacjonarne wykorzystywane w MOPS. (dowód: akta kontroli str. 8-10, 134-135 i 151-152)

3.9. W okresie objętym kontrolą nie wystąpiły przypadki fizycznej utraty danych np. w wyniku kradzieży nośnika, przypadkowego skasowania lub zniszczenia w następstwie wystąpienia sytuacji nadzwyczajnych (pożar, zalanie). W MOPS nie wystąpiły również przypadki naruszenia ochrony danych osobowych, które wymagałyby zastosowania procedur określonych w załączniku Nr 7 do Polityki bezpieczeństwa.
(dowód: akta kontroli str. 8-10 i 28-29)

Ustalone nieprawidłowości

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

Uwagi dotyczące badanej działalności

Najwyższa Izba Kontroli zwraca uwagę na potrzebę opracowania wewnętrznych regulacji 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 MOPS. Ponadto obowiązek zabezpieczenia systemu informatycznego służącego do przetwarzania danych osobowych przed utratą danych spowodowaną awarią zasilania lub zakłóceniami w sieci zasilającej wynika z regulacji rozdz. A pkt. III załącznika do rozporządzenia w sprawie dokumentacji i warunków technicznych.

Ocena cząstkowa

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

4. Przetwarzanie zasobów informacyjnych zgodnych z zakresem działalności jednostki kontrolowanej

Opis stanu faktycznego

4.1. Dane osobowe w MOPS przetwarzane były w 10 zbiorach danych. Wszystkie zbiory prowadzono zarówno w wersji papierowej, jak i w formie elektronicznej. Do GIODO zgłoszono 10 zbiorów danych, w tym dwa[13] w okresie objętym kontrolą. Wszystkie zbiory zostały ujęte w Polityce bezpieczeństwa. (dowód: akta kontroli str. 6-7 i 136-150)

4.2. W latach 2016 – 2017 MOPS dokonał aktualizacji danych w rejestrze prowadzonym przez GIODO w odniesieniu do tych zbiorów, które były zarejestrowane. (dowód: akta kontroli str.136-137)

4.3. We wszystkich zbiorach zgłoszonych przez MOPS do GIODO zakres przetwarzanych danych był zgodny ze zgłoszeniem. W przypadku jednego zbioru nie wskazano faktu powierzenia przetwarzania danych innemu podmiotowi, co szerzej opisano w dalszej części wystąpienia pokontrolnego, w sekcji „Ustalone nieprawidłowości".

Zakres gromadzonych i przetwarzanych w MOPS danych osobowych był niezbędny do realizacji zadań dotyczących opieki społecznej. (dowód: akta kontroli str. 8-10 i 136-137)

W latach 2016 – 2017 w MOPS prowadzono dwa postępowanie dotyczące naboru kandydatów do pracy. W ogłoszeniach wskazano informacje wymagane przepisem art. 24 ust. 1 ustawy o ochronie danych osobowych. Każda z tych 13 osób wyraziła zgodę na przetwarzanie jej danych osobowych. (dowód: akta kontroli str. 8-10)

4.4. MOPS korzystał z elektronicznej wersji zbioru danych osobowych „Karta Dużej Rodziny"[14], do którego uzyskał dostęp 15 września 2015 r.[15]. Z kolei dane osobowe w Samorządowej Elektronicznej Platformie Informacyjnej („SEPI") przetwarzano na podstawie umowy powierzenia nr 5/2013 z 2 stycznia 2014 r., w związku z zawarciem 9 września 2013 r. porozumienia w sprawie korzystania z SEPI pomiędzy Kierownikiem MOPS a dyrektorem Powiatowego Urzędu Pracy w Białymstoku (dalej „PUP"). Strony zobowiązały się do zachowania w tajemnicy danych osobowych beneficjentów oraz do ich zabezpieczenia, zgodnie z przepisami określonymi w ustawie o ochronie danych osobowych. Kierownik MOPS upoważniła pracowników PUP do przetwarzania tych danych. Uzyskanie dostępu do ww. zbiorów nie wymagało spełnienia przez jednostkę specjalnych warunków takich, jak np. stworzenie wydzielonego łącza internetowego, czy też budowy określonej struktury sieci. (dowód: akta kontroli str. 181-230)

Ustalone nieprawidłowości

W działalności kontrolowanej jednostki w przedstawionym wyżej zakresie stwierdzono nieprawidłowość, polegającą na nieaktualizowaniu zgłoszenia rejestracyjnego do GIODO dotyczącego zbioru „Pomoc społeczna", w związku z powierzeniem PUP przetwarzania danych w tym zbiorze. Zgodnie z przepisem art. 41 ust. 2 ustawy o ochronie danych osobowych, w terminie 30 dni od dokonania zmiany, ADO ma obowiązek zgłosić GIODO zmianę zakresu gromadzonych danych w zbiorze. Kierownik MOPS wyjaśniła, że: *„Nie dokonano aktualizacji zgłoszenia rejestracyjnego do GIODO (...), ponieważ (...) do dnia dzisiejszego nie było zdarzenia, abyśmy powierzyli PUP jakiekolwiek dane*

[13] Świadczenia wychowawcze „Program Rodzina 500 plus", Wsparcie kobiet w ciąży i rodzin „Za życiem".
[14] System informatyczny do obsługi KDR, znajdujący się na stronie internetowej Ministerstwa Rodziny, Pracy i Polityki Społecznej – kdr.mpips.gov.pl.
[15] Na podstawie umowy użyczenia Nr 1422/MPiPS/KDR/2015 zawartej z Ministerstwem Pracy i Polityki Społecznej.

osobowe, przetwarzane przez tut. Ośrodek. Niezwłocznie zostanie dokonana aktualizacja zgłoszenia rejestracyjnego do GIODO". (dowód: akta kontroli str. 8-10 i 22-27)

Ocena cząstkowa

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

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[16], wnosi o:

1. Utworzenie w systemach operacyjnych komputerów MOPS konta administratora i użytkownika oraz nadanie osobom wykorzystującym te urządzenia uprawnień odpowiadającym zakresom ich obowiązków.
2. Analizowanie i zabezpieczenie przed modyfikacją lub zniszczeniem logów systemów operacyjnych komputerów wykorzystywanych w MOPS.
3. Zapewnienie szkoleń osobom zaangażowanym w proces przetwarzania informacji, z uwzględnieniem zagrożenia jej bezpieczeństwa, skutków naruszenia zasad bezpieczeństwa, konsekwencji prawnych i środków zapewniających jej bezpieczeństwo, stosownie do przepisu § 20 ust. 2 pkt 6 rozporządzenia KRI.
4. Dokonanie aktualizacji danych rejestracyjnych zbioru „Pomoc społeczna" o informacje dotyczące powierzenia PUP przetwarzania danych w tym zbiorze.
5. Wywiązywanie się z obowiązków wynikających z § 20 ust. 2 pkt. 3 i 14 rozporządzenia KRI, dotyczących przeprowadzania okresowych analiz ryzyka utraty integralności, dostępności lub poufności informacji oraz corocznych audytów wewnętrznych z zakresu bezpieczeństwa informacji.

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 26 stycznia 2018 r.

Kontroler
Tomasz Ambrozik
Doradca ekonomiczny

Ambrozik
.....
podpis

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

.....
podpis

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