NAJWYŻSZA IZBA KONTROLI
Delegatura w Białymstoku

LBI.410.023.20.2017
P/17/062

00366418

WYSTĄPIENIE POKONTROLNE

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

I. Dane identyfikacyjne kontroli

Numer i tytuł kontroli	P/17/062 – Bezpieczeństwo elektronicznych zasobów informacyjnych w jednostkach samorządu terytorialnego w województwie podlaskim
Jednostka przeprowadzająca kontrolę	Najwyższa Izba Kontroli Delegatura w Białymstoku
Kontroler	Piotr Jurkin – starszy inspektor kontroli państwowej, upoważnienie do kontroli nr LBI/176/2017 z 18 grudnia 2017 r. (dowód: akta kontroli str. 1-2)
Jednostka kontrolowana	Miejski Ośrodek Pomocy Społecznej w Siemiatyczach, ul. 11 Listopada 35a, 17-300 Siemiatycze[1]
Kierownik jednostki kontrolowanej	Ewa Romaniuk – Dyrektor Ośrodka[2] (dowód: akta kontroli str. 3)

II. Ocena kontrolowanej działalności[3]

Ocena ogólna

Najwyższa Izba Kontroli ocenia negatywnie zapewnienie przez MOPS właściwej ochrony elektronicznych zasobów informacyjnych przed nieuprawnionym dostępem, przejęciem lub zniszczeniem[4].

Uzasadnienie oceny ogólnej

Stwierdzono bowiem nieprawidłowości, polegające w szczególności na:

- nadaniu dziewięciu pracownikom MOPS uprawnień do zarządzania systemami operacyjnymi komputerów w stopniu większym niż wymagany do realizacji przez nich zadań i obowiązków, co naruszało § 20 ust. 2 pkt 4 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[5],
- niezabezpieczeniu hasłami dwóch (z 21 objętych oględzinami) komputerów, za pomocą których przetwarzano dane osobowe oraz zabezpieczeniu kolejnych sześciu hasłami o nieodpowiedniej jakości, co naruszało § 20 ust. 2 pkt 7 lit. c rozporządzenia KRI w związku z § 6 ust. 4 i części B pkt VIII rozporządzenia Ministra Spraw Wewnętrznych i Administracji z dnia 29 kwietnia 2004 r. w sprawie dokumentacji przetwarzania danych osobowych oraz warunków technicznych i organizacyjnych, jakim powinny odpowiadać urządzenia i systemy informatyczne służące do przetwarzania danych osobowych[6],
- przetwarzaniu przez dwóch pracowników (z 22 objętych badaniem) danych w zbiorach danych osobowych bez niezbędnych upoważnień, co naruszało art. 37 ustawy z dnia 29 sierpnia 1997 r. o ochronie danych osobowych[7],
- niezgłoszeniu do rejestru zbiorów danych osobowych prowadzonego przez Generalnego Inspektora Ochrony Danych Osobowych (dalej: „GIODO") czterech (z dziewięciu) takich zbiorów oraz przetwarzaniu w czterech zbiorach danych w zakresie szerszym niż zgłoszony do GIODO, co naruszało odpowiednio art. 40 i art. 41 ust. 1 pkt 3a ustawy o ochronie danych osobowych,
- nieanalizowaniu i niezabezpieczeniu przed modyfikacją lub zniszczeniem logów systemów operacyjnych, mimo takiego wymogu zawartego w § 20 ust. 2 pkt 7 lit a rozporządzenia KRI,

---

1 Dalej: „MOPS" lub „ Ośrodek".
2 Pełniąca funkcję od 1 czerwca 1990 r.
3 Najwyższa Izba Kontroli stosuje 3-stopniową skalę ocen: pozytywna, pozytywna mimo stwierdzonych nieprawidłowości, negatywna.
4 Kontrolą objęty został okres od 1 stycznia 2016 r. do zakończenia czynności kontrolnych.
5 Dz. U. z 2017 poz.2247. Rozporządzenie zwane dalej: „rozporządzeniem KRI".
6 Dz. U. Nr 100 poz. 1024. Rozporządzenie zwane dalej: „rozporządzeniem w sprawie dokumentacji przetwarzania danych osobowych".
7 Dz. U. 2016 poz. 922.

- opracowaniu polityki bezpieczeństwa informacji[8] nieodpowiadającej wymogom § 2 pkt 15 w związku z § 20 ust. 1 rozporządzenia KRI,
- nieprzeprowadzaniu okresowych analiz ryzyka utraty integralności, dostępności i poufności informacji oraz corocznych audytów wewnętrznych z zakresu bezpieczeństwa informacji, co było niezgodne z przepisem § 20 ust. 2 pkt 3 i 14 rozporządzenia KRI.

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

Opis stanu faktycznego

1.1. W okresie objętym kontrolą do gromadzenia i przetwarzania danych, w tym danych osobowych, w MOPS wykorzystywano dziewięć programów / systemów informatycznych, które funkcjonowały na 21 stacjach roboczych (20 komputerach i jednym laptopie[9]). Oględziny 21 stacji roboczych z wykorzystaniem, których gromadzono i przetwarzano dane wykazały m.in., że: [1] w 13 komputerach dostęp do systemu zabezpieczony był w sposób odpowiedni, co szerzej opisano w pkt. 1.5. niniejszego wystąpienia, natomiast na dwóch komputerach nie wprowadzono tego typu zabezpieczeń, a dostęp do kolejnych sześciu był zabezpieczony hasłem nieodpowiedniej jakości; [2] użytkownicy posiadali dostęp do oprogramowania niezbędnego w ich pracy; [3] wszystkie stacje robocze posiadały dostęp do Internetu; [4] zainstalowany na 11 komputerach system operacyjny Windows 7 Pro i jednym LINUX CentOS automatycznie podlegały aktualizacji, a w przypadku pozostałych dziewięciu komputerów z systemem Windows XP producent oprogramowania zakończył udzielanie wsparcia technicznego dla tego systemu; [5] na wszystkich komputerach zainstalowano program antywirusowy, który był codziennie automatycznie aktualizowany. Zagadnienia przedstawione w pkt. 1 szerzej opisano w dalszej części wystąpienia, w sekcji „Ustalone nieprawidłowości". (dowód: akta kontroli str. 4, 6-9)

1.2. 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. 9)

1.3. Porównanie dostępu 22 pracowników do systemów informatycznych MOPS[10] z posiadanymi przez nich upoważnieniami oraz zadaniami przypisanymi im w zakresach obowiązków wykazało, że 19 pracownikom zakres nadanych upoważnień oraz indywidualnych loginów i haseł do poszczególnych systemów operacyjnych odpowiadał zakresowi obowiązków. Jednemu pracownikowi nie nadano natomiast upoważnień do przetwarzania danych w systemach Płatnik oraz Kadry i Płace, mimo posiadania do nich dostępu oraz przypisania odpowiednich zadań w zakresach czynności. Kolejny pracownik, mimo braku tego rodzaju zadań z zakresach obowiązków i bez upoważnienia, przetwarzał dane osobowe w systemie Elektronicznego Zarządzania Dokumentami („EZD") SmartDoc. Przedmiotowy zbiór danych obsługiwano korzystając z loginu i hasła nadanego dla Dyrektor Ośrodka. Nie posiadał on także upoważnienia do przetwarzania danych w systemie Płatnik, mimo przypisania mu tego rodzaju zadań w zakresie obowiązków. Informatyk Ośrodka[11] dysponował upoważnieniem do dostępu i przetwarzania danych w pięciu zbiorach danych osobowych wykorzystywanych w MOPS. Nie przypisano mu jednak loginów i haseł do systemów dziedzinowych Ośrodka obsługujących wymienione w upoważnieniu zbiory danych. Faktycznie wykonywał on funkcję administratora jedynie dla poszczególnych stacji roboczych. Administrowaniem programami / systemami dziedzinowymi zajmował się podmiot zewnętrzny. Poza ww. przykładem nie stwierdzono przypadku użytkowania jednego konta przez więcej niż jednego użytkownika. Ponadto dziewięciu pracowników nadano uprawnienia administratora dla systemu operacyjnego, mimo nieokreślenia tego

[8] Opisane w Polityce Bezpieczeństwa przetwarzania danych osobowych (dalej: „Polityka bezpieczeństwa") oraz Instrukcji zarządzania systemem informatycznym służącym do przetwarzania danych osobowych (dalej: „Instrukcja zarządzania").

[9] MOPS posiadało dwa mobilne terminale służące do przeprowadzania wywiadów środowiskowych w miejscu przebywania klientów Ośrodka.

[10] W okresie objętym kontrolą jedna osoba odeszła na emeryturę, ale nie korzystała ona z elektronicznych zasobów Ośrodka.

[11] Zrezygnował z pracy w MOPS z dniem 31 grudnia 2017 r.

rodzaju zadań w zakresach ich obowiązków, co szerzej opisano w pkt 2.4. niniejszego wystąpienia oraz w dalszej części wystąpienia w sekcji „Ustalone nieprawidłowości".

(dowód: akta kontroli str. 4, 9-28)

1.4. Dla żadnej z 21 objętych oględzinami stacji roboczych nie prowadzono rejestru dostępu do komputera[12]. Nie gromadzono również logów aktywności użytkowników systemu co uniemożliwiało analizowanie ruchu sieciowego. Nie analizowano także danych wychodzących z sieci lokalnej MOPS do sieci publicznej, co szerzej opisano w dalszej części wystąpienia pokontrolnego, w sekcji „Ustalone nieprawidłowości".

(dowód: akta kontroli str. 4, 6-8, 29-34)

1.5. W okresie objętym kontrolą Ośrodek posiadał sieci Wi-Fi, ale nie była ona użytkowana przez pracowników MOPS[13]. W związku z tym nie opracowano zasad dostępu do zbiorów danych za jej pośrednictwem.

Zgodnie z § 3 części II Instrukcji zarządzania, przy wykorzystywaniu systemów przetwarzających dane osobowe stosuje się m.in. odpowiedniej jakości hasła, a każdy użytkownik zobowiązany był do jego zmiany co 30 dni. Przeprowadzone w trakcie kontroli oględziny 21 stacji roboczych wykazały także, że na pięciu urządzeniach hasła dostępowe do systemu operacyjnego spełniały wymagania przewidziane dla środków bezpieczeństwa na poziomie wysokim, tj. każdorazowe uwierzytelnienie użytkownika w systemie następowało po podaniu identyfikatora, a system wymuszał (nie rzadziej niż co 30 dni) zmianę hasła o odpowiedniej długości i jakości. W dwóch przypadkach dostęp do urządzeń nie był zabezpieczony hasłem, a kolejne sześć komputerów było zabezpieczone hasłami nieodpowiedniej długości. Na 12 stacjach roboczych nie wymuszano zmiany haseł co 30 dni, co szerzej opisano w dalszej części wystąpienia pokontrolnego, w sekcji „Ustalone nieprawidłowości".

Analogiczne, wymagane Instrukcją zarządzania, zabezpieczenia funkcjonowały tylko w jednym z dziewięciu lokalnych programów objętych oględzinami, służącymi do przetwarzania danych osobowych (Smart Doc). Natomiast w przypadku programu / systemu Pomost Std.[14], który wymuszał zmianę hasa co 30 dni, trzech pracowników (z 10, którym nadano stosowne uprawnienia) do dnia rozpoczęcia kontroli NIK, posługiwało się hasłami o niższej liczbie znaków. W kolejnych siedmiu programach (Płatnik[15], Budżet[16], Kadry i Płace, Amazis02[17], Izyda[18], Nemezis[19], WinDom[20]) stosowano hasła o niższej złożoności oraz nie zawsze wymuszano ich zmianę co 30 dni. Dyrektor MOPS wyjaśniła, iż brak wysokiego poziomu zabezpieczeń we wskazanych systemach wynikał z niedopatrzenia zatrudnionego informatyka, spowodowanego nadmiarem obowiązków służbowych. (dowód: akta kontroli str. 6-9, 29-36, 98-126)

1.6. W regulacjach wewnętrznych nie przewidziano możliwości wykorzystywania sprzętu prywatnego do realizacji zadań służbowych. Pracownicy MOPS nie mogą używać sprzętu domowego do pracy nad zadaniami powierzonymi w ramach obowiązków oraz nie mogą korzystać ze służbowych urządzeń informatycznych poza siedzibą jednostki. W Ośrodku nie opracowano zasad bezpiecznej pracy przy przetwarzaniu mobilnym i pracy na odległość. Dyrektor wyjaśniła, że funkcjonuje powszechny ustny zakaz do korzystania ze sprzętu prywatnego w celach służbowych (dotyczący m.in. komputerów, telefonów oraz tabletów). W trakcie oględzin nie stwierdzono przypadków wykorzystywania sprzętu prywatnego do celów służbowych. (dowód: akta kontroli str. 4, 9, 33-34, 37-40, 81-126)

---

[12] Biegły ustalił, że na żadnym z komputerów nie znaleziono oprogramowania, służącego do monitorowania ich pracy ani też ruchu sieciowego.

[13] Sieć była zabezpieczona hasłem. Korzystał z niej podmiot zewnętrzny świadczący usługi informatyczne przy administrowaniu systemami dziedzinowymi.

[14] Program do przetwarzania danych w zakresie świadczeniobiorców MOPS w Siemiatyczach.

[15] System do przetwarzania w zakresie dotyczącym m.in. objęcia ubezpieczeniem zdrowotnym i społecznym świadczeniobiorców MOPS w Siemiatyczach.

[16] Program finansowo-księgowy.

[17] Program do przetwarzania danych w zakresie świadczeń rodzinnych.

[18] Program do przetwarzania danych w zakresie świadczeń 500+.

[19] Program do przetwarzania danych w zakresie świadczeń alimentacyjnych.

[20] Program do przetwarzania danych w zakresie dodatków mieszkaniowych.

1.7. W okresie objętym kontrolą nie występowały przypadki wykrycia nieautoryzowanych działań związanych z przetwarzaniem informacji / danych osobowych, w tym nie stwierdzono penetracji systemów informatycznych przez osoby nieuprawnione.
(dowód: akta kontroli str. 33-34)

1.8. W MOPS nie wykonywano obowiązków służbowych z wykorzystaniem mobilnego przetwarzania danych, w tym pracy na odległość. W terenie nie wykorzystywano także dwóch mobilnych terminali służących do przeprowadzania wywiadów środowiskowych w miejscu przebywania klientów MOPS. Pracownice użytkujące te urządzenia wyjaśniły, że wywiady środowiskowe nie były realizowane w terenie z powodu obawy o jego utratę lub zniszczenie (związanej z pracą w środowisku patologicznym) oraz braku dostępu do energii elektrycznej, co wiązało się z ryzykiem niedokończenia wywiadu środowiskowego i niewygenerowaniem sumy kontrolnej. W związku z powyższym nie opracowano zasad wykorzystywania urządzeń mobilnych do tych celów, co szerzej opisano w dalszej części wystąpienia pokontrolnego, w sekcji „Ustalone nieprawidłowości".
(dowód: akta kontroli str. 4, 33-34, 41)

1.9. W okresie objętym kontrolą Ośrodek nie korzystał z naprawy komputerów przez podmioty zewnętrzne. Wszelkie naprawy lub usterki sprzętu oraz zgłoszenia nieprawidłowej pracy programów sieciowych wykonywał informatyk. W dwóch umowach dotyczących serwisu i aktualizacji programów wykorzystywanych w MOPS do gromadzenia i przetwarzania danych osobowych zawarto zapisy zobowiązujące ich dostawcę do zachowania tajemnicy i nieudostępnienia przekazywanych danych osobowych. Natomiast w obowiązujących w 2016 i 2017 roku umowach na świadczenie usług informatycznych przez podmiot zewnętrzny, w tym administrowanie wykorzystywanymi w MOPS systemami / programami, nie zamieszczono zapisów gwarantujących odpowiedni poziom bezpieczeństwa informacji oraz ich zabezpieczenia w sposób uniemożliwiający ujawnienie osobom nieuprawnionym, co szerzej opisano w dalszej części wystąpienia pokontrolnego, w sekcji „Ustalone nieprawidłowości". W dniu 2 stycznia 2018 r. z podmiotem świadczącym przedmiotowe usługi zawarto umowę powierzenia przetwarzania danych osobowych, w której ujęto odpowiednie zapisy. (dowód: akta kontroli str. 4, 42-52)

1.10. W celu ochrony systemów informatycznych MOPS, zastosowano zabezpieczenie w postaci firewalla i na wszystkich komputerach zainstalowano program antywirusowy (bez modułu centralnego zarządzania), którego aktualizacja odbywała się automatycznie, co szerzej opisano w pkt 1.1. niniejszego wystąpienia. (dowód: akta kontroli str. 33-34)

1.11. MOPS nie zawarł umowy na świadczenie usług poczty elektronicznej. Korzystał z poczty udostępnionej przez Urząd Miejski w Siemiatyczach.
(dowód: akta kontroli str. 33-34)

1.12. Zgodnie z zapisami w Instrukcji zarządzania, kopie bezpieczeństwa dla poszczególnych systemów powinny być wykonywane co tydzień. Dla wszystkich ośmiu systemów, dla których administratorem był Dyrektor MOPS – Administrator Danych Osobowych (dalej: „ADO"), sporządzano kopie bezpieczeństwa z ustaloną częstotliwością i przechowywano je na serwerze oraz jednym z komputerów[21]. Co dwa tygodnie wykonywano testy kopii zapasowych. (dowód: akta kontroli str. 9, 29-34, 98-126)

1.13. Na 12 poddanych oględzinom stacjach roboczych zainstalowane były wyłącznie aktualne systemy operacyjne, a na pozostałych dziewięciu – oprogramowanie Windows XP, nieposiadające wsparcia producenta. Pracownicy dysponowali także możliwością ściągnięcia aplikacji i plików z możliwością ich zainstalowania i uruchomienia, co opisano w dalszej części wystąpienia, w sekcji „Uwagi dotyczące badanej działalności".
(dowód: akta kontroli str. 6-8, 29-32)

1.14. Powołany w trakcie niniejszej kontroli biegły stwierdził, że wszystkie zbadane komputery (poza wykorzystującymi system Windows XP) posiadały aktualne wersje systemów operacyjnych i aplikacji bezpieczeństwa. Aktualizacje były wykonywane zgodnie

[21] MOPS użytkowało dziewięć programów, z których dla ośmiu administratorem danych była Dyrektor MOPS, a dla jednego – podmiot zewnętrzny.

z harmonogramem ustawionym przez administratora. Aktualna była również wersja specjalistycznego oprogramowania zainstalowanego na komputerach i na serwerze.
(dowód: akta kontroli str. 29-32)

1.15. Zgodnie z obowiązującą w MOPS polityką rachunkowości, poza tradycyjną formą (papierową) sporządzania i przesyłania przelewów stosuje się wykonywane płatności drogą elektroniczną. Nie opracowano procedury dokonywania płatności drogą elektroniczną. Zasady dokonywania płatności tą drogą regulowała umowa zawarta z bankiem. Wykonanie przelewu po zatwierdzeniu dokumentu pod względem merytorycznym i formalno-rachunkowym wymagało wprowadzenia indywidualnego kodu PIN przez wyznaczonego pracownika Wydziału Finansowego. Do wykonania transakcji konieczna była dwukrotna autoryzacja (dokonywały jej dwie osoby poprzez bankowy podpis elektroniczny – dyrektor MOPS, główna księgowa oraz dwóch upoważnionych pracowników Ośrodka).
(dowód: akta kontroli str. 33-34)

Ustalone nieprawidłowości

W działalności kontrolowanej jednostki w przedstawionym wyżej zakresie stwierdzono nieprawidłowości.

1. W MOPS dostęp do dwóch[22] (z 21 objętych oględzinami) komputerów, za pomocą których przetwarzano dane osobowe nie był zabezpieczony hasłem, a kolejne sześć zabezpieczono hasłami nieodpowiedniej długości. Z kolei na 12 stacjach roboczych nie wymuszano zmiany hasła co 30 dni, czym naruszono przepis § 20 ust. 2 pkt 7 lit. c rozporządzenia KRI w związku z § 6 ust. 4 i części B pkt VIII rozporządzenia w sprawie dokumentacji przetwarzania danych osobowych. Ponadto, zgodnie z § 3 części II Instrukcji zarządzania, przy wykorzystywaniu systemów przetwarzających dane osobowe należało stosować m.in. odpowiedniej jakości hasła, a każdy użytkownik zobowiązany był do jego zmiany co 30 dni. Dyrektor wyjaśniła, że z powodu nadmiaru obowiązków informatyk nie zabezpieczył dostępu do dwóch komputerów hasłami oraz nie zdążył dokonać weryfikacji ich jakości dla kolejnych sześciu. Natomiast niezastosowanie wymuszenia zmiany haseł co 30 dni wynikało z przeoczenia informatyka, spowodowanego nadmiarem obowiązków służbowych.
(dowód: akta kontroli str. 6-8, 37-40, 98-126)

2. W MOPS nie przeprowadzano okresowych analiz ryzyka utraty integralności, dostępności lub poufności informacji, mimo takiego wymogu zawartego w § 20 ust. 2 pkt 3 rozporządzenia KRI. Dyrektor wyjaśniła, że nie przeprowadzano takich analiz z powodu niezatrudnienia pracownika do realizacji zadań wynikających z ustawy o ochronie danych osobowych. Sama zaś nie przeprowadzała takich analiz z uwagi na obciążenie obowiązkami służbowymi. (dowód: akta kontroli str. 9, 56-58)

3. W latach 2016 – 2017 w MOPS nie analizowano i nie zabezpieczano przed modyfikacją lub zniszczeniem logów systemów operacyjnych wykorzystywanych komputerów, mimo takiego wymogu zawartego w § 20 ust. 2 pkt 7 lit a rozporządzenia KRI, gdyż nie analizowano logów poszczególnych aplikacji, ruchu sieciowego, a także danych wychodzących z sieci lokalnej Ośrodka do sieci publicznej. Dyrektor wyjaśniła, że nie monitorowano dostępu do informacji z powodu niezatrudniania odpowiedniej osoby, co było spowodowane brakiem środków finansowych w budżecie MOPS.
(dowód: akta kontroli str. 4, 6-8, 29-34, 56-58)

4. W umowach na świadczenie usług serwisowych przez podmiot zewnętrzny obowiązujących w latach 2016 i 2017, nie zamieszczono zapisów gwarantujących odpowiedni poziom bezpieczeństwa informacji oraz ich zabezpieczenia w sposób uniemożliwiający ujawnienie danych osobom nieuprawnionym, co naruszało § 20 ust. 2 pkt 10 rozporządzenia KRI. Dyrektor Ośrodka wyjaśniła, że wynikało to z nieuwagi. *„W umowie zawartej na 2018 rok (...) zawarto zapisy gwarantujące odpowiedni poziom bezpieczeństwa informacji".* (dowód: akta kontroli str. 42-52, 56-58)

5. W obowiązujących w Ośrodku wewnętrznych przepisach nie określono zasad użytkowania komputerów przenośnych / mobilnych. Praca taka była możliwa na dwóch terminalach przekazanych MOPS 23 grudnia 2013 roku w ramach Projektu *„Emp@tia* –

[22] Użytkownikom tych komputerów nadano uprawnienia administratora systemu operacyjnego.

Platforma komunikacyjna obszaru zabezpieczenia społecznego". 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. Dyrektor wyjaśniła, że: *„Nie użytkowano posiadanych dwóch terminali poza budynkiem Ośrodka. W związku z tym sądziłam, że nie ma potrzeby opracowania przepisów / zasad dotyczących ich użycia poza siedzibą MOPS. Odpowiednie regulacje wewnętrzne zostaną wprowadzone*". W założeniach projektu Emp@tia przedmiotowe terminale miały służyć wyłącznie do pracy poza siedziba MOPS. W sytuacji, gdy wynikłaby konieczność użycia terminali na zewnątrz – należałoby stworzyć zasady użytkowania tego sprzętu. Takie mechanizmy powinny być przygotowane z wyprzedzeniem, aby pracownicy Ośrodka mieli czas na zapoznanie się z nimi.
(dowód: akta kontroli str. 4, 33-36, 41)

6. Dziewięciu użytkującym komputery pracownikom MOPS nadano uprawnienia administratora dla systemu operacyjnego, mimo nieprzypisania im tego rodzaju zadań w zakresach obowiązków. Pozostali użytkownicy mieli możliwość administrowania kontami użytkowników. Takie postępowanie stanowiło naruszenie § 20 ust. 2 pkt 4 rozporządzenia KRI. Dyrektor wyjaśniła, że spowodowane to było przeoczeniem informatyka i w najbliższym czasie będzie to skorygowane.
(dowód: akta kontroli str. 6-9, 29-32, 35-36)

Uwagi dotyczące badanej działalności

Najwyższa Izba Kontroli zwraca uwagę, że w Ośrodku wykorzystywano dziewięć komputerów z zainstalowanym systemem XP, dla którego z dniem 8 kwietnia 2014 r. producent oprogramowania zakończył udzielanie wsparcia, co mogło wpłynąć na obniżenie poziomu bezpieczeństwa danych przetwarzanych na urządzeniach wykorzystujących ww. system. Dyrektor Ośrodka wyjaśniła, że powodem wykorzystywania systemu operacyjnego Windows XP był brak środków finansowych na zakup aktualnego oprogramowania. (dowód: akta kontroli str. 6-8, 29-34, 37-40)

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.

2. Dokumentacja i procedury dotyczące ochrony danych osobowych

Opis stanu faktycznego

2.1. W latach 2016 – 2017 w MOPS przetwarzano dane osobowe w dziewięciu zbiorach danych (w tym w siedmiu z wykorzystaniem systemów elektronicznych). Wykaz zbiorów danych osobowych, będący załącznikiem Nr 2 do Polityki bezpieczeństwa danych osobowych, w którym powinny zostać one ujęte był nierzetelny, ponieważ wykazano w nim jedynie sześć zbiorów (w tym pięć funkcjonujących z wykorzystaniem systemów informatycznych), co szerzej opisano w dalszej części wystąpienia pokontrolnego, w sekcji „Ustalone nieprawidłowości".

Obowiązkowi zgłoszenia do rejestru zbiorów danych osobowych prowadzonych przez GIODO podlegały wszystkie dziewięć zbiorów danych osobowych przetwarzanych w MOPS, z których zgłoszono tylko pięć, co szerzej opisano w dalszej części wystąpienia pokontrolnego, w sekcji „Ustalone nieprawidłowości". Zgłoszenia zbiorów danych do rejestracji zawierały elementy wymienione w art. 41 ust 1 ustawy o ochronie danych osobowych. W okresie objętym kontrolą nie aktualizowano danych oraz nie występowano do GIODO o wykreślenie zarejestrowanego zbioru (nie nastąpiła również odmowa rejestracji). (dowód: akta kontroli str. 4, 9, 33-34, 37-40, 53-55, 59-75)

2.2. W § 15 Polityki bezpieczeństwa przewidziano możliwość powołania Administratora Bezpieczeństwa Informacji (dalej: „ABI"). Dyrektor MOPS nie skorzystała z takiego uprawnienia, określonego również w art. 36 a ust. 1 ustawy o ochronie danych osobowych, i nie wyznaczyła osoby do pełnienia tej funkcji. Wyjaśniła, że: „(...) *wiązałoby się to z jego zatrudnieniem, a ograniczone środki finansowe na utrzymanie Ośrodka Pomocy Społecznej nie pozwalają na taki wydatek*". (dowód: akta kontroli str. 59-60, 82-97)

2.3. Dyrektor Ośrodka (ADO), zgodnie z wymogami art. 36b ustawy o ochronie danych osobowych, w latach 2016 – 2017 zapoznała pracowników przetwarzających dane z wymaganymi przepisami, co potwierdziła analiza dokumentacji 22 pracowników.

ADO nie wywiązała się natomiast z obowiązku przeprowadzenia kontroli zgodności przetwarzania danych osobowych z przepisami o ochronie danych osobowych, co szerzej opisano w dalszej części wystąpienia pokontrolnego, w sekcji „Ustalone nieprawidłowości".
(dowód: akta kontroli str. 9-13, 16)

2.4. Ośrodek dysponował ewidencją osób upoważnionych do przewarzania danych osobowych, zawierającą wszystkie elementy określone w art. 39 ust. 1 ustawy o ochronie danych osobowych. Analiza zakresów obowiązków 22 pracowników merytorycznych jednostki wykazała, że jednemu pracownikowi nie nadano upoważnienia do przetwarzania danych w systemach Płatnik oraz Kadry i Płace, mimo posiadania do nich dostępu oraz przypisania odpowiednich zadań w zakresach czynności. Kolejny pracownik, mimo braku tego rodzaju zadań w zakresach obowiązków i bez stosownego upoważnienia, przetwarzał dane osobowe w systemie EZD SmartDoc, korzystając z loginu i hasła nadanego dla Dyrektor Ośrodka. Nie dysponował on także upoważnieniem do przetwarzania danych w systemie Płatnik, mimo przypisania mu tego rodzaju zadania w zakresie obowiązków[23]. Ponadto dziewięciu pracowników legitymowało się uprawnieniami administratora dla systemu operacyjnego, mimo nieprzypisania im tego rodzaju zadań w zakresach obowiązków, natomiast pozostałe osoby posiadające ograniczone uprawnienie, miały możliwość administrowania kontami użytkowników, co szerzej opisano w sekcji „Ustalone nieprawidłowości" w pkt 1 niniejszego wystąpienia.
(dowód: akta kontroli str. 9-13, 18-24, 29-32, 76-80)

2.5. Zarządzeniem Nr 9/17 Dyrektora MOPS w Siemiatyczach, 4 września 2017 r. wprowadzono Politykę bezpieczeństwa oraz Instrukcję zarządzania. Poza ww. dokumentami nie wydano wewnętrznych aktów prawnych, procedur, instrukcji dotyczących gromadzenia i przetwarzania zasobów informatycznych. W okresie objętym kontrolą nie wystąpiły zmiany organizacyjne uzasadniające potrzebę aktualizacji regulacji wewnętrznych dotyczących gromadzenia i przetwarzania przedmiotowych zasobów.
(dowód: akta kontroli str. 9, 81-126)

2.6. Zgodnie z zakresem czynności, obowiązki dotyczące bezpieczeństwa informacji oraz związane z administrowaniem systemami, w których m.in. gromadzono i przetwarzano dane osobowe powierzono informatykowi Ośrodka. Do jego zadań należało m.in. administrowanie siecią i serwerem, okresowe kontrole stanu instalacji i urządzeń, nadzór nad pracą programów biurowych i systemowych, archiwizacja danych, dokonywanie przeglądów i konserwacja sprzętu. Natomiast stosownie do umów na świadczenie usług informatycznych[24] zawartych z podmiotem zewnętrznym do jego obowiązków należało m.in. administrowania systemem Pomost Std. oraz programami dziedzinowymi: Amazis, Izyda, Nemezis oraz WinDom. Informatyk złożył oświadczenie zobowiązujące go do zachowania w tajemnicy przetwarzanych danych oraz ich zabezpieczania. W umowie powierzenia przetwarzania danych osobowych, zawartej w dniu 2 stycznia 2018 r. z podmiotem świadczącym przedmiotowe usługi, zamieszczono zapisy upoważniające świadczeniodawcę do przetwarzania danych osobowych w celu i na potrzeby realizacji umowy i gwarantujące odpowiedni poziom bezpieczeństwa informacji oraz ich zabezpieczenia w sposób uniemożliwiający ujawnienie danych osobom nieuprawnionym, co opisano w pkt 1.9. niniejszego wystąpienia. (dowód: akta kontroli str. 25-28, 42-52)

2.7. W MOPS w latach 2016 – 2017 (do 19 grudnia) 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. 9)

2.8. W okresie objętym kontrolą żaden z pracowników, poza informatykiem[25], nie uczestniczył w szkoleniach z zakresu bezpieczeństwa przetwarzania informacji, w tym danych osobowych, co szerzej opisano w dalszej części wystąpienia pokontrolnego, w sekcji „Ustalone nieprawidłowości". Dyrektor MOPS wyjaśniła, że szkolenie

[23] W trakcie kontroli nadano stosowne upoważnienia obu pracownikom oraz uzupełniono zakres obowiązków.
[24] Umowy nr: 2/2016 z 2 stycznia 2016 r., nr 13/2017 i nr 15/2017 odpowiednio z 2 stycznia i 2 maja 2017 r. oraz nr 7/2018 z 2 stycznia 2018 r.
[25] Informatyk uczestniczył w jednodniowym szkoleniu (6 października 2017 r.) z zakresu ochrony danych osobowych.

dla pracowników z zakresu bezpieczeństwa informacji i ochrony danych osobowych są planowane w II kwartale 2018 roku. (dowód: akta kontroli str. 9, 28, 37-40)

2.9. W okresie objętym kontrolą w MOPS nie były prowadzone zewnętrzne kontrole w zakresie bezpieczeństwa danych osobowych. Nie wpłynęły także skargi związane z przypadkami ujawnienia danych osobowych. (dowód: akta kontroli str. 33-34)

2.10. Obowiązująca w Ośrodku dokumentacja określająca sposób przetwarzania danych osobowych, środków technicznych i organizacyjnych zapewniających ochronę tych danych oraz zarządzania bezpieczeństwem informacji przyjęta została zarządzeniem Nr 9/17 Dyrektor MOPS z dnia 4 września 2017 r. Składały się na nią Polityka bezpieczeństwa oraz Instrukcja zarządzania. Dokumentacja ta nie była aktualizowana.

Polityka bezpieczeństwa zawierała elementy wymagane § 4 pkt 1-5 rozporządzenia w sprawie dokumentacji przetwarzania danych osobowych, jednak będący załącznikiem Nr 2 do Polityki bezpieczeństwa wykaz zbiorów danych osobowych zawierał tylko sześć z dziewięciu takich zbiorów wykorzystywanych w Ośrodku. Natomiast Instrukcja zarządzania spełniała wymogi określone w § 5 pkt 1 – 4 oraz pkt 6 i 8 powołanego rozporządzenia. W przedmiotowych dokumentach nie określono natomiast okresu przechowywania kopii zapasowych i sposobu realizacji wymogów, o których mowa w § 7 rozporządzenia. Przyjęte uregulowania i procedury związane z użytkowaniem systemów informatycznych służących do przetwarzania danych dotyczyły jedynie danych osobowych. Nie odnosiły się one do ochrony innych danych będących w posiadaniu jednostki. Nie spełniały zatem wymogu określonego w § 2 pkt 15 w związku z § 20 ust. 1 rozporządzenia KRI, co szerzej opisano w dalszej części wystąpienia pokontrolnego, w sekcji „Ustalone nieprawidłowości".

(dowód: akta kontroli str. 9, 33-34, 53-55, 59-62, 81-126)

Ustalone nieprawidłowości

W działalności kontrolowanej jednostki w przedstawionym wyżej zakresie stwierdzono nieprawidłowości.

1. Dyrektor MOPS, wbrew obowiązkowi wynikającemu z art. 40 ustawy o ochronie danych osobowych, do rejestru zbiorów danych osobowych prowadzonych przez GIODO nie zgłosiła czterech[26] (z dziewięciu) takich zbiorów. Wyjaśniła ona, że spowodowane to było nadmiarem pracy i zadań realizowanych przez MOPS oraz brakami kadry pracowniczej. Dodała, że: „(...) *W MOPS brak jest etatu dla pracownika, który w swoim zakresie miałby realizację zadań wynikających z ustawy o ochronie danych osobowych. Powyższe braki wynikają z ograniczonych środków finansowych w budżecie Ośrodka*".
(dowód: akta kontroli str. 9, 37-40, 60-75, 182-197)

2. W prowadzonym przez MOPS wykazie zbiorów danych osobowych ujęto sześć z dziewięciu wykorzystywanych w Ośrodku takich zbiorów, co naruszało § 5 pkt 2 Polityki bezpieczeństwa danych osobowych. Dyrektor wyjaśniła, że spowodowane to było przeoczeniem. (dowód: akta kontroli str. 37-40, 53-55, 59-62)

3. ADO nie wywiązała się z obowiązku przeprowadzenia kontroli zgodności przetwarzania danych osobowych z przepisami o ochronie danych osobowych, mimo takiego wymogu zawartego w art. 36a ust. 2 pkt 1lit a w związku z art. 36b ustawy o ochronie danych osobowych. Dyrektor wyjaśniła, że powodem nieprzeprowadzania przedmiotowych czynności był brak osoby do realizacji obowiązków wynikających z ustawy o ochronie danych osobowych. Dodała, że *„Sama również nie wykonywałam takich sprawdzeń / kontroli z powodu dużej ilości innych obowiązków*".
(dowód: akta kontroli str. 9, 37-40)

4. Jednemu pracownikowi Ośrodka nie nadano upoważnień do przetwarzania danych w systemach Płatnik oraz Kadry i Płace, mimo posiadania do nich dostępu oraz przypisania odpowiednich zadań w zakresach czynności. Kolejny pracownik przetwarzał dane osobowe w systemie EZD SmartDoc, mimo braku tego rodzaju zadań z zakresach obowiązków i bez upoważnienia wymaganego przepisami prawa. Dane w tym zbiorze

[26] Do GIODO nie zgłoszono zbiorów danych osobowych: „Dziennik Korespondencji', „Elektroniczne zarządzanie dokumentami Smart Doc", „Płatnik" – w zakresie objęcia świadczeniobiorców MOPS ubezpieczeniami społecznymi i zdrowotnymi, „Świadczenia rodzinne". W trakcie kontroli zgłoszono do rejestru prowadzonego przez GIODO te zbiory.

przetwarzano korzystając z loginu i hasła nadanego dla Dyrektor Ośrodka. Nie dysponował on także upoważnieniem do przetwarzania danych w systemie Płatnik, mimo przypisania mu tego rodzaju zadań w zakresie obowiązków. Takie postępowanie stanowiło naruszenie art. 37 ustawy o ochronie danych osobowych. Dyrektor wyjaśniła, że nienadanie przedmiotowych upoważnień spowodowane było nieuwagą.

(dowód: akta kontroli str. 9-24, 35-40)

5. W MOPS w latach 2016 – 2017 nie przeprowadzano audytów wewnętrznych z zakresu bezpieczeństwa informacji, mimo obowiązku wynikającego z § 20 ust. 2 pkt 14 rozporządzenia KRI. W konsekwencji nie dysponowano rzetelną oceną skuteczności przyjętych rozwiązań w zakresie ochrony danych osobowych. Dyrektor wyjaśniła, że: *„Nie przeprowadzano corocznych audytów wewnętrznych z zakresu bezpieczeństwa z uwagi na brak środków finansowych w budżecie Ośrodka".*

(dowód: akta kontroli str. 33-34, 37-40)

6. Obowiązująca w MOPS Instrukcja zarządzania nie określała okresu przechowywania wykonanych kopii zapasowych zbiorów danych oraz sposobu realizacji wymogów, o których mowa w § 7 ust 1 pkt 4 rozporządzenia w sprawie dokumentacji przetwarzania danych osobowych, czym naruszono § 5 pkt 5 lit. b powołanego rozporządzenia. Dyrektor wyjaśniła, że: *„Spowodowane to było przeoczeniem w trakcie opracowywania tego dokumentu".* (dowód: akta kontroli str. 33-34, 37-40, 98-126)

7. Przyjęte w Ośrodku uregulowania i procedury składające się na politykę bezpieczeństwa informacji dotyczyły jedynie ochrony danych osobowych. Nie odnosiły się one do innych danych będących w posiadaniu jednostki. W konsekwencji nie spełniono wymogu określonego w § 2 pkt 15 w związku z § 20 ust. 1 rozporządzenia KRI. Dyrektor wyjaśniła, że wynikało to z braku środków finansowych na zakup profesjonalnej usługi audytu i przygotowania dokumentacji dotyczącej polityki bezpieczeństwa informacji.

(dowód: akta kontroli str. 33-34, 56-58, 81-126)

8. W okresie objętym kontrolą żaden z pracowników Ośrodka, poza informatykiem, nie uczestniczył w szkoleniach z zakresu bezpieczeństwa informacji i ochrony danych osobowych, co stanowiło naruszenie § 20 ust. 2 pkt 6 rozporządzenia KRI, zgodnie z którym należy zapewnić szkolenie osób zaangażowanych w proces przetwarzania informacji. Dyrektor wyjaśniła, że spowodowane to było brakiem środków finansowych w budżecie MOPS. (dowód: akta kontroli str. 9, 28, 33-36)

Ocena cząstkowa

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

3. Sposób przechowywania oraz zabezpieczenia danych

Opis stanu faktycznego

3.1. W Polityce bezpieczeństwa określono zabezpieczenia techniczne budynku i pomieszczeń, w których przetwarzano dane osobowe, na które składały się: elektroniczny system alarmowy nadzorujący budynek, kontrola dostępu do zbiorów danych osobowych, przechowywanie papierowych zbiorów danych w zamykanych szafach, zamykanie na klucz pomieszczeń w czasie nieobecności pracowników. Nie przyjęto polityki kluczy, jednak w załączniku nr 5 do Polityki bezpieczeństwa określono m.in. zasadę, że klucze powinny być przechowywane w sposób uniemożliwiający dostęp do nich przez osoby nieupoważnione. Oględziny 10 pomieszczeń Ośrodka oraz archiwum wykazały, że przetwarzanie danych osobowych odbywało się w pomieszczeniach wskazanych w zał. Nr 1 do Polityki bezpieczeństwa, które wynajmowano od Zarządu Mienia Komunalnego w Siemiatyczach. W budynku nie był zainstalowany monitoring wizyjny ani system alarmowy. Serwer umieszczono w pokoju Dyrektor Ośrodka (I piętro). Tylko jedno okno było wzmocnione szybą antywłamaniową. W budynku nie zainstalowano żadnego systemu przeciwpożarowego, dysonowano jedynie dwoma gaśnicami. Archiwum oraz pomieszczenie z serwerem nie posiadało żadnych rozwiązań zapobiegających zalaniu akt, przez co nie zapewniono danym tam przechowywanym właściwej ochrony przed działaniem czynników fizycznych i zdarzeń losowych, jak pożar czy zalanie. Zagadnienie to opisano w dalszej części wystąpienia, w sekcji „Ustalone nieprawidłowości".

Serwer posiadał zabezpieczenia na wypadek nagłej utraty zasilania w postaci urządzenia UPS. (dowód: akta kontroli str. 4, 82-126, 131-137)

3.2. Informatyk jedynie dla sześciu komputerów (z 21) na bieżąco gromadził dane, o których mowa w § 20 ust. 2 pkt 2 rozporządzenia KRI, tj. prowadził w formie elektronicznej ewidencję obejmującą aktualne dane dotyczące całości służbowego sprzętu informatycznego (rodzaj sprzętu wraz z konfiguracją) i oprogramowania (systemy operacyjne, programy i aplikacje branżowe, licencje itp.), co szerzej opisano w dalszej części wystąpienia, w sekcji „Ustalone nieprawidłowości". (dowód: akta kontroli str. 6-8)

3.3. W okresie objętym kontrolą nie likwidowano komputerów i innego sprzętu biurowego. (dowód: akta kontroli str. 33-34)

3.4. Do niszczenia bieżących wydruków oraz dokumentów niewymagających archiwizacji wykorzystywano cztery niszczarki, jednak nie opracowano w tym zakresie żadnych wytycznych lub procedur. Według Dyrektor nie zlecano zewnętrznemu podmiotowi wykonywania usług niszczenia dokumentów, uznając to za zbyteczne z uwagi na posiadanie własnych niszczarek. (dowód: akta kontroli str. 35-36, 131-137)

3.5. Dyrektor wyjaśniła, że pracownicy MOPS nie mogą używać sprzętu domowego do pracy nad zadaniami powierzonymi w ramach obowiązków służbowych oraz nie mogą korzystać ze służbowych urządzeń informatycznych poza siedzibą jednostki (z wyjątkiem dwóch przenośnych terminali), co szerzej omówiono w pkt 1.6 niniejszego wystąpienia pokontrolnego. (dowód: akta kontroli str. 4, 37-40)

3.6. Sprzątaniem pomieszczeń zajmowała się sprzątaczka – pracownik MOPS. Czynności te były wykonywane w godzinach od 14^{00} do 22^{00} i obejmowały także sprzątanie pomieszczenia, w którym umiejscowiono serwer. Pracownika sprzątającego zobowiązano do zachowania w tajemnicy danych osobowych, jednak do dnia rozpoczęcia kontroli nie posiadała ona zgody na przebywanie w obszarze przetwarzania danych, co szerzej opisano w dalszej części wystąpienia pokontrolnego, w sekcji „Ustalone nieprawidłowości".

W trakcie oględzin stwierdzono, że pomieszczenia w których przetwarzano dane osobowe, podczas nieobecności pracowników były zamykane na klucz. Ponadto Dyrektor wyjaśniła, że: *„(...) w Ośrodku od wielu lat funkcjonuje zasada, że z chwilą zakończenia wykonywania pracy wszystkie dokumenty chowane są do zamykanych szaf. Takim postępowaniem pracownicy spełniają zasadę tzw. „czystego biurka".*

(dowód: akta kontroli str. 4, 10-13, 35-36, 131-138)

3.7. Zgodnie § 8 części II Instrukcji zarządzania, za przeglądy oraz konserwacje sprzętu i oprogramowania informatycznego miał odpowiadać ASI. Powinny one być wykonywane w wypadku wystąpienia takiej potrzeby. W okresie objętym kontrolą nie wykonywano przeglądów i konserwacji systemu informatycznego oraz nośników informacji służących do przetwarzania danych. Wszelkie naprawy lub usterki sprzętu oraz zgłoszenia nieprawidłowej pracy programów sieciowych wykonywał informatyk. Nie korzystano też z napraw świadczonych przez firmy zewnętrzne. (dowód: akta kontroli str. 33-34, 98-126)

3.8. Serwer MOPS był wyposażony w urządzenie UPS, a przeprowadzone w trakcie kontroli oględziny wykazały, że 12 komputerów posiadało zasilanie awaryjne UPS. Nie opracowało procedur na wypadek wystąpienia sytuacji nadzwyczajnych, w tym długotrwałego braku zasilania, dotyczących 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". MOPS nie posiadał także agregatu prądotwórczego. Nie dysponowano więc skutecznymi zabezpieczeniami przed utratą zasilania dla kluczowych systemów teleinformatycznych. (dowód: akta kontroli str. 4, 6-8, 33-34, 131-138)

3.9. W okresie objętym kontrolą nie stwierdzono w MOPS przypadków fizycznej utraty danych i konieczności ich odtwarzania ze sporządzonych kopii bezpieczeństwa. (dowód: akta kontroli str. 33-34)

Ustalone nieprawidłowości

W działalności kontrolowanej jednostki w przedstawionym wyżej zakresie stwierdzono nieprawidłowości.

1. Pomieszczenie archiwum i pokój, w którym umiejscowiono serwer nie posiadały czujników ostrzegających o pożarze oraz nie zastosowano w nich rozwiązań zapobiegających zalaniu zainstalowanego tam sprzętu i przetrzymywanych dokumentów. Taka sytuacja nie zapewniała właściwej ochrony zbiorów danych przed działaniem czynników fizycznych i zdarzeń losowych, jak pożar lub zalanie. Stanowiło to naruszenie art. 36 ust. 1 ustawy o ochronie danych osobowych, stosownie do którego ADO powinien zastosować środki techniczne i organizacyjne zapewniające ochronę przetwarzanych danych osobowych odpowiednią do zagrożeń oraz kategorii danych objętych ochroną, a w szczególności powinien zabezpieczyć dane m.in. przed uszkodzeniem lub zniszczeniem. Ponadto – stosownie do § 6 załącznika nr 6 do rozporządzenia w sprawie działania archiwów zakładowych[27] – pomieszczenie archiwum powinno posiadać system do wykrywania ognia i dymu (przeciwpożarowy). Dyrektor wyjaśniła, że: *„Miejski Ośrodek Pomocy Społecznej w Siemiatyczach mieści się w budynku zarządu Mienia Komunalnego, liczba pokoi jest nieadekwatna do zadań realizowanych przez MOPS. W Ośrodku brakuje pomieszczeń na wydzielenie serwerowni bądź ustawienie szafy chłodniczej dla serwera. Pomieszczenia MOPS nie mają zabezpieczeń antywłamaniowych, przeciwpożarowych, ani (...) przed zalaniem, gdyż jest do budynek Zarządu Mienia Komunalnego (...). Planowana jest zmiana siedziby MOPS, nowy budynek będzie właściwie zabezpieczony i zapewni właściwą ochronę zbiorom danych osobowych"*.
(dowód: akta kontroli str. 37-40, 131-137)

2. Osoba sprzątające pomieszczenia MOPS do dnia rozpoczęcia kontroli NIK nie posiadała zgody do przebywania w obszarze przetwarzania danych, w tym osobowych, wymaganego w części A pkt I ust. 2 załącznika do rozporządzenia w sprawie dokumentacji przetwarzania danych osobowych. Dyrektor wyjaśniła, że: *„Pracownica została zapozna z przepisami prawa dotyczącymi bezpieczeństwa informacji i ochrony danych osobowych. W wyniku przeoczenia nie miała zgody na przebywanie w obszarze przetwarzania danych, w tym osobowych. Uchybienie sprostowano 15 stycznia 2018 r."*
(dowód: akta kontroli str. 10-13, 35-36, 138)

3. Informatyk dla 15 (z 21) wykorzystywanych w MOPS stacjach roboczych nie posiadał informacji dotyczących m.in. rodzaju sprzętu wraz z konfiguracją oraz użytkowanym oprogramowaniem, co stanowiło naruszenie § 20 ust. 2 pkt 2 rozporządzenia KRI. Dyrektor Ośrodka wyjaśniła, że: *„Informatyk (...) został zatrudniony od 1 lipca 2017 r. na ½ etatu, zinwentaryzował sześć komputerów, więcej nie zdążył, kolejne będą konsekwentnie inwentaryzowane"*. (dowód: akta kontroli str. 6-8, 37-40)

Uwagi dotyczące badanej działalności

Najwyższa Izba Kontroli zwraca uwagę na potrzebę opracowania w MOPS wewnętrznych regulacji dotyczących rozwiązań na wypadek wystąpienia sytuacji nadzwyczajnych, np. długotrwałego braku zasilania lub przywracania systemów po awarii oraz planu ciągłości działania, umożliwiającego kontynuację wykonywania zadań. Dokument ten powinien określić systemy i aplikacje o znaczeniu krytycznym oraz wszystkie podporządkowane lub powiązane plany. Istotne jest, aby były one jasno udokumentowane, przekazane pracownikom i aktualizowane w celu odzwierciedlenia bieżącej działalności Ośrodka. Dyrektor wyjaśniła, że: *„W dotychczasowej pracy MOPS nie wystąpiły sytuacje wymagające np. przywracania systemów po awarii czy długotrwałe okresy bez prądu. Podejmiemy jednak działania w celu opracowania takich regulacji."* (dowód: akta kontroli str. 4, 35-36)

Ocena cząstkowa

Najwyższa Izba Kontroli ocenia negatywnie działania MOPS dotyczące przestrzegania przyjętych procedur przechowywania i zabezpieczania danych oraz zapewnienia właściwej ich ochrony.

[27] Rozporządzenie Prezesa Rady Ministrów z dnia 18 stycznia 2011 r. w sprawie instrukcji kancelaryjnej, jednolitych rzeczowych wykazów akt oraz instrukcji w sprawie organizacji i zakresu działania archiwów zakładowych. (Dz. U. Nr 14, poz. 67 ze zm.).

4. Przetwarzanie zasobów informacyjnych zgodnych z zakresem działalności kontrolowanej jednostki

Opis stanu faktycznego

4.1. W okresie objętym kontrolą w MOPS przetwarzano dane osobowe w dziewięciu zbiorach danych (w tym siedmiu z wykorzystaniem systemów elektronicznych). W wykazie zbiorów danych, będących załącznikiem do Polityki bezpieczeństwa ujęto sześć z dziewięciu prowadzonych zbiorów. (dowód: akta kontroli str. 9, 53-55, 59-61)

4.2. W okresie objętym kontrolą nie dokonywano aktualizacji zbiorów danych zgłoszonych przez MOPS do rejestracji do GIODO, mimo zaistnienia w czterech przypadkach (z dziewięciu objętych analizą) okoliczności, które powodowały konieczność takiej aktualizacji, co szerzej opisano w dalszej części niniejszego wystąpienia, w sekcji „Ustalone nieprawidłowości". (dowód: akta kontroli str. 33-34, 139-140)

4.3. Analiza danych przetwarzanych w dziewięciu zbiorach wykazała, że we wszystkich przypadkach gromadzone dane były niezbędne do realizacji zadań, dla których je prowadzono.

Zgodnie z regulaminem naboru na wolne stanowiska urzędnicze w MOPS[28], warunkiem udziału w naborze było wyrażenie zgody przez kandydata na przetwarzanie danych osobowych zawartych w ofercie, niezbędnych do realizacji procesu rekrutacji. W latach 2016 – 2017 w czterech ogłoszeniach o naborze wskazano informacje wymagane art. 24 ust. 1 ustawy o ochronie danych osobowych. (dowód: akta kontroli str. 139-150)

4.4. MOPS, na podstawie umowy zawartej 18 grudnia 2013 r. z Dyrektorem Powiatowego Urzędu Pracy w Siemiatyczach, uzyskał – za pośrednictwem platformy SEPI – dostęp do danych osobowych beneficjentów MOPS zarejestrowanych w PUP. Strony umowy zobowiązały się do zachowania w tajemnicy danych osobowych beneficjentów oraz ich zabezpieczenia zgodnie z zasadami określonymi w ustawie o ochronie danych osobowych. Pracownicy PUP zostali upoważnieni do przetwarzania tych danych przez Dyrektor MOPS.

Korzystano także z platformy wymiany informacji Emp@tia, tj. portalu prowadzonego przez Ministerstwo Rodziny Pracy i Polityki Społecznej służącemu m.in. do pozyskiwania i wymianie informacji o klientach MOPS pomiędzy jednostkami pomocy społecznej.

Uzyskanie dostępu do ww. zbiorów nie wymagało spełnienia przez Ośrodek specjalnych warunków takich, jak np. stworzenie wydzielonego łącza internetowego czy budowy określonej struktury sieci. (dowód: akta kontroli str. 33-34, 151-172)

Ustalone nieprawidłowości

W działalności kontrolowanej jednostki w przedstawionym wyżej zakresie stwierdzono nieprawidłowość, polegającą na niezaktualizowaniu zgłoszenia rejestracyjnego czterech zbiorów danych osobowych, w związku z gromadzeniem w nich danych w szerszym zakresie niż był zgłoszony do GIODO[29]. 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 MOPS wyjaśnił, że: *„Nie dokonywano aktualizacji zbiorów danych zgłoszonych przez MOPS (...) z uwagi na fakt niepoinformowania mnie przez kierowników poszczególnych działów, w których te zbiory prowadzono o takiej sytuacji. Samodzielnie nie jestem w stanie wszystkiego sprawdzić".*

(dowód: akta kontroli str. 56-58, 139-140, 198-213)

Ocena cząstkowa

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

---

[28] Zarządzenie Nr 5/15 z 15 października 2015 r. kierownika MOPS w Siemiatyczach w sprawie ustalenia Regulaminu naboru pracowników na wolne stanowiska urzędnicze w MOPS w Siemiatyczach.

[29] W rejestrach przetwarzano dane, które nie zostały wskazane we wnioskach o rejestrację zbiorów. W zbiorze „Fundusz alimentacyjny" dodatkowo przetwarzano: imiona i nazwiska rodziców, miejsce urodzenia, miejsce pracy i zawód oraz dane dotyczące skazania; w zbiorze „Świadczenia wychowawcze 500+ Miasto Siemiatycze" dodatkowo przetwarzano: imiona i nazwiska rodziców oraz stan zdrowia; w zbiorze „Dodatki mieszkaniowe" dodatkowo przetwarzano dane dotyczące stanu zdrowia; w zbiorze „Zespół Interdyscyplinarny ds. przeciwdziałania przemocy w Mieście Siemiatycze" dodatkowo gromadzono: imiona i nazwiska rodziców, miejsce pracy, stan zdrowia, nałogi, orzeczenia wydane w postępowaniach sądowych lub administracyjnych. W trakcie kontroli zgłoszono do GIODO aktualizację danych w ww. zbiorach.

IV. Wnioski

Wnioski pokontrolne

Przedstawiając powyższe oceny 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[30], wnosi o:

1. Zabezpieczenie odpowiedniej jakości hasłami dostępu do wszystkich komputerów i systemów dziedzinowych wykorzystanych do przetwarzania danych osobowych.
2. Ujęcie w prowadzonym w MOPS wykazie zbiorów danych osobowych wszystkich zbiorów wykorzystywanych w Ośrodku.
3. Wywiązywanie się z obowiązków określonych w § 20 ust. 2 pkt 2 i 3 oraz pkt 7 lit. a rozporządzenia KRI.
4. Dostosowanie upoważnień poszczególnych pracowników do dostępu do systemów wykorzystywanych w MOPS do zakresu ich obowiązków.
5. Przeprowadzanie, w ramach obowiązku wynikającego z art. 36a ust. 2 w związku z art. 36b ustawy o ochronie danych osobowych, okresowych sprawdzeń przetwarzania danych osobowych z przepisami o ochronie danych osobowych.
6. Przeprowadzanie corocznych audytów wewnętrznych z zakresu bezpieczeństwa informacji, zgodnie z wymogiem wynikającym z § 20 ust. 2 pkt 14 rozporządzenia KRI.
7. Opracowanie i wdrożenie Polityki bezpieczeństwa informacji, stosownie do wymogów wynikających z § 2 pkt 15 w związku z § 20 ust. 1 i ust. 2 rozporządzenia KRI.
8. Zapewnienie szkoleń dla wszystkich pracowników MOPS z zakresu m.in. bezpieczeństwa przetwarzania informacji.
9. Zapewnienie danym osobowym przechowywanym w archiwum i serwerze właściwej ochrony przed działaniem czynników fizycznych i zdarzeń losowych.

V. Pozostałe informacje i pouczenia

Prawo zgłoszenia zastrzeżeń

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

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

Obowiązek poinformowania NIK o sposobie wykorzystania uwag i wykonania wniosków

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

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

Białystok, dnia 9 lutego 2018 r.

Kontroler
Piotr Jurkin
starszy inspektor kontroli państwowej

Piotr Jurkin
.....
podpis

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

.....
podpis

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