NAJWYŻSZA IZBA KONTROLI
Delegatura w Białymstoku

LBI.410.023.24.2017
P/17/062

00370218

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 — Marek Zapolski – doradca ekonomiczny, upoważnienie do kontroli nr LBI/5/2018 z 3 stycznia 2018 r. (dowód: akta kontroli str. 1-2)

Jednostka kontrolowana — Miejski Ośrodek Pomocy Społecznej w Zambrowie, 18-300 Zambrów, ul. Fabryczna 3 (dalej: „MOPS" lub „Ośrodek")

Kierownik jednostki kontrolowanej — Janina Komorowska – dyrektor MOPS[1]. (dowód: akta kontroli str. 3)

II. Ocena kontrolowanej działalności[2]

Ocena ogólna

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

Uzasadnienie oceny ogólnej

Stwierdzono bowiem nieprawidłowości, polegające w szczególności na:

- nadaniu jednemu pracownikowi MOPS uprawnień do zarządzania systemem operacyjnym komputera w stopniu większym niż wymagany do realizowania przez niego zadań i obowiązków,
- dopuszczeniu do przetwarzania danych osobowych osoby nieposiadającej upoważnienia do przetwarzania danych osobowych,
- niemonitorowaniu dostępu do zasobów informacyjnych Ośrodka,
- nieprzeprowadzaniu analiz ryzyka utraty integralności, dostępności lub poufności informacji oraz corocznych audytów wewnętrznych z zakresu bezpieczeństwa informacji,
- nieprowadzeniu bieżącej inwentaryzacji sprzętu i oprogramowania służącego do przetwarzania informacji w Ośrodku,
- niedopełnieniu obowiązku zgłoszenia GIODO[4] jednego zbioru danych osobowych,
- nieprawidłowym sporządzeniu dokumentacji opisującej sposób przetwarzania danych w Ośrodku,
- nieprowadzeniu przez ABI[5] rejestru zbioru danych osobowych,
- nierzetelnym sporządzaniu przez ABI sprawozdania ze sprawdzenia zgodności przetwarzania danych osobowych w Ośrodku z przepisami o ochronie danych osobowych oraz nieprawidłowym przygotowaniem planów tych sprawdzeń,
- niezapewnieniu wszystkim pracownikom zaangażowanym w proces przetwarzania informacji szkoleń dotyczących ochrony danych osobowych oraz bezpieczeństwa informacji,
- nieokreśleniu podstawowych zasad gwarantujących bezpieczną pracę przy przetwarzaniu mobilnym i pracy na odległość.

---

1 Od 1 marca 1994 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, tj. do 23 stycznia 2018 r.
4 Generalny Inspektor Ochrony Danych Osobowych.
5 Administrator Bezpieczeństwa Informacji.

III. Opis ustalonego stanu faktycznego

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

Opis stanu faktycznego

1.1. MOPS wyposażony był w 32 stacjonarne zestawy komputerowe spięte wewnętrzną siecią LAN z dostępem do Internetu oraz dwa laptopy. Dysponował też dwoma terminalami przenośnymi, co opisano w punkcie 3.5 wystąpienia. Do gromadzenia i przetwarzania danych niezbędnych do załatwienia spraw z zakresu pomocy społecznej wykorzystywano pięć informatycznych systemów dziedzinowych, co szerzej opisano w punkcie 4.1 wystąpienia. Ponadto Ośrodek korzystał z systemu „Płace i Budżet" do prowadzenia obsługi księgowości oraz spraw kadrowo-płacowych, aplikacji „Płatnik" do przygotowania oraz transmisji dokumentów ubezpieczeniowych do ZUS, Samorządowej Elektronicznej Platformy Informacyjnej (dalej: „SEPI") oraz platformy Emp@tia, co opisano w punkcie 4.4 wystąpienia. Dostęp do ww. systemów informatycznych mieli użytkownicy 24 komputerów. Pozostałe osiem komputerów oraz dwa laptopy Ośrodek wykorzystywał jako stacje dostępowe do Internetu i edytory tekstów.

Według powołanego przez NIK biegłego w dziedzinie bezpieczeństwa systemów informatycznych, w sieci LAN Ośrodka pracowały dwa serwery. Oba umiejscowiono w wydzielonym pomieszczeniu, do którego dostęp miały tylko osoby uprawnione. W pomieszczeniu tym urządzono też archiwum akt, co opisano w punkcie 3.1 wystąpienia. W sieci brak było serwera plików, czy maszyny służącej do obsługi backupów.

(dowód: akta kontroli str. 4-5, 8-11, 12-13,14-15, 67-76, 178-183)

1.2. W okresie objętym kontrolą w Ośrodku nie przeprowadzono analizy ryzyka utraty integralności, dostępności lub poufności informacji wymaganej w § 20 ust. 2 pkt 3 rozporządzenia Rady Ministrów z dnia 12 kwietnia 2012 r. w sprawie Krajowych Ram Interoperacyjności, minimalnych wymagań dla rejestrów publicznych i wymiany informacji w postaci elektronicznej oraz minimalnych wymagań dla systemów teleinformatycznych[6], co opisano w dalszej części wystąpienia w sekcji „Ustalone nieprawidłowości".

(dowód: akta kontroli str. 12-13)

1.3. Według stanu na 23 stycznia 2018 r., spośród 36 pracowników Ośrodka, do przetwarzania danych w informatycznych systemach dziedzinowych upoważniono 25 osób, a 11 – do baz danych prowadzonych w jedynie wersji papierowej. Analiza akt osobowych 30 pracowników wykazała, że posiadali oni dostęp do zbiorów danych w zakresie wynikającym z wyznaczonych im zadań. Według opinii biegłego w dziedzinie bezpieczeństwa systemów informatycznych, na wszystkich komputerach wydzielone były dwa konta, tj. administratora i użytkownika (bez uprawnień administratora), z wyjątkiem komputera obsługiwanego przez główną księgową Ośrodka, która miała takie uprawnienia. Osoby przetwarzające dane w systemach informatycznych posiadały własny login i indywidualne hasła dostępowe o odpowiedniej liczbie znaków. Aktywowany był mechanizm wymuszenia okresowej zmiany (co 30 dni) hasła do systemu operacyjnego, którego długość odpowiadała wysokiemu poziomowi bezpieczeństwa. Podobnie aplikacje dziedzinowe wykorzystywane w Ośrodku wymuszały zmianę hasła co 30 dni. Obowiązująca w MOPS Instrukcja zarządzania systemem informatycznym nie określała warunków złożoności haseł dostępowych do systemów informatycznych Ośrodka. Nie stwierdzono przypadków użytkowania jednego konta przez kilku użytkowników, a konta osób niepracujących już w MOPS zostały zablokowane.

(dowód: akta kontroli str. 8-11, 24-31, 32-34, 150-153, 315)

1.4. W okresie objętym kontrolą nie prowadzono rejestru dostępu do systemów. Ustalenia biegłego wskazują, że każdy z komputerów domyślnie (rejestr zdarzeń systemu operacyjnego) gromadził logi systemowe na własnym dysku lokalnym. Nie były one jednak zabezpieczane przed modyfikacją (poza jednym komputerem), nie były agregowane ani automatycznie analizowane. W MOPS nie były gromadzone logi ruchu sieciowego z racji zbudowania sieci na niskiej klasy routerze. Nie zastosowano żadnych środków, które

[6] Dz. U. z 2017 r. poz. 2247. Rozporządzenie zwane dalej „rozporządzeniem KRI".

chroniłyby gromadzące się na komputerach logi przed utratą integralności lub skasowaniem (logi nie były objęte procesem tworzenia kopii danych), co szerzej opisano w dalszej części wystąpienia pokontrolnego, w sekcji „Ustalone nieprawidłowości".

(dowód: akta kontroli str. 8-11)

1.5. Środkiem zabezpieczającym przed nieautoryzowanym dostępem do systemów operacyjnych komputerów oraz systemów dziedzinowych było hasło użytkownika. W ramach sieci LAN Ośrodka nie działała sieć WI-FI. Urządzenia sieciowe były zabezpieczone przed fizyczną ingerencją osób do tego nieupoważnionych z racji umieszczenia ich w pomieszczeniu o ograniczonym dostępie. Według opinii biegłego poziom zabezpieczeń odpowiedzialnych za autoryzację dostępu do sieci MOPS był wykonany odpowiednio. (dowód: akta kontroli str. 8-11)

1.6. Z opinii biegłego wynika, że konfiguracja sieciowa umożliwiała podłączenie do infrastruktury jednostki sprzętu (pamięci przenośne, laptopy, telefony, tablety) niestanowiącego własności pracodawcy, a porty USB nie były zabezpieczone przed zapisem i odczytem. Fakt podłączenia takich akcesoriów był odnotowywany w logach systemów operacyjnych, lecz informacja o zaistniałej sytuacji nie była zabezpieczana w sposób trwały, co opisano w pkt. 1.5 wystąpienia. W ocenie biegłego powyższe okoliczności pozwalają uznać, że elektroniczne zasoby informacyjne MOPS nie były właściwie chronione przed nieuprawnionym dostępem lub przejęciem.

ABI wyjaśnił, że: *„Istnieje możliwość podłączenia do sytemu zewnętrznego nośnika pamięci (pendrive, dysk przenośny) i skopiowanie danych z komputera. Jednakże pracownicy MOPS są zobowiązani do zachowania poufności na temat danych, które są przez nich przetwarzane. Dla zwiększenia bezpieczeństwa danych zostanie wprowadzona blokada instalowania nośników zewnętrznych w systemie komputerowym oraz filtrowanie adresów MAC, co spowoduje, że do sieci MOPS nie będzie możliwości podłączenia sprzętu nie będącego własnością pracodawcy".* (dowód: akta kontroli str. 8-11, 78)

1.7. Z wyjaśnień dyrektora Ośrodka oraz ABI wynika, że w latach 2016 – 2017 w MOPS nie odnotowano działań związanych z nieautoryzowanym przetwarzaniem informacji, tj. przypadków naruszenia bezpieczeństwa systemu informatycznego lub utraty integralności, dostępności lub poufności informacji. (dowód: akta kontroli str. 35-39, 50-55)

1.8. W MOPS nie przewidziano zdalnego dostępu do zasobów informacyjnych Ośrodka i taki dostęp nie funkcjonował. (dowód: akta kontroli str. 8-11)

1.9. Ośrodek nie zlecał podmiotom zewnętrznym realizacji usług serwisowych urządzeń komputerowych. Usuwaniem awarii i drobnych problemów technicznych w funkcjonowaniu urządzeń, zajmował się ASI[7], pełniący jednocześnie funkcję ABI. Wyjaśnił on, że: *„W latach 2016 – 2017 nie wystąpiły awarie sprzętu ani oprogramowania, które wymagałyby interwencji podmiotów zewnętrznych. Czasami zdarzają się takie przypadki jak zacięcie drukarki, źle działająca myszka, klawiatura. Są to nieliczne zdarzenia, które rozwiązuję we własnym zakresie. W powyższym okresie nie odnotowano zainfekowania komputerów złośliwym oprogramowaniem".* (dowód: akta kontroli str. 77-78)

W okresie objętym kontrolą Ośrodek posiadał umowę o świadczenie usług serwisowych oprogramowania „Płace i Budżet". W umowie serwisowej zawarto zapis gwarantujący odpowiedni poziom bezpieczeństwa informacji. (dowód: akta kontroli str. 65-66)

1.10. System informatyczny MOPS zabezpieczono przed działaniem oprogramowania, którego celem jest uzyskanie nieuprawnionego dostępu. Powołany przez NIK biegły stwierdził, że dostęp do Internetu realizowany był poprzez łącze światłowodowe, a sieć odseparowana była od Internetu firewallem, stanowiącym integralną część routera odpowiedzialnego za zarządzanie siecią w MOPS. Wszystkie komputery Ośrodka wchodzące w skład sieci lokalnej posiadały aktualne wersje aplikacji zabezpieczających. Nie zastosowano jednak w nich konsoli centralnego zarządzania, umożliwiającej m.in. monitorowanie komputerów działających w sieci. (dowód: akta kontroli str. 8-11)

---

[7] Administrator Systemów Informatycznych.

ABI wyjaśnił, że: *„Ze względu na brak środków finansowych nie był w MOPS zakupiony program, czy urządzenie, które by pozwalało na śledzenie ruchu sieciowego. Obecnie jest planowany zakup urządzenia klasy UTM, które pozwoli na rozwiązanie tej kwestii".*
(dowód: akta kontroli str. 76)

1.11. Ośrodek korzystał z możliwości posługiwania się pocztą elektroniczną. W ogólnych warunkach umowy (rozdział II pkt 2) dostawca usługi zobowiązał się do podjęcia wszelkich technicznie możliwych i uzasadnionych kroków w celu ochrony danych zgromadzonych w panelu Ośrodka przed dostępem i ingerencją osób trzecich, jak również przed nieuprawnionym użyciem panelu MOPS. ABI wyjaśnił, że: *„Poczta elektroniczna ma uruchomiony filtr antyspamowy, który sprawdza przychodzące wiadomości i określa czy dana wiadomość to spam".* (dowód: akta kontroli str. 82-87, 314)

1.12. Zgodnie z pkt. 9 obowiązującej w Ośrodku Polityki Bezpieczeństwa[8] (dalej PB), kopie bezpieczeństwa zbiorów danych przetwarzanych informatycznie powinny być wykonywane okresowo i przechowywane na nośnikach zewnętrznych. W pkt 4 Instrukcji zarządzania systemem informatycznym przewidziano, że: [1] za systematyczne przygotowanie kopii bezpieczeństwa odpowiada ABI, [2] kopie bezpieczeństwa wykonywane są na dysku twardym oraz okresowo na nośniku zewnętrznym, [3] nośniki z kopiami bezpieczeństwa przechowywane są w szafach zabezpieczonych zamkiem, uniemożliwiających bezpośredni dostęp osobom niepowołanym. Z opinii biegłego wynika, że w MOPS były tworzone kopie bezpieczeństwa danych. Bazy danych wszystkich aplikacji dziedzinowych były backupowane średnio raz na dwa tygodnie – przy okazji wykonywania aktualizacji aplikacji. Kopie były zapisywane na wydzielonej partycji dysku twardego serwera i przechowywane przez okres około dwóch lat. W trakcie oględzin stwierdzono, że w sejfie przechowywano 15 nośników optycznych (płyty CD) zawierających bazy danych (ośmiokrotnie skopiowane w 2016 roku i siedmiokrotnie w 2017 roku). ABI wyjaśnił, że: *„Przechowywane kopie baz danych są sprawdzane. Do chwili obecnej nie wystąpiła konieczność odzyskania bazy danych z kopii zapasowej."* (dowód: akta kontroli str. 8-11, 88, 170-175, 178-183, 314)

1.13. Na 16 stycznia 2018 r. systemy operacyjne 30 komputerów objęte były wsparciem technicznym producenta tego oprogramowania, a 8 kwietnia 2014 r. takie wsparcie ustało dla systemów operacyjnych czterech pozostałych komputerów, co zostało opisane w dalszej części wystąpienia pokontrolnego, w sekcji „Uwagi dotyczące badanej działalności". Biegły w dziedzinie bezpieczeństwa systemów informatycznych stwierdził, że pełne uprawnienia do zarządzania komputerami posiadał tylko ABI. Jednak pracownicy MOPS dysponowali możliwością ściągania aplikacji i plików wykonalnych. Pomimo, że nie posiadali oni uprawnienia do instalacji ściągniętych aplikacji i plików (z wyjątkiem głównej księgowej), w ocenie biegłego stwarzało to zagrożenie zainfekowania komputerów złośliwym oprogramowaniem. W Ośrodku nie prowadzono ewidencji programów zainstalowanych na poszczególnych stacjach komputerowych. Dopiero w trakcie kontroli ABI sporządził wykazy zainstalowanego oprogramowania na każdej jednostce.
(dowód: akta kontroli str. 4-5, 8-11, 12-13)

1.14. Według opinii biegłego, aktualizacje systemów operacyjnych były wykonywane zgodnie z harmonogramem domyślnie ustawionym przez dostawcę systemu. Aktualne było również oprogramowanie dziedzinowe. Tryb jego aktualizacji wynikał również z domyślnych ustawień aplikacji. (dowód: akta kontroli str. 8-11)

1.15. Od czerwca 2012 roku Ośrodek korzystał z sytemu bankowości internetowej na podstawie umowy zawartej z bankiem prowadzącym obsługę rachunków MOPS. Przelewy świadczeń pieniężnych na rzecz osób uprawnionych (po zweryfikowaniu danych beneficjenta) realizowano na podstawie dyspozycji Ośrodka, potwierdzonych podpisem elektronicznym przez dwóch pracowników, którym Polska Wytwórnia Papierów Wartościowych S.A. w Warszawie wystawiła certyfikaty, zgodnie z umową z 1 lipca 2016 r. o świadczenie usług certyfikacyjnych. (dowód: akta kontroli str. 88-99)

[8] Ustalona zarządzeniem Or. 021.1.20.2016 dyrektora Miejskiego Ośrodka Pomocy Społecznej w Zambrowie z dnia 22 grudnia 2016 r. w sprawie wprowadzenia „Polityki bezpieczeństwa" i „Instrukcji zarzadzania systemem informatycznym służącym do przetwarzania danych osobowych".

Ustalone nieprawidłowości

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

1. W MOPS nie przeprowadzono analizy ryzyka utraty integralności, dostępności lub poufności informacji, wymaganej § 20 ust. 2 pkt 3 rozporządzenia KRI.

   Dyrektor Ośrodka nie podała przyczyn braku takich analiz. Wyjaśniła, że: *„Aktualnie zostały podjęte działania w celu dokonania analizy ryzyka utraty integralności, dostępności lub poufności informacji oraz zgromadzenia ofert w tym zakresie".*

   (dowód: akta kontroli str: 12-13, 37-39)

2. W Ośrodku nie monitorowano dostępu do jego zasobów informacyjnych. Nie prowadzono papierowej wersji rejestru dostępu do systemów informatycznych wykorzystywanych do przetwarzania danych, a logi gromadzone domyślnie w rejestrze zdarzeń systemów operacyjnych komputerów wykorzystywanych w MOPS nie były agregowane, analizowane ani chronione przed utratą integralności i skasowaniem. Nie objęto ich też procesem tworzenia kopii danych (backupu). Mogło to uniemożliwić odtworzenie tego co działo się z zasobami informacyjnymi MOPS, w tym w wyniku podłączenia akcesoriów do portów USB komputerów. Monitorowanie dostępu do informacji jest – w myśl § 20 ust. 2 pkt 7 lit. a) rozporządzenia KRI – jednym z elementów zarządzania jej bezpieczeństwem, zmierzającym do zapewnienia ochrony przetwarzanych informacji przed kradzieżą, nieuprawnionym dostępem, uszkodzeniami lub zakłóceniami.

   ABI wyjaśnił, że: *„W MOPS w Zambrowie nie jest prowadzony rejestr dostępu do systemu, ze względu na uciążliwość dla użytkowników systemów jaką by prowadzenie takiego rejestru powodowała. W każdym systemie jest domyślnie prowadzony rejestr zdarzeń, który jest zapisywany na dysku lokalnym komputera. Do tej pory nie były one archiwizowane na innym nośniku. Postanowiono uszczegółowić zapisy w polityce bezpieczeństwa dotyczące tej kwestii i określenia okresu z jakim powinny być logi systemowe kopiowane na zewnętrznych nośnikach. Ze względu na brak środków finansowych nie był w MOPS zakupiony program, czy urządzenie, które by pozwalało na śledzenie ruchu sieciowego."* (dowód: akta kontroli str. 8-11, 78)

3. Główna księgowa Ośrodka w bieżącej pracy wykorzystywała konto z uprawnieniami administratora systemu operacyjnego komputera. W wyniku tego mogła – nawet w sposób przypadkowy – pobierać aplikacje i pliki wykonalne oraz je instalować. 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.

   ABI wyjaśnił, że: *„Główna księgowa Ośrodka posiada uprawnienia administratora do pracy w systemie operacyjnym komputera, ponieważ wykorzystuje program „Budżet" oraz system sprawozdawczy „Besti@", który do poprawnego działania wymaga uruchomienia przez administratora. Ponadto osoba ta, poza dostępem do papierowego zbioru „Ewidencja klientów Ośrodka Pomocy Społecznej w Zambrowie" nie posiada upoważnień do pozostałych zbiorów prowadzonych za pomocą dziedzinowych systemów informatycznych".* (dowód: akta kontroli str. 8-11, 314)

Uwagi dotyczące badanej działalności

Najwyższa Izba Kontroli zwraca uwagę na możliwość pełniejszego wykorzystania aplikacji bezpieczeństwa użytkowanej w Ośrodku, bowiem aplikacja ta, poza funkcją ochrony przez złośliwym oprogramowaniem, udostępnia narzędzia do monitorowania i zabezpieczenia komputerów działających w sieci lokalnej. Najwyższa Izba Kontroli zwraca też uwagę, że podłączanie do sieci LAN Ośrodka komputerów z systemami operacyjnymi, które nie są objęte wsparciem technicznym producenta może stanowić zagrożenie bezpieczeństwa sieci.

ASI wyjaśnił, że: *„W miarę możliwości finansowych w MOPS są dokonywane wymiany komputerów stacjonarnych z systemem Windows XP na komputery z zainstalowanymi aktualnymi wersjami systemu Windows. Obecnie zostały zakupione dwa komputery*

z systemem Windows 10, które zastąpią wykorzystywane obecnie komputery z systemem Windows XP. Wymiana pozostałych komputerów będzie dokonana, gdy pozwolą na to środki finansowe". (dowód: akta kontroli str. 314)

Ocena cząstkowa

Najwyższa Izba Kontroli ocenia negatywnie skuteczność przyjętych w MOPS rozwiązań dotyczących zabezpieczenia poszczególnych systemów informatycznych i usług sieciowych przed nieuprawnionym dostępem, przejęciem lub zniszczeniem danych.

2. Dokumentacja i procedury dotyczące ochrony danych

Opis stanu faktycznego

2.1. W MOPS prowadzono 11 zbiorów danych osobowych. W PB wyszczególniono dziewięć z nich. Nie wykazano dwóch zbiorów: „Dodatki energetyczne" oraz „Świadczenia za życiem", którego nie zgłoszono też do zarejestrowania GIODO, co opisano w dalszej części wystąpienia, w sekcji „Ustalone nieprawidłowości". Do dnia kontroli GIODO zarejestrował sześć[9] z dziewięciu zgłoszonych zbiorów, z tego: jeden („Ewidencja klientów Ośrodka Pomocy Społecznej w Zambrowie") w 2000 roku i pięć w styczniu i lutym 2012 roku. W okresie objętym kontrolą MOPS nie aktualizował danych rejestracyjnych zbiorów zgłoszonych do GIODO, mimo że wystąpiła taka potrzeba, co opisano w punkcie 4.3 wystąpienia. W przypadku trzech zgłoszonych zbiorów[10] (do dnia zakończenia kontroli) brak było informacji o odmowie rejestracji. Z dokumentacji wynika, że w czerwcu 2016 roku GIODO zażądał od dyrektora Ośrodka wyjaśnień dotyczących zamiaru przetwarzania danych ujawniających pochodzenie etniczne w zbiorze „Rodzina 500+" i pochodzenie rasowe w zbiorze „Wspieranie rodziny". Z udzielonych wyjaśnień wynika, że Ośrodek w tym zakresie powołał się na art. 100 ust. 2 ustawy z dnia 12 marca 2004 r. o pomocy społecznej[11], który przed przyznaniem i udzieleniem świadczeń z pomocy społecznej umożliwia przetwarzanie danych osób ubiegających się i korzystających z tych świadczeń dotyczących: pochodzenia etnicznego, stanu zdrowia, nałogów, skazań, orzeczeń o ukaraniu, a także innych orzeczeń wydanych w postępowaniu sądowym lub administracyjnym. Do dnia kontroli brak jest stanowiska GIODO w powyższej sprawie. W wykazanych w PB zbiorach nie określono zakresu danych w nich przetwarzanych. Ośrodek nie dysponuje też rejestrem zbioru danych, co opisano w dalszej części wystąpienia, w sekcji „Ustalone nieprawidłowości".

(dowód: akta kontroli str. 40-47, 53-55, 100-124, 170-175)

2.2. Na podstawie umowy z 2 stycznia 2015 r. Kierownik MOPS powierzyła informatykowi Urzędu Miejskiego w Zambrowie pełnienie funkcji ABI oraz funkcji ASI, którego zakres obowiązków opisano w punkcie 2.6 wystąpienia. Kierownik Ośrodka, w terminie określonym w art. 46b ust. 1 ustawy z dnia 29 sierpnia 1997 r. o ochronie danych osobowych[12], zgłosiła GIODO do rejestracji powołanie ABI. W zgłoszeniu zawarto wszystkie elementy wymagane w art. 46b ust. 2 ww. ustawy. Jednak dopiero w trakcie kontroli ABI wydano upoważnienie do przetwarzania danych osobowych, co opisano w dalszej części wystąpienia, w sekcji „Ustalone nieprawidłowości". (dowód: akta kontroli str. 48, 125-131 132-133)

2.3. Z dokumentacji Ośrodka wynika, że ABI w okresie objętym kontrolą nie wywiązał się z obowiązków określonych w art. 36a ust. 2 uodo, gdyż:

- dokumentacja opisująca sposób przetwarzania danych była wadliwa, co opisano w punkcie 2.10 wystąpienia,
- w aktach osobowych pracowników Ośrodka brak było potwierdzeń, że zostali zapoznani z przepisami o ochronie danych osobowych, co opisano w punkcie 2.8 wystąpienia,
- nie dopełnił obowiązku prowadzenia rejestru zbioru danych, co opisano w dalszej części wystąpienia, w punkcie 3 sekcji „Ustalone nieprawidłowości",
- przeprowadził sprawdzenie zgodności przestrzegania zasad ochrony danych osobowych niezgodnie z zasadami określonymi w § 3 ust. 4 rozporządzenia Ministra Administracji i Cyfryzacji z dnia 11 maja 2015 r. w sprawie trybu i sposobu realizacji zadań w celu zapewniania przestrzegania przepisów o ochronie danych osobowych przez

[9] „Ewidencja Klientów Ośrodka Pomocy Społecznej w Zambrowie", „Przemoc w Rodzinie", „Świadczenia Rodzinne", „Świadczenia alimentacyjne i dłużnicy alimentacyjni", „Dodatki mieszkaniowe", „Przeciwdziałanie alkoholizmowi".

[10] „Zasiłek dla opiekuna", „Wspieranie rodziny" i „Rodzina 500+".

[11] Dz. U. z 2017 r. poz. 1769, ze zm.

[12] Dz. U. 2016 r. poz. 922. Ustawa zwana dalej: „uodo".

administratora bezpieczeństwa informacji[13]. Z dokumentacji zrealizowanych czynności wynika bowiem, że plany sprawdzeń nie odpowiadały formie i treści określonej w § 3 ust. 3 powołanego rozporządzenia, a w sprawozdaniu ze sprawdzenia podano nierzetelne informacje, co opisano w dalszej części wystąpienia, w sekcji „Ustalone nieprawidłowości". (dowód: akta kontroli str. 134-138)

2.4. Według stanu na 4 stycznia 2018 r., prowadzona w Ośrodku ewidencja osób upoważnionych do przetwarzania danych osobowych nie odpowiadała wymogom określonym w art. 39 ust. uodo, gdyż nie zawierała informacji o zakresie upoważnienia do przetwarzania danych oraz zawierała nierzetelne dane. Wykazano w niej bowiem, że:

- 12 pracowników Ośrodka upoważnionych było do przetwarzania danych w zbiorze „Ewidencja klientów Ośrodka Pomocy Społecznej w Zambrowie" – dopiero w trakcie kontroli (4 stycznia 2018 r.) ewidencję tę uzupełniono i wykazano nazwiska wszystkich 20 osób upoważnionych do tych danych,
- ośmiu pracowników upoważnionych było do danych w zbiorze „Świadczenia rodzinne", a dopiero w trakcie kontroli ewidencję uzupełniono o nazwisko jednego pracownika upoważnionego do zbioru w maju 2017 roku,
- sześciu pracowników upoważnionych było do danych w zbiorze „Świadczenia alimentacyjne i dłużnicy alimentacyjni" – w trakcie kontroli ewidencję zaktualizowano poprzez wykazanie daty cofnięcia upoważnienia jednemu pracownikowi (z dniem 3 marca 2017 r.), uzupełniano o jednego pracownika upoważnionego 28 maja 2017 r. oraz dopisano nazwisko zastępcy dyrektora Ośrodka,
- sześć osób upoważnionych było do danych w zbiorze „Rodzina 500+", natomiast w trakcie kontroli ewidencję zaktualizowano, poprzez odnotowanie daty cofnięcia upoważnienia jednemu pracownikowi z dniem 3 marca 2017 r. oraz wykazano datę nadania upoważnienia jednemu pracownikowi z dniem 28 maja 2017 r.,
- jeden pracownik upoważniony był do danych w zbiorze „Dodatki mieszkaniowe", któremu cofnięto upoważnienie z dniem 31 maja 2017 r., a w trakcie kontroli ewidencję zaktualizowano o nazwisko jednego pracownika upoważnionego 28 czerwca 2017 r. oraz dopisano nazwisko zastępcy dyrektora Ośrodka,
- jeden pracownik był upoważniony do danych w zbiorze „Przeciwdziałanie alkoholizmowi", natomiast w trakcie kontroli wykaz zaktualizowano o nazwisko zastępcy dyrektora Ośrodka,
- 12 pracowników upoważnionych było do danych w zbiorze „Przemoc w rodzinie", podczas gdy w trakcie kontroli odnotowano cofnięcie upoważnienia jednemu pracownikowi w dniu 25 kwietnia 2017 r. oraz uzupełniono o nazwiska dwóch pracowników upoważnionych odpowiednio w lipcu i listopadzie 2017 roku.

(dowód: akta kontroli str. 139-145)

2.5. W okresie objętym kontrolą w Ośrodku nie zaszły zmiany organizacyjne powodujące konieczność wprowadzenia nowych lub zmiany istniejących wewnętrznych procedur, instrukcji i poleceń, dotyczących sposobu gromadzenia i przetwarzania zasobów informacyjnych w jednostce. (dowód: akta kontroli str. 12-13)

2.6. W okresie objętym kontrolą pełnienie obowiązków ASI zlecono osobie pełniącej jednocześnie obowiązki ABI. Był on zobowiązany do opieki i nadzoru nad sprzętem i oprogramowaniem komputerowym w MOPS. W szczególności do:

- kontaktowania się z producentami i aktualizowania oprogramowania dziedzinowego,
- uczestniczenia w odbiorze ilościowym i jakościowym sprzętu komputerowego dostarczanego do MOPS,
- usuwania awarii sprzętu, a w razie awarii nie dającej się usunąć we własnym zakresie – dostarczenie sprzętu do punktu napraw, a następnie jego odbiór,
- dokonywania przeglądów sprzętu, a w razie jego nieużyteczności sporządzanie protokołów ich kasacji,

[13] Dz. U. poz. 745. Rozporządzenie zwane dalej „rozporządzeniem w sprawie realizacji zadań ABI".

- instalowania i uruchamiania aplikacji użytkowych i ich aktualizacji,
- prowadzenia instruktażu pracowników MOPS w zakresie obsługi,
- przesyłania danych do ZUS i Wydziału Spraw Społecznych Podlaskiego Urzędu Wojewódzkiego w Białymstoku,
- obsługi stron internetowych MOPS. (dowód: akta kontroli str. 125-131)

2.7. W okresie objętym kontrolą nie wywiązano się z obowiązku prowadzenia corocznych audytów wewnętrznych z zakresu bezpieczeństwa informacji, wymaganych § 20 ust. 2 pkt 14 rozporządzenia KRI, co opisano w dalszej części wystąpienia, w sekcji „Ustalone nieprawidłowości". (dowód: akta kontroli str. 12-13)

2.8. W latach 2016 – 2017 pracownicy Ośrodka nie uczestniczyli w szkoleniach dotyczących zagadnień związanych z ochroną danych osobowych oraz bezpieczeństwem informacji, co opisano w dalszej części wystąpienia pokontrolnego, w sekcji „Ustalone nieprawidłowości". Z analizy akt osobowych pracowników zatrudnionych w MOPS w Zambrowie wynika, że żaden z nich nie dysponował zaświadczeniem potwierdzającym odbycie szkolenia z zakresu ochrony danych osobowych. (dowód: akta kontroli str. 150-153)

W okresie objętym kontrolą dyrektor Ośrodka nie organizowała szkolenia związanego ze zmianą przepisów o ochronie danych osobowych, która ma wejść w życie 25 maja 2018 r., w związku z implementacją rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (ogólne rozporządzenie o ochronie danych)[14].

Dyrektor Ośrodka wyjaśniła, że: *„W związku z niezadowalającym dotychczas prowadzeniem dokumentacji dotyczącej ochrony danych osobowych, w dniu 15 stycznia 2018 r. MOPS w Zambrowie wystąpił z zapytaniem ofertowym dotyczącym świadczenia usługi w zakresie ABI w MOPS w Zambrowie. Aktualnie została już wybrana oferta i w dniu 5 lutego b.r. zostanie podpisana umowa na świadczenie tych usług. W Zapytaniu ofertowym MOPS w Zambrowie na świadczenie usługi ABI, zawarto zakres prac do wykonania przez usługobiorcę, który stanowić będzie załącznik do umowy na wykonywanie funkcji ABI w MOPS w Zambrowie. Usługobiorca zobowiązany będzie do:*

- *pełnienia funkcji ABI, zarządzania upoważnieniami do przetwarzania danych osobowych, prowadzenia ewidencji osób upoważnionych i jej aktualizowania, prowadzenia rejestru zbiorów danych,*
- *przejęcia funkcji inspektora ochrony danych osobowych po wejściu w życie Rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE,*
- *przeszkolenia pracowników MOPS w zakresie przepisów dotyczących ochrony danych osobowych,*
- *stworzenia bądź zaktualizowania Polityki Bezpieczeństwa, Instrukcji Zarządzania Systemem Informatycznym oraz ponowne zaktualizowanie tych dokumentów po wejściu w życie Rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r."* (dowód: akta kontroli str. 12-13, 316-322)

2.9. W latach 2016 – 2017 w Ośrodku nie prowadzono zewnętrznych kontroli w zakresie bezpieczeństwa danych. Nie odnotowano też skarg dotyczących ujawnienia danych osobowych lub naruszenia przepisów o ochronie danych osobowych. W trakcie kontroli (17 stycznia 2018 r.) do Ośrodka wpłynęło pismo dyrektora Wydziału Polityki Społecznej Podlaskiego Urzędu Wojewódzkiego w Białymstoku, w którym nakazano podjęcie działań zapewniających bezpieczeństwo informatyczne w jednostce.
(dowód: akta kontroli str. 12-13, 154, 155-157)

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

2.10. Do 21 grudnia 2016 r. w Ośrodku obowiązywały: [1] „Instrukcja ochrony danych osobowych w Miejskim Ośrodku Pomocy Społecznej w Zambrowie", [2] „Instrukcja zarządzania systemem informatycznym służącym do przetwarzania danych osobowych w Miejskim Ośrodku Pomocy Społecznej w Zambrowie", oraz [3] „Instrukcja postępowania w sytuacji naruszenia ochrony danych osobowych". Zarządzeniem Or.021.1.20.2016 dyrektora MOPS z dnia 22 grudnia 2016 r. wprowadzono natomiast PB i Instrukcję zarządzania systemem informatycznym służącym do przetwarzania danych osobowych". Analiza ich treści wykazała, że PB nie zawierała elementów wykazanych w § 4 pkt 1, 3, 4 i 5 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[15], a Instrukcja – elementów wyszczególnionych w § 5 pkt 8 ww. rozporządzenia, co opisano w dalszej części wystąpienia, w sekcji „Ustalone nieprawidłowości". W żadnym z ww. dokumentów nie określono też poziomu bezpieczeństwa przetwarzania danych osobowych w systemach informatycznych MOPS.

(dowód: akta kontroli str. 158-175)

Ustalone nieprawidłowości

W działalności kontrolowanej jednostki w przedstawionym zakresie stwierdzono następujące nieprawidłowości:

1. Do GIODO – wbrew postanowieniom art. 40 ust. uodo – nie zgłoszono do rejestracji zbioru danych osobowych „Świadczenia za życiem", który zawierał dane wrażliwe.

   Dyrektor Ośrodka wyjaśniła, że nie dokonała zgłoszenia zbioru „Za życiem", ponieważ *„(...) pierwszą decyzję wydano w lipcu 2017 roku i drugą we wrześniu 2017 roku. Do chwili obecnej więcej postępowań w tym zakresie nie było".* Dodała też, że 11 stycznia 2018 r. zbiór danych został zgłoszony do rejestracji w GIODO drogą elektroniczną, a wersja papierowa została wysłana pocztą.

   (dowód: akta kontroli str. 37-39, 40-47)

2. Wprowadzona 22 grudnia 2016 r. PB nie określała: szczegółowo obszaru przetwarzania danych; struktury zbiorów danych wskazującej zawartość poszczególnych pól informacyjnych i powiązania między nimi; sposobu przepływu danych pomiędzy poszczególnymi systemami; środków niezbędnych dla zapewnienia rozliczalności przetwarzanych danych, tj. elementów wymaganych § 4 pkt 1, 3, 4 i 5 rozporządzenia MSWiA. Natomiast w Instrukcji zarządzania systemem informatycznym nie określono procedury wykonywania przeglądów i konserwacji systemów oraz nośników informacji służących do przetwarzania danych, tj. elementów określonych w § 5 pkt 8 powołanego rozporządzenia.

   Dyrektor Ośrodka wyjaśniła, że dokumentację tę przygotowano we własnym zakresie. Wskazała, że: *„Nie została uszczegółowiona zgodnie z wymogami zawartymi w § 4 i 5 rozporządzenia (...), ponieważ uznano, że dokumenty te powinny zawierać zasadnicze treści odnoszące się do ochrony danych osobowych i powinny być w zapisach czytelne i zrozumiałe dla pracowników MOPS, a nie bardzo uszczegółowione i skomplikowane".* Wskazała też, że: *„Aktualnie zostały podjęte działania w celu zlecenia tych zadań firmie zewnętrznej specjalizującej się w tym zakresie i działaniach ABI oraz zgromadzenia ofert w zakresie opracowania dokumentacji i funkcjonowania administratora bezpieczeństwa informacji".*

   ABI zatrudniony w Ośrodku, który zgodnie z art. 36a ust. 2 pkt 1b uodo jest odpowiedzialny m.in. za nadzorowanie opracowania i aktualizowania przedmiotowej dokumentacji wyjaśnił: *„Powodem takiego opracowania ww. dokumentów było przeświadczenie, aby były one zrozumiałe i czytelne dla wszystkich pracowników MOPS, którzy muszą je stosować w codziennej pracy".*

   (dowód: akta kontroli str. 37-39, 53-55, 170-175)

3. ABI nie wywiązał się z obowiązku określonego w art. 36a ust. 2 pkt 2 uodo i nie prowadził rejestru zbioru danych.

[15] Dz. U. Nr 100, poz. 1024. Rozporządzenie zwane dalej „rozporządzeniem MSWiA".

ABI wyjaśnił, że: *„Do dnia kontroli nie prowadziłem Rejestru zbiorów danych. Wszystkie zbiory danych osobowych w MOPS są zgłoszone do GIODO. Obecnie jestem w trakcie wykonywania takiego rejestru".* (dowód: akta kontroli str. 53-55, 170-175)

4. Regulacje składające się na politykę bezpieczeństwa informacji określoną w § 2 pkt 15 rozporządzenia KRI nie odpowiadały wszystkim wymogom § 20 ust. 1 tego rozporządzenia. W szczególności nie wskazano w nich, że przetwarzanie danych osobowych w systemie informatycznym MOPS, zgodnie z § 6 ust. 1 i 4 rozporządzenia MSWiA, wymaga wysokiego poziomu bezpieczeństwa.

   Dyrektor Ośrodka wyjaśniła, że: *„W Instrukcji zarządzania systemem informatycznym, służącym do przetwarzania danych osobowych nie określono poziomu bezpieczeństwa przetwarzania danych osobowych, o którym mowa w § 6 ww. rozporządzenia MSWiA, ponieważ zostało to przeoczone. Aktualnie zostały podjęte działania w celu zlecenia tych zadań firmie zewnętrznej specjalizującej się w tym zakresie i obowiązująca dokumentacja zostanie w najbliższym czasie uzupełniona bądź opracowana nowa".*

   ABI wyjaśnił natomiast, że: *„W dokumentacji przetwarzania danych osobowych wprowadzonej w MOPS nie ma zapisu, że przetwarzanie danych osobowych odbywa się na poziomie wysokim, ponieważ zostało to przeoczone. Na komputerach zastosowano programy antywirusowe i firewall systemowy, które są elementami wysokiego poziomu zabezpieczeń. MOPS planuje zakupić urządzenie typu UTM, które zapewni spełnienie wszystkich wymagań wysokiego poziomu zabezpieczeń. Jednocześnie podjęto działania mające na celu dostosowanie Polityki bezpieczeństwa do wymagań prawnych".*
   (dowód: akta kontroli str. 37-39, 53-55,170-175)

5. Ewidencja osób upoważnionych do przetwarzania danych w Ośrodku nie odpowiadała wymogom określonym w art. 39 ust. 1 pkt 2 uodo, gdyż nie wskazano w niej zakresu upoważnienia nadanego pracownikom. Ponadto prowadzono ją nierzetelnie, co opisano w pkt. 2.4 wystąpienia pokontrolnego.

   Dyrektor Ośrodka wyjaśniła, że: *„Ewidencja osób upoważnionych do przetwarzania danych w poszczególnych zbiorach nie zawiera w upoważnieniu zakresu przetwarzania danych, bowiem uważano, że wystarczy podanie samej nazwy zbioru. W aktualizacji z dnia 4 stycznia 2018 r. ujęto osoby upoważnione do przetwarzania danych osobowych w różnych zbiorach w wersji elektronicznej i tradycyjnej – papierowej".*
   (dowód: akta kontroli str. 24-31, 37-39)

6. Od 2 stycznia 2015 r. do 12 stycznia 2018 r. Dyrektor Ośrodka dopuściła ABI (ASI) do przetwarzania danych osobowych, pomimo że nie posiadał on upoważnienia do przetwarzania danych osobowych, co było sprzeczne z art. 37 uodo.

   Dyrektor wyjaśniła, że: *„Ze zleceniobiorcą, pełniącym zarazem funkcję ABI i ASI nie zawarto umowy w zakresie przetwarzania danych, zgodnie a art. 31 ust 1 ww. ustawy oraz nie nadano upoważnienia do przetwarzania danych, zgodnie z wymogiem art. 37 ww. ustawy z uwagi na przeoczenie tego faktu. Aktualnie, w dniu 12.01.2017 r. ABI i ASI został upoważniony do przetwarzania danych osobowych w 11 zbiorach funkcjonujących w MOPS w Zambrowie".* (dowód: akta kontroli str. 24-31, 35-49)

7. Pracownicy Ośrodka zaangażowani w proces przetwarzania informacji nie uczestniczyli w szkoleniach dotyczących zagadnień związanych z ochroną danych osobowych oraz bezpieczeństwem informacji. Obowiązek zapewnienia szkoleń takim osobom, z uwzględnieniem zagrożenia jej bezpieczeństwa, skutków naruszenia zasad bezpieczeństwa, konsekwencji prawnych i środków zapewniających jej bezpieczeństwo, ustalono w § 20 ust. 2 pkt 6 rozporządzenia KRI.

   Dyrektor Ośrodka wyjaśniła, że: *„Pracownicy, którym nadano upoważnienia do przetwarzania danych osobowych zostali poinstruowani z zakresu ochrony danych osobowych, natomiast nie odbyli szkoleń w tym zakresie. W budżecie MOPS w latach 2016 – 2017 nie było wystarczających środków na szkolenia. Aktualnie podjęte zostały działania w celu zwiększenia środków i przeszkolenia pracowników z zakresu ochrony danych osobowych w 2018 roku".*

   ABI, który zgodnie z art. 36a ust.2 pkt 1c uodo jest zobowiązany do zapewniania zapoznania osób upoważnionych do przetwarzania danych osobowych z przepisami

o ochronie danych osobowych wyjaśnił, że: *„Ze względu na specyfikę pracy w MOPS (praca w terenie, obsługa bieżąca petentów itp.) pracownicy nie odbyli zbiorowego szkolenia w zakresie ochrony danych osobowych. Natomiast pracownikom MOPS udzielono instruktażu i zaznajomiono z zasadami ochrony danych osobowych przy stanowiskach roboczych".* (dowód: akta kontroli str. 12-13, 37-39, 53-55, 150-153)

8. W okresie objętym kontrolą w MOPS nie przeprowadzano okresowych (nie rzadziej niż raz w roku) audytów wewnętrznych z zakresu bezpieczeństwa informacji, mimo wymogu wynikającego z § 20 ust. 2 pkt. 14 rozporządzenia KRI.

   Dyrektor Ośrodka wyjaśniła, że: *„W latach 2016 – 2017 nie było przeprowadzonego audytu wewnętrznego z zakresu bezpieczeństwa informacji (...), bowiem nikt z zatrudnionych w Ośrodku osób nie posiada kompetencji w tym względzie, a ponadto nie były planowane wydatki na ten cel. Aktualnie zostały podjęte działania w celu przeprowadzenia audytu wewnętrznego z zakresu bezpieczeństwa informacji oraz zgromadzenia ofert w tym zakresie".* (dowód: akta kontroli str. 12-13, 37-39)

9. Plany sprawdzeń zgodności przetwarzania danych osobowych z przepisami o ochronie danych osobowych nie odpowiadały formie i wymogom określonym w § 3 rozporządzenia w sprawie realizacji zadań ABI. Nie uwzględniono w nich bowiem m.in. zbiorów danych osobowych i systemów informatycznych służących do przetwarzania danych osobowych oraz konieczności weryfikacji zgodności przetwarzania danych osobowych z zasadami wyszczególnionymi w § 3 pkt 1 – 4 powołanego rozporządzenia. Ponadto w dokumentacji ze sprawdzenia, ABI wskazał, że: *„(...) W podmiocie są wszystkie wymagane dokumenty i są one sporządzone zgodnie z obowiązującymi przepisami prawa dotyczącymi ochrony danych osobowych".* Nieprawidłowość opisana w punkcie 2 wskazuje, że sprawozdanie było nierzetelne.

   ABI zatrudniony w Ośrodku wyjaśnił, że: *„W dokumencie tym zawarłem w formie tabelarycznej informacje określone w § 3 ust. 3 rozporządzenia Ministra Administracji i Cyfryzacji z dnia 11 maja 2015 r. (...)".* Ponadto wyjaśnił, że: *(...) W toku sprawdzenia zgodności przestrzegania zasad ochrony danych osobowych w Miejskim Ośrodku Pomocy Społecznej w Zambrowie stwierdziłem, że wymagane dokumenty są sporządzone zgodnie z przepisami prawa. Polityka bezpieczeństwa i Instrukcja zarządzania systemami informatycznymi nie zawiera wszystkich elementów wymienionych w § 4 i 5 rozporządzenia MSWiA, ponieważ została sporządzona w sposób ogólnikowy, bez stosowania specjalistycznych sformułowań, aby była przejrzysta i zrozumiała dla wszystkich pracowników Ośrodka".*
   (dowód: akta kontroli str. 53-55, 134-138, 323-324)

10. W dokumentacji Ośrodka nie określono zasad sprawowania kontroli nad tym, jakie dane osobowe, kiedy i przez kogo zostały do zbioru wprowadzone oraz komu są przekazywane, co jest sprzeczne z art. 38 uodo.

    Dyrektor Ośrodka wyjaśniła, że: *„W systemach informatycznych dane przetwarzają tylko pracownicy merytoryczni prowadzący postępowania, odpowiedzialni też za przetwarzanie danych w systemach informatycznych, którzy wykonują swoją pracę sumiennie, ponadto uważano, że wpisanie w zakresie czynności tych pracowników obsługi danego systemu informatycznego wystarczy".*
    (dowód: akta kontroli str. 11-13, 177)

Ocena cząstkowa

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

3. Sposób przechowywania oraz zabezpieczenia danych

Opis stanu faktycznego

3.1. W pkt 3 ppkt 2 PB określono, że administrator danych osobowych jest obowiązany zastosować środki techniczne i organizacyjne zapewniające ochronę przetwarzanych danych osobowych, a w szczególności powinien zabezpieczyć dane przed udostępnieniem osobom nieupoważnionym, zabraniem przez osobę nieuprawnioną, przetwarzaniem z naruszeniem ustawy oraz zmianą, utratą, uszkodzeniem lub zniszczeniem. Wskazano też, że bezpieczeństwo danym Ośrodka zapewnia: [1] umiejscowienie MOPS w budynku monitorowanym i dozorowanym, [2] przetwarzanie danych w pomieszczeniach zamykanych

oraz przechowywanie dokumentacji papierowej w szafach zamykanych, [3] wprowadzenie identyfikatorów i haseł dostępowych do systemów informatycznych, [4] zabezpieczenie komputerów aktualnym programem antywirusowym, [5]] zabezpieczenie komputerów przed zanikiem napięcia poprzez zainstalowanie UPS, [6] okresowe sporządzanie kopii bezpieczeństwa zbiorów danych i przechowywanie ich na nośnikach zewnętrznych.
(dowód: akta kontroli str. 170-175)

Oględziny wykazały, że: [1] Ośrodek umiejscowiony był na trzecim piętrze budynku biurowego, zajmowanym też przez Urząd Miejski w Zambrowie, Urząd Gminy Zambrów, Starostwo Powiatowe w Zambrowie i Powiatowy Urząd Pracy w Zambrowie, [2] korytarze budynku biurowego były monitorowane i dozorowane, [3] obszar biurowy MOPS nie był wydzielony jako oddzielna strefa użytkowania, [4] do dyspozycji Ośrodka wydzielono 14 pomieszczeń biurowych, [5] interesanci obsługiwani byli bezpośrednio w pomieszczeniach biurowych, [6] monitory ustawione były na biurkach w sposób uniemożliwiający zapoznanie się z treścią tam wyświetlaną, [7] dokumentacja papierowa przechowywana była w szafach zamykanych na klucz, [8] podczas nieobecności pracowników stosowano politykę „czystych biurek", [9] wszystkie pomieszczenia MOPS były zabezpieczone drzwiami zamykanymi na klucz, [10] w oknach pomieszczeń nie było zainstalowanych krat, rolet lub folii antywłamaniowej, [11] w pomieszczeniach Ośrodka nie było systemu przeciwpożarowego w postaci czujek dymowych, sygnalizatorów alarmowych, [12] pomieszczenie archiwum (umiejscowione na tym samym piętrze) nie posiadało systemu przeciwpożarowego oraz zabezpieczania drzwi, a część akt składowano szafach drewnianych i bezpośrednio na podłodze, co szerzej opisano w dalszej części wystąpienia pokontrolnego, w sekcji „Ustalone nieprawidłowości", [13] na wyposażeniu Ośrodka było osiem gaśnic proszkowych, [14] Ośrodek dysponował sejfem metalowym, w którym w dniu oględzin (12 stycznia 2018 r.) przechowywano 14 dysków wymontowanych z wycofanych komputerów oraz kasetę metalową, w której gromadzono płyty CD z kopiami baz danych, [15] spośród 32 stacjonarnych komputerów, 19 wyposażono w UPS. (dowód: akta kontroli str. 178-184)

ASI wyjaśnił, że: *„Ze względu na awarie zasilaczy UPS 11 komputerów stacjonarnych nie jest chronionych przed zanikiem napięcia. W miarę możliwości finansowych Ośrodka są dokonywane zakupy nowych zasilaczy"*. Dodał też, że: *„Dyski twarde z wycofanych komputerów są gromadzone w sejfie Ośrodka od 2012 roku"* oraz, że: *„Nie zostały one jeszcze zlikwidowane, ponieważ planowałem, gdy zbierze się ich większa ilość, zamówienie firmy, która specjalizuje się w niszczeniu dysków twardych, przy użyciu profesjonalnego sprzętu służącego do trwałego rozmagnesowania talerzy dyskowych, a następnie ich trwałym uszkodzeniu fizycznym"*. (dowód: akta kontroli str. 78, 313-314)

Ośrodek w okresie objętym kontrolą nie posiadał instrukcji określającej procedury postępowania z kluczami oraz zabezpieczeniami pomieszczeń. Dyrektor Ośrodka wyjaśniła, że: *„Zasady (polityka) dysponowania kluczami do pomieszczeń MOPS nie były opracowane, ale zasady takie były stosowane i dostęp do kluczy mieli tylko pracownicy MOPS. Interesanci w pokojach zawsze byli pod nadzorem pracowników, a klucze były niedostępne dla osób postronnych. Aktualnie* (18 stycznia 2018 r. – przyp. NIK) *została opracowana Instrukcja postępowania z kluczami do pomieszczeń MOPS w Zambrowie, zostały wydane pracownikom upoważnienia do pobierania kluczy, ponadto od pracowników odebrano stosowne oświadczenia dotyczące zachowania szczególnej dbałości w tym zakresie"*.
(dowód: akta kontroli str. 12-13, 206-217)

3.2. W okresie objętym kontrolą w Ośrodku nie prowadzono bieżącej inwentaryzacji zasobów informatycznych w celu ustalenia specyfikacji technicznej każdej ze stacji roboczych oraz zainstalowanych wersji oprogramowania. Takiego wymogu nie określono też w Instrukcji zarządzania systemem informatycznym, co opisano w dalszej części wystąpienia pokontrolnego, w sekcji „Ustalone nieprawidłowości".
(dowód: akta kontroli str. 12-13)

3.3. W okresie objętym kontrolą podmioty zewnętrzne nie dokonywały napraw sprzętu będącego nośnikiem zasobów informacyjnych MOPS. Stwierdzone awarie usuwane były przez ASI. W latach 2016 – 2017 zlikwidowano cztery komputery, które poddano utylizacji,

po usunięciu z nich dysków twardych. W trakcie oględzin ustalono, że 14 dysków twardych wymontowanych ze zlikwidowanych komputerów od 2012 roku przechowywano w sejfie Ośrodka. (dowód: akta kontroli str. 178-183, 185-197, 313-314)

3.4. W MOPS stosowana była polityka „czystych biurek", zgodnie z którą dane osobowe w wersji papierowej zabezpieczane były przed kradzieżą lub wglądem osób nieupoważnionych w zamykanych szafach. Do niszczenie dokumentów papierowych w Ośrodku wykorzystywano siedem niszczarek mechanicznych.
(dowód: akta kontroli str. 12-13, 178-183)

3.5. W PB oraz Instrukcji zarządzania systemem informatycznym nie określono zasad korzystania ze służbowych urządzeń informatycznych poza siedzibą jednostki, chociaż Ośrodek od 23 grudnia 2013 r. dysponował dwoma terminalami mobilnymi do przeprowadzania wywiadów środowiskowych (problem opisano też w dalszej części wystąpienia, w sekcji „Ustalone nieprawidłowości"). Urządzenia te w sierpniu 2014 roku przekazano dwóm pracownicom MOPS. Osoba dysponująca tym urządzeniem wyjaśniła, że wykorzystywała je sporadycznie (pięć lub sześć razy). (dowód: akta kontroli str. 199-203)

3.6. Sprzątaniem pomieszczeń MOPS zajmowała się pracownica Ośrodka zatrudniona w pełnym wymiarze czasu pracy. Odbywało się ono w godzinach pracy Ośrodka i w obecności pracowników jednostki. Osoba ta była też upoważniona do danych przetwarzanych w zbiorze „Ewidencja klientów Ośrodka Pomocy Społecznej w Zambrowie", prowadzonym w formie papierowej (doręczała decyzje i korespondencję Ośrodka).
(dowód: akta kontroli str. 12-13)

3.7. Do dnia kontroli w Ośrodku nie opracowano procedury, przeglądów i konserwacji systemów oraz nośników informacji służących do przetwarzania danych, co opisano w dalszej części wystąpienia, w sekcji „Ustalone nieprawidłowości".

ASI wyjaśnił, że: *„W latach 2016 – 2017 były przeprowadzane okazjonalnie przeglądy komputerów, polegające między innymi na sprawdzeniu dysków twardych, przeskanowania systemów programem antywirusowym. Nie prowadzono dokumentacji w tym zakresie".*
(dowód: akta kontroli str. 12-13, 78)

3.8. MOPS nie posiada wewnętrznych regulacji opisujących działania, jakie należy podjąć w sytuacji wystąpienia zdarzeń nadzwyczajnych, np. awarii serwera, sieci, awarii systemów zaatakowanych wirusem, długotrwałego braku zasilania. Nie opracowano też procedur przywracania sprawności tych systemów oraz planu ciągłości działania umożliwiającego kontynuację wykonywania zadań publicznych, co szerzej opisano w dalszej części wystąpienia pokontrolnego, w sekcji „Uwagi dotyczące badanej działalności".
(dowód: akta kontroli str. 12-13)

3.9. Dyrektor Ośrodka wyjaśniła, że w latach 2016 – 2017 nie wystąpiły przypadki fizycznej utraty danych, będące wynikiem kradzieży nośnika, przekazania go nieuprawnionej osobie, przypadkowego skasowania lub zniszczenia danych w rezultacie wystąpienia sytuacji nadzwyczajnych (pożar, zalanie). (dowód: akta kontroli str. 53-55)

Ustalone nieprawidłowości

W działalności kontrolowanej jednostki w przedstawionym zakresie stwierdzono następujące nieprawidłowości:

1. W Ośrodku nie prowadzono bieżącej inwentaryzacji sprzętu i oprogramowania służącego do przetwarzania informacji, w tym obejmującej ich rodzaj i konfigurację. Obowiązek gromadzenia takich danych wynika § 20 ust. 2 pkt 2 rozporządzenia KRI. Zgodnie z powołanym przepisem kierownik jednostki powinien zapewnić utrzymywanie aktualności inwentaryzacji sprzętu i oprogramowania, służącego do przetwarzania informacji obejmującej ich rodzaj oraz konfigurację, co ma umożliwić szybkie odtworzenie informatycznego środowiska pracy po nagłym zdarzeniu losowym (np. pożar, zalanie).

   Dyrektor Ośrodka wyjaśniła, że: *„W MOPS nie przeprowadzono inwentaryzacji zasobów informatycznych w celu ustalenia specyfikacji technicznej każdej ze stacji roboczych oraz zainstalowanych wersji oprogramowania, ponieważ uważano, że wystarczy sporządzana inwentaryzacja roczna na dzień 31 grudnia każdego roku. W związku*

z niniejszą kontrolą sporządzono specyfikację techniczną każdej ze stacji roboczej i zainstalowanych w nich wersji oprogramowania na arkuszach Konfiguracja komputera".
(dowód: akta kontroli str. 12-13, 206-207, 218-252)

2. Ośrodek pomimo, że od grudnia 2013 roku dysponował dwoma terminalami mobilnymi do dokumentowania wywiadów środowiskowych, nie określił podstawowych zasad gwarantujących bezpieczną pracę przy przetwarzaniu mobilnym i pracy na odległość. Obowiązek ustalenia takich zasad wynika z § 20 ust. 2 pkt 8 rozporządzenia KRI.

   Dyrektor Ośrodka wyjaśniła, że: *„(...) zostało to przeoczone. Aktualnie zostały podjęte działania w celu aktualizacji bądź stworzenia nowej dokumentacji, w której zostaną też uregulowane te kwestie (...). Terminale mobilne wykorzystywane były sporadycznie, w związku z tym nieefektywnie. Sprawne wykorzystywanie terminali w pracy pracownika socjalnego w terenie utrudnia zbyt mały ekran uniemożliwiający sprawne nanoszenie danych. Ponadto korzystanie z terminali w terenie naraża na utratę danych i sprzętu, jego zniszczenie ze strony agresywnych klientów".*
   (dowód: akta kontroli str. 199-203, 206-207)

3. Pomieszczenie archiwum nie odpowiadało wymogom określonym w rozdziale 3 załącznika nr 6 do rozporządzenia w sprawie działania archiwów zakładowych[16]. Nie posiadało bowiem systemu przeciwpożarowego, drzwi nie były odpowiednio zabezpieczone, a część dokumentacji archiwalnej składowana była bezpośrednio na podłodze. Ponadto znajdowały się tam dwa komputery pełniące funkcję serwerów Ośrodka, co było niezgodne z § 8 ust. 3 pkt 1 Instrukcji archiwalnej, stanowiącej załącznik nr 6 do ww. rozporządzenia. Taki stan nie zapewnia właściwej ochrony papierowych zbiorów danych przed działaniem czynników fizycznych i zdarzeń losowych (pożar, kradzież).

   Dyrektor Ośrodka wyjaśniła, że: *„Pomieszczenie Składnicy akt (archiwum) nie odpowiada wymogom określonym w rozdziale 3 załącznika nr 6 do rozporządzenia w sprawie działania archiwów zakładowych, ponieważ tylko takim pomieszczeniem dysponuje MOPS i nie ma możliwości pozyskania w budynku dodatkowego pomieszczenia. Dotychczas MOPS nie dysponował budżetem, który pozwoliłby na dostosowanie pomieszczenia do wymogów określonych w ww. załączniku. Pomieszczenie posiada wentylację grawitacyjną, nie jest narażone na działanie promieni słonecznych, posiada oświetlenie zapewniającą odpowiednia widoczność. Aktualnie została zainstalowana w pomieszczeniu czujka dymu, podjęto działania w celu zakupienia regałów na dokumenty, wzmocnienia drzwi i zainstalowania dodatkowego zamka".*
   (dowód: akta kontroli str. 206-207)

Uwagi dotyczące badanej działalności

Najwyższa Izba Kontroli zwraca uwagę, że niezbędne jest opracowanie wewnętrznych regulacji dotyczących rozwiązań na wypadek wystąpienia sytuacji nadzwyczajnych, np. długotrwałego braku zasilania bądź przywracania systemów po awarii, a także planu ciągłości działania, umożliwiającego kontynuację wykonywania zadań jednostki. Plan ten powinien określić systemy i aplikacje o znaczeniu krytycznym oraz wszystkie podporządkowane lub powiązane plany. Istotne jest, aby plany te były jasno udokumentowane, przekazane pracownikom i aktualizowane w celu odzwierciedlenia bieżącej działalności 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 cz. A pkt. III załącznika do rozporządzenia MSWiA.

Dyrektor Ośrodka wyjaśniła, że: *„Nie opracowano wewnętrznych regulacji opisujących działania, jakie należy podjąć w sytuacji wystąpienia zdarzeń nadzwyczajnych (...), ponieważ kwestie te zostały przeoczone. Aktualnie zostały podjęte działania w celu stworzenia dokumentacji, w której zostaną też uregulowane te kwestie".*
(dowód: akta kontroli str. 178-184, 206-207)

[16] 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.).

Ocena cząstkowa

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

4. Przetwarzanie zasobów informacyjnych zgodnych z zakresem działalności jednostki kontrolowanej

Opis stanu faktycznego

4.1. W okresie objętym kontrolą Ośrodek dysponował 11 zbiorami danych osobowych, spośród których dziewięć prowadzono z wykorzystaniem pięciu dziedzinowych systemów informatycznych:

- TT-POMOC – do wprowadzania wniosków w sprawach dotyczących pomocy społecznej, wprowadzania rodzinnych wywiadów środowiskowych, wydawania decyzji w sprawach przyznania świadczeń z pomocy społecznej (zasiłek celowy, okresowy, stały, świadczenie pieniężnie na zakup żywności lub posiłku, obiady dla dzieci, usługi opiekuńcze, skierowanie do domu pomocy społecznej, przyznanie schronienia), sporządzania list wypłat świadczeń, sporządzania sprawozdań resortowych kwartalnych, półrocznych i rocznych oraz zbiorów centralnych,
- SW „Świadczenia wychowawcze" – do ewidencjonowania spraw związanych z przyznaniem i wypłatą świadczeń wychowawczych,
- FA „Fundusz Alimentacyjny" – do ewidencjonowania zdarzeń związanych przyznaniem i wypłatą świadczeń alimentacyjnych oraz rozliczeniem zaległości dłużników alimentacyjnych,
- SR „Świadczenia rodzinne" – do przyznania i wypłaty świadczeń rodzinnych wraz z dodatkami, zasiłku dla opiekuna i świadczeń za życiem,
- CHEOPS – do ewidencjonowania dodatków mieszkaniowych oraz wypłaconych ryczałtów energetycznych.

Ponadto Ośrodek korzystał z systemu „Płace i Budżet" (do prowadzenia pełnej obsługi księgowości oraz spraw kadrowo-płacowych) oraz z systemu informatycznego „PŁATNIK' do zgłaszania i wyrejestrowania osób z ubezpieczenia zdrowotnego i społecznego.
(dowód: akta kontroli str. 67-76, 315)

4.2. Zakres gromadzonych i przetwarzanych w Ośrodku danych osobowych był niezbędny do realizacji zadań wynikających m.in. z ustawy z dnia 12 marca 2004 r. o pomocy społecznej, ustawy z dnia 7 września 2007 r. o pomocy osobom uprawnionym do alimentów[17] ustawy z dnia 11 lutego 2016 r. o pomocy państwa w wychowywaniu dzieci[18], ustawy z dnia 29 lipca 2005 r. o przeciwdziałaniu przemocy w rodzinie[19] oraz z rozporządzeń wykonawczych.

Analiza wszystkich sześciu zbiorów danych osobowych zarejestrowanych przez GIODO wykazała, że w jednym przypadku[20] zakres faktycznie przetwarzanych danych osobowych odpowiadał zgłoszeniu. W pięciu pozostałych był on szerszy niż ujęty w rejestrze GIODO, co szerzej opisano w dalszej części wystąpienia pokontrolnego, w sekcji „Ustalone nieprawidłowości" (dowód: akta kontroli str. 255-258, 329-330)

W okresie objętym w MOPS prowadzono trzy postępowania dotyczące naboru kandydatów do pracy na stanowiskach urzędniczych Ośrodka. W ogłoszeniu wskazano informacje wymagane art. 24 ust. 1 uodo. Każda osoba biorąca udział w naborze oraz zatrudniona w MOPS złożyła wymagane oświadczenia, w których wyraziła zgodę na przetwarzanie jej danych osobowych. (dowód: akta kontroli str. 302-310)

4.3. W latach 2016 – 2017 Ośrodek korzystał też ze zbiorów danych osobowych, których administratorami są podmioty zewnętrzne, w tym z Samorządowej Elektronicznej Platformy Informatycznej SEPI (aktualizowanej przez Powiatowy Urząd Pracy w Zambrowie). W ramach projektu Emp@tia realizowanego przez Ministerstwo Pracy i Polityki Socjalnej; Ośrodek uzyskał też dostęp do Centralnego Systemu Informacji Zabezpieczenia Społecznego, w tym z możliwości pobierania danych z systemów zewnętrznych: PESEL,

[17] Dz. U. z 2017 r. poz. 489, ze zm.
[18] Dz. U. z 2017 r. poz. 1851, ze zm.
[19] Dz. U. z 2015 r. poz. 1390.
[20] „Dodatki mieszkaniowe".

e-Podatki[21], ZUS, AC Rynek Pracy[22], EKSMOoN[23], NFZ-CWU[24], CEIDG[25], CBB[26], CAS[27]. Za pomocą Portalu Informacyjno-Usługowego może też odbierać wnioski elektroniczne składane przez wnioskodawców. (dowód: akta kontroli str. 56-60, 311-312)

Ustalone nieprawidłowości

W działalności kontrolowanej jednostki w przedstawionym wyżej zakresie stwierdzono nieprawidłowość, polegającą na niezaktualizowaniu zgłoszonego GIODO zakresu przewarzania danych w pięciu[28] (z sześciu) zarejestrowanych zbiorach, co stanowiło naruszenie art. 41 ust. 2 i ust. 3 uodo. Przetwarzane przez pracowników Ośrodka dane obejmowały (oprócz danych zgłoszonych do rejestracji) także: nazwisko panieńskie matki, płeć, imiona rodziców, narodowość i status uchodźcy. Zgodnie z art. 41 ust. 2 i ust. 3 uodo, zmiana w zbiorze danych powinna być zgłoszona w terminie 30 dni od dnia jej dokonania, a w przypadku danych wrażliwych – przed dokonaniem zmiany w zbiorze.

Z wyjaśnień Dyrektora Ośrodka wynika, że niezaktualizowanie zgłoszeń GIODO wynikało z przeoczenia. (dowód: akta kontroli str. 177, 255-258, 329-330)

Ocena cząstkowa

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

IV.Wnioski

Wnioski pokontrolne

Przedstawiając powyższe oceny i uwagi wynikające z ustaleń kontroli, Najwyższa Izba Kontroli, na podstawie art. 53 ust. 1 pkt 5 ustawy z dnia 23 grudnia 1994 r. o Najwyższej Izbie Kontroli[29], wnosi o:

1. Przeprowadzanie okresowej analizy ryzyka utraty integralności, dostępności lub poufności informacji oraz – nie rzadziej niż raz w roku – okresowego audytu bezpieczeństwa informacji, stosownie do § 20 ust. 2 pkt 3 i 14 rozporządzenia KRI.
2. Zapewnienie skutecznego monitorowania dostępu do zasobów informacyjnych, wymaganego § 20 ust. 2 pkt 7 lit. a) rozporządzenia KRI.
3. Nadawanie pracownikom uprawnień do systemów operacyjnych komputerów w stopniu adekwatnym do realizowanych przez nich zadań, stosownie do § 20 ust. 2 pkt 4 rozporządzenia KRI.
4. Uzupełnienie PB i Instrukcji zarządzania systemem informatycznym służącym do przetwarzania danych osobowych zgodnie z wymogami § 20 ust. 1 rozporządzenia KRI oraz § 4 i 5 rozporządzenia MSWiA.
5. Prowadzenie przez ABI rejestru zbiorów danych osobowych przetwarzanych w Ośrodku, stosownie do art. 36a ust. 2 pkt 2 uodo, oraz – rzetelnej i zgodnej z art. 39 ust. 1 pkt 2 powołanej ustawy – ewidencji osób upoważnionych do przetwarzania danych osobowych.
6. Zapewnienie wszystkim pracownikom zaangażowanym w proces przetwarzania informacji w Ośrodku szkoleń, o których mowa w § 20 ust. 2 pkt 6 rozporządzenia KRI.
7. Rzetelne sporządzanie przez ABI dokumentacji ze sprawdzeń zgodności przetwarzania danych osobowych z przepisami o ochronie danych osobowych oraz przygotowanie planów tych sprawdzeń zgodnie z § 3 rozporządzenia w sprawie realizacji zadań ABI.

---

[21] Portal podatkowy.
[22] Aplikacja Centralna Rynek Pracy.
[23] Elektroniczny Krajowy System Orzekania o Niepełnosprawności.
[24] Narodowy Fundusz Zdrowia Centralny Wykaz Ubezpieczonych.
[25] Centralna Ewidencja i Informacja o Działalności Gospodarczej.
[26] Centralna Baza Beneficjentów.
[27] Centralna Aplikacja Statystyczna.
[28] „Ewidencja Klientów Ośrodka Pomocy Społecznej w Zambrowie", „Przemoc w Rodzinie", „Świadczenia alimentacyjne i dłużnicy alimentacyjni, „Świadczenia Rodzinne", „Przeciwdziałanie alkoholizmowi".
[29] Dz. U. z 2017 r. poz. 524. Ustawa zwana dalej „ustawą o NIK".

8. Określenie zasad kontroli nad tym, jakie dane osobowe, kiedy i przez kogo zostały do zbiorów danych osobowych wprowadzone oraz komu były przekazywane, stosownie do art. 38 uodo.
9. Prowadzenie aktualnego rejestru zasobów informatycznych, zgodnie z wymogami określonymi w § 20 ust. 2 pkt 2 rozporządzenia KRI.
10. Określenie podstawowych zasad gwarantujących bezpieczną pracę przy przetwarzaniu mobilnym i pracy na odległość, wymaganych § 20 ust. 2 pkt 8 rozporządzenia KRI.
11. Zapewnienie właściwej ochrony papierowym zbiorom danych znajdujących się w archiwum Ośrodka przed działaniem czynników fizycznych i zdarzeń losowych.
12. Zgłoszenie GIODO zmian danych rejestracyjnych pięciu zbiorów danych osobowych.

V. Pozostałe informacje i pouczenia

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

Prawo zgłoszenia zastrzeżeń

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.

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 19 lutego 2018 r.

Kontroler
Marek Zapolski
doradca ekonomiczny

.....
podpis

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

.....
podpis