NAJWYŻSZA IZBA KONTROLI
Delegatura w Białymstoku

LBI.410.023.23.2017
P/17/062

00373618

WYSTĄPIENIE POKONTROLNE

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

I. Dane identyfikacyjne kontroli

Numer i tytuł kontroli

P/17/062 – Bezpieczeństwo elektronicznych zasobów informacyjnych w jednostkach samorządu terytorialnego w województwie podlaskim

Jednostka przeprowadzająca kontrolę

Najwyższa Izba Kontroli Delegatura w Białymstoku

Kontrolerzy

Joanna Muszyńska – specjalista kontroli państwowej, upoważnienie do kontroli nr LBI/4/2018 z 2 stycznia 2018 r. (dowód: akta kontroli str. 1-2)

Jednostka kontrolowana

Miejsko-Gminny Ośrodek Pomocy Społecznej w Suchowoli, Plac Kościuszki 5, 16-150 Suchowola (dalej: „MGOPS" lub „Ośrodek")

Kierownik jednostki kontrolowanej

Barbara Pikus – Kierownik Miejsko-Gminnego Ośrodka Pomocy Społecznej w Suchowoli[1] (dowód: akta kontroli str. 3)

Ocena ogólna

II. Ocena kontrolowanej działalności[2]

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

Uzasadnienie oceny ogólnej

Stwierdzono bowiem nieprawidłowości polegające w szczególności na:

- nadaniu użytkownikom wszystkich komputerów Ośrodka uprawnień administratora systemu operacyjnego,
- nieprzestrzeganiu przyjętych zasad i procedur dotyczących tworzenia i przechowywania kopii zapasowych baz danych,
- niezapewnieniu właściwego poziomu zabezpieczeń odpowiedzialnych za autoryzację dostępu systemów operacyjnych komputerów Ośrodka,
- nieanalizowaniu i niezabezpieczeniu przed modyfikacją lub zniszczeniem logów systemów operacyjnych komputerów wykorzystywanych w MGOPS,
- umożliwieniu zdalnego dostępu do zasobów firmie serwisującej składniki systemu bez konieczności autoryzacji i bez nadzoru administratora systemu,
- użytkowaniu konta pocztowego, które nie gwarantowało właściwego zabezpieczenia informacji przed jej ujawnieniem nieuprawnionej osobie, modyfikacją, usunięciem lub zniszczeniem,
- niezgłoszeniu do zarejestrowania Generalnemu Inspektorowi Ochrony Danych Osobowych[4] pięciu przetwarzanych w MGOPS zbiorów danych oraz niezaktualizowaniu zakresu przetwarzanych danych w zbiorze już zarejestrowanym,
- nienadaniu dwóm osobom upoważnień do przetwarzania danych osobowych w zbiorze, do którego miały one dostęp,
- niewykonywaniu przeglądów technicznych sprzętu informatycznego, wymaganych regulacjami wewnętrznymi Ośrodka,
- niewywiązaniu się z obowiązków, dotyczących utrzymywania aktualności inwentaryzacji sprzętu i oprogramowania służącego do przetwarzania informacji obejmujących ich rodzaj i konfigurację oraz przeprowadzania corocznych audytów wewnętrznych z zakresu bezpieczeństwa informacji.

---

[1] Pełniąca funkcję Kierownika Miejsko-Gminnego Ośrodka Pomocy Społecznej od 30 grudnia 2017 roku. Wcześniej funkcję tę pełniła Honorata Świderska w okresie od 1 stycznia 1991 r. do 29 grudnia 2017 r.

[2] Najwyższa Izba Kontroli stosuje 3-stopniową skalę ocen: pozytywna, pozytywna mimo stwierdzonych nieprawidłowości, negatywna.

[3] Kontrolą objęty został okres od 1 stycznia 2016 r. do zakończenia czynności kontrolnych.

[4] Dalej: „GIODO".

III. Opis ustalonego stanu faktycznego

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

Opis stanu faktycznego

1.1. W MGOPS informacje gromadzono i przetwarzano w formie papierowej oraz wykorzystywano do tego sześć aplikacji dziedzinowych, tj. „Helios", „Cheops", „Nemezis", „Amazis", „Izyda", „KDR" oraz programy do obsługi finansowo-księgowej, tj. „Księgowość budżetowa", „Kadry i Płace", „Przelewy", "Płatnik", „Homebanking", „Rejestr VAT".

Dane osobowe w Ośrodku przetwarzane były przez dziesięciu pracowników na ośmiu komputerach (w tym jednym terminalu stacjonarnym) posiadających dostęp do Internetu.
(dowód: akta kontroli str. 55-56, 147-151)

Oględziny wszystkich komputerów MGOPS wykorzystywanych do przetwarzania danych osobowych wykazały m.in., że: [1] wszyscy użytkownicy posiadali uprawnienia administratora systemu operacyjnego; [2] dostęp do systemu operacyjnego (na siedmiu z ośmiu komputerów) realizowany był na domyślnym loginie „user" lub „Pracownik" i we wszystkich przypadkach zabezpieczony był hasłem; [3] na wszystkich komputerach zastosowano wygaszacz ekranu uaktywniający się po 10 minutach bezczynności użytkownika[5] oraz program antywirusowy, który posiadał aktualną bazę wirusów; [4] na wszystkich komputerach zainstalowano systemy operacyjne Windows, które były aktualizowane automatycznie, zgodnie z ustalonym harmonogramem. Szerzej problem nadanych pracownikom MGOPS uprawnień oraz dostępu do systemów operacyjnych opisano w dalszej części wystąpienia pokontrolnego, w sekcji *„Ustalone nieprawidłowości"*.
(dowód: akta kontroli str. 152-163)

1.2. W MGOPS do 21 sierpnia 2016 r. nie przeprowadzono okresowej analizy poufności, integralności i rozliczalności systemów informatycznych pod kątem zagrożeń i ryzyka, o której mowa w § 20 ust. 2 pkt 3 rozporządzenia KRI, mimo że taki obowiązek istniał od 31 maja 2012 r. Wprawdzie 22 sierpnia 2016 r. wprowadzono dokument o nazwie „Analiza zagrożeń i ryzyka przy przetwarzaniu danych osobowych"[6], w którym wskazano m.in. podstawowe zagrożenia dla systemu tj. utrata poufności, integralności i rozliczalności. zidentyfikowano największe zagrożenia (m.in. atak wirusa, brak mechanizmów uniemożliwiających skasowanie lub zmianę logów przez administratora lub innego użytkownika, pożar lub nieuprawniony dostęp do komputera czy pomieszczenia, niewłaściwe administrowanie systemem informatycznym, pomyłki użytkowników, zanik zasilania) jednak dokument był niekompletny, co szerzej opisano w sekcji „Ustalone nieprawidłowości". (dowód: akta kontroli str. 89-100)

1.3. Wszyscy pracownicy przetwarzający dane osobowe byli zaangażowani w proces przetwarzania tych danych w stopniu adekwatnym do zadań, jakie wynikały z ich zakresów obowiązków[7]. Niemniej jednak wszyscy posiadali uprawnienia administratora systemu operacyjnego w wykorzystywanych przez nich komputerach. Ponadto hasła dostępu do komputerów nie spełniały wymagań – określonych w § 2 pkt.II.1 oraz § 2 pkt. IV.2 Instrukcji zarządzania systemem informatycznym, która obowiązywała w MGOPS[8] oraz w załączniku do rozporządzenia Ministra Spraw Wewnętrznych i Administracji z dnia 29 kwietnia 2004 r. w sprawie dokumentacji przetwarzania danych osobowych oraz warunków technicznych i organizacyjnych, jakim powinny odpowiadać urządzenia i systemy informatyczne do przetwarzania danych osobowych – dla wysokiego poziomu bezpieczeństwa[9]. Szerzej problem ten opisano w dalszej części wystąpienia pokontrolnego, w sekcji „Ustalone nieprawidłowości". (dowód: akta kontroli str. 84-88, 145, 150-163)

---

[5] Powrót do systemu wymagał podania hasła użytkownika.
[6] Zarządzenie nr 6/2016 Kierownika Miejsko-Gminnego Ośrodka Pomocy Społecznej w Suchowoli z dnia 22 sierpnia 2016 r. w sprawie wdrożenia dokumentu o nazwie „Analiza zagrożeń i ryzyka przy przetwarzaniu danych osobowych".
[7] W latach 2016 – 2017 dwóm pracownikom odebrano uprawnienia, dwóm zatrudnionym osobom nadano uprawnienia, a jednej osobie rozszerzono uprawnienia stosownie do zaistniałych okoliczności.
[8] Wprowadzona zarządzeniem nr 5 /2016 Kierownika Miejsko-Gminnego Ośrodka Pomocy Społecznej w Suchowoli z dnia 22 sierpnia 2016 r. Zwana dalej „Instrukcją".
[9] Dz. U. Nr 100, poz. 1024. Rozporządzenie dalej zwane „rozporządzeniem w sprawie dokumentacji i warunków technicznych".

1.4. W MGOPS nie prowadzono zbiorczego rejestru dostępu do systemu operacyjnego ani w formie papierowej, ani elektronicznej (np. w postaci logów systemowych). Każdy z komputerów Ośrodka generował i przechowywał logi systemowe zgodnie z domyślnymi ustawieniami. Infrastruktura sieci informatycznej nie pozwalała na skuteczne monitorowanie dostępu do informacji gromadzonych w systemach informatycznych, co szerzej opisano w dalszej części wystąpienia pokontrolnego, w sekcji „Ustalone nieprawidłowości".

(dowód: akta kontroli str. 18-21, 152-163)

1.5. Środkiem zabezpieczającym przed nieautoryzowanym dostępem do wszystkich systemów operacyjnych komputerów było hasło użytkownika. Nie aktywowano mechanizmu wymuszenia okresowej jego zmiany. Aplikacje dziedzinowe wykorzystywane w MGOPS miały aktywny mechanizm wymuszania zmiany hasła co 30 dni, a użytkownicy pracowali bez uprawnień administratora tych aplikacji. Ośrodek nie posiadał serwerowni i nie funkcjonowała w nim sieć Wi-Fi. Natomiast wprowadzone środki techniczne, mające na celu zabezpieczenie dostępu do systemów operacyjnych, były niewystarczające, co opisano w dalszej części wystąpienia pokontrolnego, w sekcji „Ustalone nieprawidłowości".

(dowód: akta kontroli str. 18-21,152-163)

1.6. W procedurach wewnętrznych dotyczących ochrony danych osobowych nie uregulowano kwestii związanych z wykorzystaniem do pracy sprzętu niebędącego własnością Urzędu. Na stanowiskach pracy poddanych oględzinom nie stwierdzono prywatnych urządzań informatycznych podłączonych do sieci MGOPS lub wykorzystywanych przez pracowników do wykonywania obowiązków służbowych.

(dowód: akta kontroli str. 164-166)

Konfiguracja sieciowa umożliwiała podłączenie do infrastruktury Urzędu sprzętu (np. laptopów, telefonów, tabletów lub dysków przenośnych) niestanowiącego własności pracodawcy, jednak nie było możliwe korzystanie z zasobów sieci informatycznej Ośrodka za ich pomocą. Informacje o podłączeniu do komputerów nośników pamięci były domyślnie zapisywane w logach systemu komputerowego, jednak nie były trwale zabezpieczane. Na jednym komputerze zainstalowano aplikację pulpitu zdalnego TeamViewer, z której korzystali pracownicy firmy zewnętrznej podczas realizacji prac serwisowych. Dostęp ten nie był objęty kontrolą administratora systemów informatycznych[10]. Przy połączeniu korzystano z autoryzacji Głównej Księgowej. Problemy te opisano szerzej w dalszej części wystąpienia pokontrolnego, w sekcji „Ustalone nieprawidłowości".

(dowód: akta kontroli str. 18-21, 152-163)

1.7. Od 1 stycznia 2016 r. do 31 grudnia 2017 r. nie wystąpiły przypadki wykrycia nieautoryzowanych działań związanych z przetwarzaniem informacji.

(dowód: akta kontroli str. 172-174, 215-222)

1.8. W MGOPS nie wykonywano obowiązków służbowych z wykorzystaniem mobilnego przetwarzania danych, w tym pracy na odległość. W terenie nie wykorzystywano dwóch mobilnych terminali przeznaczonych do przeprowadzania wywiadów środowiskowych. Były one wykorzystywane testowo[11] wyłącznie w siedzibie Ośrodka. Dostęp do ich systemów operacyjnych i programu dziedzinowego[12] był zabezpieczony hasłem zgodnym z restrykcjami określonymi § 2 pkt IV.2 Instrukcji oraz w cz. A pkt IV ust. 2 załącznika do rozporządzenia w sprawie dokumentacji i warunków technicznych dla wysokiego poziomu zabezpieczeń. Kierownik MGOPS poinformowała, że: *„Sprzęt mobilny typu laptop (tzw. terminale mobilne) otrzymany w 2013 roku w ramach realizacji programu Emp@tia miał być wykorzystywany do przeprowadzania wywiadów środowiskowych, jednak nie było podstawy prawnej do ich przeprowadzania."*

Biegły stwierdził, że w badanej jednostce nie przewidziano zdalnego dostępu do zasobów sieci lokalnej i taki dostęp nie funkcjonował.

(dowód: akta kontroli str. 18-21, 152-163, 172-174,215-222)

---

[10] W MGOPS nie było osoby zatrudnionej do pełnienia tej funkcji.
[11] Od czerwca 2017 r.
[12] Kalipso – moduł systemu do „Helios".

1.9. W latach 2016 – 2017 MGOPS zawierał roczne umowy licencyjne dla programów dziedzinowych obejmujące m.in. aktualizacje wynikające z potrzeb Ośrodka oraz związane z nowelizacją przepisów prawnych. Nie zawarto w nich regulacji zobowiązujących dostawcę programu do zachowania w tajemnicy i nieudostępniania danych osobowych przekazanych przez MGOPS. (dowód: akta kontroli str. 118-127,131, 172-174,215-222)

W okresie objętym kontrolą Ośrodek zawarł dwie umowy serwisowe (na serwis oprogramowania i udostępnianie nowych wersji) dotyczące programów: „Budżet", „Kadry i Płace" oraz systemu HOMME Banking. W obu zawarto zapisy gwarantujące odpowiedni poziom bezpieczeństwa informacji, zgodnie z § 20 ust. 2 pkt 10 rozporządzenia KRI. Obejmowały one w szczególności zobowiązanie podmiotów zewnętrznych do: [1] przetwarzania danych osobowych wyłącznie w celu oraz w zakresie związanym z realizacją zawartych umów; [2] zastosowania środków technicznych i organizacyjnych zapewniających ochronę danych, co najmniej w zakresie określonym w art. 36 – 39a ustawy o ochronie danych osobowych; [3] zachowania w tajemnicy informacji uzyskanych w trakcie realizacji umów. W okresie objętym kontrolą MGOPS nie zawierał z podmiotami zewnętrznymi umów na serwis urządzeń komputerowych.

(dowód: akta kontroli str. 101-131)

1.10. Wszystkie osiem komputerów, wchodzących w skład sieci lokalnej, było zabezpieczonych przed działaniem oprogramowania, którego celem byłoby uzyskanie nieuprawnionego dostępu do systemu informatycznego. Zabezpieczenia dokonano dedykowanym do tego celu oprogramowaniem antywirusowym[13]. Dostęp do sieci lokalnej kontrolowany był przez mało skuteczny firewall programowy[14], co opisano szerzej w dalszej części wystąpienia pokontrolnego, w sekcji „Ustalone nieprawidłowości".

(dowód: akta kontroli str. 18-21,152-163)

1.11. W latach 2016 – 2017 r. Ośrodek nie zawierał umów dotyczących świadczenia usług poczty elektronicznej. Stanowisko komputerowe Głównej Księgowej MGOPS posiadało dostęp do dwóch skrzynek email Ośrodka[15]. Głowna skrzynka[16] była skonfigurowana na domenie pocztowej udostępnionej przez Urząd Miasta Suchowola, który jest stroną umowy z dostawcą usług pocztowych, gwarantującym poufność świadczonych usług. Drugie konto poczty elektronicznej hostingowane było bezpłatnie w serwisie operatora komercyjnego, co szerzej opisano w dalszej części wystąpienia pokontrolnego, w sekcji „Ustalone nieprawidłowości". (dowód: akta kontroli str. 132-136, 152-163, 172-174)

1.12. Sposób wykonywania kopii zbiorów danych (nie rzadziej niż raz na tydzień) oraz miejsce ich przechowywania (w pokoju nr 12 w kasie pancernej) określone zostały w obowiązującej w MGOPS Instrukcji (§ 2 IV.4). W praktyce kopie danych wykonywane były niesystematycznie, z mniejszą częstotliwością i przechowywane w pomieszczeniu innym niż wskazane, co szerzej opisano w dalszej części wystąpienia pokontrolnego, w sekcji „Ustalone nieprawidłowości". (dowód: akta kontroli str. 84-88,164-166)

W okresie objętym kontrolą wystąpiła konieczność odtworzenia zbioru danych ze sporządzonej kopii bezpieczeństwa. W wyniku podjętych działań odzyskano całą bazę danych[17]. (dowód: akta kontroli str. 215-222)

1.13. Pracownicy MGOPS dysponowali możliwością ściągania aplikacji i plików wykonalnych, co szerzej opisano w dalszej części wystąpienia pokontrolnego, w sekcji „Ustalone nieprawidłowości". Wszystkie komputery objęte były wsparciem producenta. Nie prowadzono odrębnej ewidencji programów zainstalowanych na poszczególnych komputerach Ośrodka. (dowód: akta kontroli str. 18-21,152-163, 240-242)

1.14. W MGOPS zadbano o aktualizację systemów operacyjnych oraz aplikacji bezpieczeństwa, zgodnie z harmonogramem ustalonym przez producenta, stosownie do § 20 ust. 2 pkt 12 lit. a rozporządzenia KRI. (dowód: akta kontroli str. 18-21,152-163)

---

[13] Badane komputery posiadały aktualne wersje i definicje wirusów programu antywirusowego ESET Endpoint bez mechanizmu centralnego zarządzania.

[14] Zapora sieciowa chroniąca sieć wewnętrzną jednostki przed dostępem z zewnątrz (np. sieci publicznej, Internetu).

[15] mgops@suchowola.pl oraz mgops_suchowola@poczta.onet.pl.

[16] Adres poczty elektronicznej udostępniony na BIP MGOPS.

[17] Odzyskanie bazy danych systemu „Księgowość budżetowa" z pomocą serwisu ZETO z automatycznie tworzonej kopii.

1.15. W MGOPS opracowano regulacje wewnętrzne w zakresie dokonywania płatności drogą elektroniczną[18]. Drukowanie przelewów odbywało się za pomocą komputera przy wykorzystaniu programu „Przelewy", zainstalowanego i użytkowanego na komputerze Głównej Księgowej. Dostęp do danych zabezpieczony był hasłem, gwarantując zachowanie poufności danych. Wykonywanie operacji bankowych odbywało się za pomocą systemu Home Banking, zainstalowanego i użytkowanego również na komputerze Głównej Księgowej. Dostęp do danych zabezpieczony był hasłem logowania, gwarantując zachowanie poufności danych. W MGOPS pojedyncze dyspozycje przelewów wprowadzane były do systemu ręcznie – na podstawie faktur, rachunków, list płac itp. Dyspozycje zbiorcze były pobierane z pliku źródłowego – na podstawie papierowych list wypłat, dostarczonych przez pracowników merytorycznych. Plik źródłowy był sporządzany w programach do obsługi świadczeń[19], a następnie zapisywany na dysku twardym komputera i wczytywany do systemu Home Banking. Dane z plikiem przelewów z dysku twardego po wykonaniu operacji były natychmiast usuwane. Wprowadzone bądź wczytane do Systemu Home Banking dane były sprawdzane co do poprawności danych, następnie autoryzowane za pomocą kodu PIN przez właściwe osoby i za pomocą kodu transmisji wysłane do uprawnionych osób bądź instytucji. (dowód: akta kontroli str. 172-174)

Ustalone nieprawidłowości

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

1. W MGOPS nie zastosowano odpowiednich środków technicznych, mających za zadanie zapewnienie ochrony przetwarzania danych osobowych, w stopniu wymaganym art. 36 ustawy o ochronie danych osobowych.
   a) Wszyscy pracownicy MGOPS posiadali uprawnienia administratora systemu operacyjnego, mimo że – zgodnie z ich zakresem obowiązków – nie realizowali oni zadań w zakresie administrowania systemami. W konsekwencji m.in. dysponowali możliwością ściągania aplikacji i plików wykonalnych oraz posiadali uprawnienia do instalowania ich na stacjach komputerowych, do których mieli dostęp. Było to sprzeczne z przepisem § 20 ust. 2 pkt 4 rozporządzenia KRI, zgodnie z którym kierownictwo podmiotu publicznego jest obowiązane do podejmowania działań zapewniających, że osoby zaangażowane w proces przetwarzania informacji posiadają stosowne uprawnienia i uczestniczą w tym procesie w stopniu adekwatnym do realizowanych zadań oraz obowiązków mających na celu zapewnienie bezpieczeństwa informacji. (dowód: akta kontroli str. 18-21, 152-163)

      Były Kierownik MGOPS poinformował, że: *„Użytkownicy przetwarzający dane osobowe na wszystkich ośmiu komputerach posiadali w systemach operacyjnych Windows uprawnienia administratora, ponieważ nie posiadałam świadomości ani wiedzy informatycznej. W omawianym okresie, tj. 2016 – 2017, w naszym ośrodku nie był zatrudniony informatyk, który obsługiwałby systemy operacyjne Windows od strony informatycznej. Brak zatrudnienia informatyka wynikał z braku środków finansowych na ten cel."* (dowód: akta kontroli str. 229-239)

   b) Hasła dostępu do żadnego z ośmiu komputerów MGOPS nie spełniały wymogów określonych w § 2 pkt.II.1 oraz § 2 pkt. IV.2 Instrukcji oraz w cz. A pkt IV ust. 2 załącznika do rozporządzenia w sprawie dokumentacji i warunków technicznych dla wysokiego poziomu zabezpieczeń. Nie aktywowano bowiem mechanizmu wymuszania okresowej zmiany haseł, wymogu określonej ich złożoności ani minimalnej długości hasła. (dowód: akta kontroli str. 18-21, 84-88, 152-163)

      Była Kierownik MGOPS wyjaśniła, że: *„Użytkownicy komputerów, przetwarzający dane osobowe nie zmieniali haseł dostępu do systemu Windows, a hasła nie spełniały określonych wymagań, ponieważ zarówno ja, jak i pracownicy nie posiadaliśmy wiedzy informatycznej, nie byliśmy też świadomi, że należy dokonywać zmian haseł w systemie Windows. Zmienialiśmy hasła jedynie w programach*

[18] Załącznik do zarządzenia Nr 3/2016 Kierownika Miejsko-Gminnego Ośrodka Pomocy Społecznej w Suchowoli z dnia 23 maja 2016 r., zmieniającego załącznik Nr 5 do zarządzenia Nr 4/2015 Kierownika Miejsko-Gminnego Ośrodka Pomocy Społecznej w Suchowoli z dnia 31 grudnia 2015 r. w sprawie ustalenia planu kont dla MGOPS oraz wprowadzenia zasad rachunkowości w MGOPS.

[19] Wykazanych w załączniku Nr 7 w części „Programy stosowane dla realizacji zadań statutowych".

dziedzinowych, tj. Amazis, Nemezis, Cheops, Izyda i Helios oraz w programie Płatnik, Księgowość budżetowa, Kady i Płace oraz Przelewy."

(dowód: akta kontroli str. 229-239)

c) W MGOPS jedno z dwóch kont poczty elektronicznej hostingowane było bezpłatnie przez operatora komercyjnego, z którym Ośrodek nie miał podpisanej umowy na świadczenie takiej usługi. Biegły w dziedzinie bezpieczeństwa systemów informatycznych stwierdził, że wykorzystywanie w pracy MGOPS konta poczty elektronicznej hostingowanej przez operatora komercyjnego nie gwarantuje bezpieczeństwa takiej usługi. Obowiązek zabezpieczenia informacji w sposób uniemożliwiający nieuprawnionemu jej ujawnienie, modyfikacje, usunięcie lub zniszczenie wynika z przepisu § 20 ust. 2 pkt 9 rozporządzenia KRI. Dodatkowo poczta ta nie była zabezpieczona przed niechcianymi lub niepotrzebnymi wiadomości elektronicznymi. (dowód akta kontroli str. 18-21, 152-162)

Była Kierownik MGOPS wyjaśniła, że : *„W Miejsko-Gminnym Ośrodku Pomocy Społecznej w Suchowoli używano w okresie 2016 – 2017 konta poczty elektronicznej na darmowym serwerze, ponieważ nie byłam świadoma niebezpieczeństwa przy przetwarzaniu danych osobowych, a nie mamy zatrudnionego informatyka, który uzmysłowiłby nam te niebezpieczeństwa. Konto poczty elektronicznej, jest podane do kontaktu w części instytucji, z którymi nasz Ośrodek współpracuje. Jest ono sukcesywnie wycofywane z użytku z przekierowaniem na korzystanie z konta mgops@suchowola.pl".* (dowód: akta kontroli str. 229-239)

2. W Ośrodku nie monitorowano dostępu do przetwarzanych informacji, w celu zapewnienia im ochrony przed kradzieżą, nieuprawnionym dostępem, uszkodzeniami lub zakłóceniami, o których mowa w § 20 ust. 2 pkt 7 lit. a rozporządzenia KRI, ponieważ: [1] nie prowadzono zbiorczego rejestru dostępu do systemu, [2] nie zabezpieczono przed modyfikacją i zniszczeniem logów zapisywanych na komputerach użytkowników, a informacji w nich zawartych nie przetwarzano automatycznie, [3] nie zabezpieczono trwale informacji o podłączeniu do komputerów zewnętrznych nośników pamięci, [4] nie nadzorowano pracowników firmy zewnętrznej podczas realizacji prac serwisowych przy wykorzystaniu aplikacji pulpitu zdalnego TeamViewer[20], zainstalowanej na dwóch komputerach. Ponadto, jak stwierdził biegły, dostęp do sieci lokalnej kontrolowany był przez mało skuteczny firewall programowy[21], zainstalowany na niskiej klasy routerze, niechroniącym odpowiednio zasobów sieci przed ingerencją z zewnątrz. (dowód: akta kontroli str. 18-21, 152-163)

Była Kierownik Ośrodka wyjaśniła, że: *„W MGOPS nie monitorowano dostępu do przetwarzanych informacji, w celu zapewnienia im ochrony przed kradzieżą, nieuprawnionym dostępem, uszkodzeniami lub zakłóceniami(...) ze względu na braki kadrowe, nie wyznaczono osoby do realizacji tego zadania. Nadzór nad realizacją prac serwisowych przy wykorzystaniu aplikacji pulpitu zdalnego sprawowała Główna Księgowa, która jest jedynym operatorem w programach księgowych. Korzystanie z aplikacji pulpitu zdalnego TeamViewer jest zapisane w umowie z firmą ZETO – dostawcą oprogramowania. Dostęp do aplikacji jest zabezpieczony – w celu połączenia się niezbędne jest podanie ID oraz hasła. Umowa z firmą ZETO zawiera również klauzulę poufności dla Wykonawcy."* (dowód: akta kontroli str. 229-239)

W opinii biegłego połączenia z wykorzystaniem aplikacji TeamViewer nie wymagają od podłączanego użytkownika autoryzacji – korzysta on z autoryzacji użytkownika, który udostępnia mu pulpit (serwisant pracuje na koncie z uprawnieniami użytkownika zalogowanego do systemu). Autoryzacja w przypadku tej aplikacji dotyczy jedynie nawiązania połączenia (kanału), a nie dostępu do zasobów komputera.

(dowód: akta kontroli str. 18-21)

3. W okresie objętym kontrolą nie przestrzegano regulacji określonych w § 2 pkt IV.3 obowiązującej w MGOPS Instrukcji, dotyczących procesu tworzenia kopii bezpieczeństwa, zgodnie z którym powinny one być tworzone *„nie rzadziej niż raz*

[20] Aplikacja umożliwiająca zdalny dostęp do komputerów Urzędu w celu naprawy zainstalowanych na nich programów.
[21] Zapora sieciowa chroniąca sieć wewnętrzną jednostki przed dostępem z zewnątrz (np. sieci publicznej, Internetu).

w tygodniu". W rzeczywistości kopie danych programów dziedzinowych sporządzano średnio raz na miesiąc[22], natomiast kopie zapasowe baz danych części systemów finansowo-księgowych, tj. "Księgowość budżetowa", „Kadry i Płace", „Przelewy" utworzono na zewnętrznych dyskach tylko dwa razy, a „Rejestr VAT" i „Płatnik" – w ogóle.

Ponadto – wbrew przyjętym regulacjom – nośniki zawierające kopie baz danych przechowywano w pok. 104, tj. tym samym co jednostka komputerowa, na której znajdowały się dane podlegające procesowi tworzenia kopii, natomiast innym, niż lokalizacja wskazana w § 2 pkt IV.4. Instrukcji (pok. 12). W MGOPS nie sprawdzano poprawności ich wykonania, co nie zapewniało odpowiedniego poziomu bezpieczeństwa przechowywanych danych. Ponadto w trakcie oględzin przeprowadzonych w ramach niniejszej kontroli ustalono, że wykonanie kopii danych z poziomu programu Helios i Cheops nie było możliwe. (dowód: akta kontroli str. 84-88,152-163, 243-244)

Była Kierownik MGOPS wyjaśniła, że: *„W okresie objętym kontrolą 2016 – 2017 kopie zapasowe zbiorów danych przetwarzanych w Miejsko-Gminnym Ośrodku Pomocy Społecznej w Suchowoli tworzono raz w miesiącu, jedynie przy okazji aktualizacji, wynikało to z nieumiejętności tworzenia kopii zapasowych. Zaś kopie części programów księgowych, tj. Księgowość budżetowa, Kadry i Płace, Przelewy wykonano w okresie 2016 – 2017 jedynie dwa razy z powodu dużej ilości zadań nałożonych na księgową."*
(dowód: akta kontroli str. 229-239)

W sprawie sprawdzania poprawności kopii danych Kierownik MGOPS wyjaśniła: *„Jestem Kierownikiem jednostki od niedawna. Z informacji uzyskanych od Gł. Księgowej, w której pomieszczeniu znajduje się sejf z kopiami danych wynika, że nie były pobierane nośniki danych w celu ich testowego odtwarzania. Ustaliłam, że w tym okresie nie było informatyka ani osoby zobowiązanej, ani uprawnionej do tych czynności".*
(dowód: akta kontroli str. 243-244)

Zdaniem NIK, rutynowe kopiowanie plików, programów komputerowych i dokumentów o znaczeniu krytycznym oraz przechowywanie tych kopii w bezpiecznej, zdalnej lokalizacji jest zazwyczaj najbardziej opłacalnym działaniem, jakie jednostka może podjąć w celu ograniczenia przerw w działaniu. Stwarza to możliwości odzyskiwania systemu informacji i jego przywrócenie do stanu pierwotnego.

4. MGOPS dopiero w 2016 roku przeprowadził analizę ryzyka utraty integralności, dostępności lub poufności informacji, mimo że obowiązek ten został wprowadzony z dniem 31 maja 2012 r. (§ 20 ust. 2 pkt 3 rozporządzenia KRI). Była ona jednak niekompletna, gdyż wprawdzie zdefiniowano skalę zagrożeń utraty poufności, integralności, rozliczalności, ale nie określono żadnej z tych wartości. Przewidziano wskazanie wartości wymagań z podziałem na ww. zagrożenia, jednak ich nie zwymiarowano (rubryki nazwa stanu / wartość stanu były we wszystkich przypadkach puste). Nie sformułowano wniosków ani nie zaproponowano działań naprawczych (rubryki w punkcie 6 dokumentu były puste). Nie uzupełniono ani nie przeprowadzono ponownie takiej analizy, mimo określenia w tym dokumencie, corocznej częstotliwości jej wykonywania. (dowód: akta kontroli str. 89-100, 172-174)

   Była Kierownik MGOPS wyjaśniła, że: *„Nie przeprowadzano okresowej analizy ryzyka utraty integralności, dostępności lub poufności informacji, ponieważ nie wyznaczono osoby do pełnienia ww. funkcji, a co za tym idzie nie przeprowadzono ww. analizy."*
   (dowód: akta kontroli str. 229-239)

   Ponadto w przeprowadzonej w 2016 roku analizie wskazano Administratora Bezpieczeństwa Informacji[23] oraz Administratora Systemu Informatycznego, jako osoby odpowiedzialne za wykonanie kolejnych analiz w tym zakresie. Do zakończenia kontroli nie powołano żadnej osoby do pełnienia ww. funkcji.

[22] Z wyjątkiem maja i grudnia w 2016 roku.
[23] Zwany dalej „ABI".

Była Kierownik MOPS wyjaśniła, że: „*W MGOPS planowano zatrudnić osobę pełniącą obowiązki Administratora Systemów Informatycznych, jednakże z powodu braku środków finansowych nie zatrudniono takiej osoby.*"

(dowód: akta kontroli str. 89-100, 172-174, 229-239)

W ocenie NIK, przeprowadzenie niekompletnej analizy dopiero po ponad czterech latach obowiązywania tego wymogu nie zapewnia rzetelnej wiedzy o występowaniu ww. ryzyk.

Ocena cząstkowa

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

2. Dokumentacja i procedury dotyczące ochrony danych

Opis stanu faktycznego

2.1. MGOPS zgłosił do rejestracji GIODO jeden (z siedmiu) przetwarzanych zbiorów danych osobowych, tj. „Świadczenia wychowawcze – Program 500+". Zgłoszenie do rejestracji tego zbioru danych osobowych zawierało wszystkie elementy określone w art. 41 ust 1 ustawy o ochronie danych. W okresie objętym kontrolą Ośrodek nie wnosił do GIODO o wykreślenie z rejestru tego zbioru. Jeden zbiór, Karta Dużej Rodziny nie podlegał rejestracji przez MGOPS, gdyż – w myśl art. 21 ust. 2 ustawy o Karcie Dużej Rodziny – administratorem danych osobowych przetwarzanych w tym zbiorze jest Burmistrz Suchowoli i to on powinien dokonać rejestracji. Szerzej problem niezgłaszania do GIODO pozostałych pięciu zbiorów danych osobowych opisano w dalszej części wystąpienia pokontrolnego, w sekcji „Ustalone nieprawidłowości".

(dowód: akta kontroli str. 10-15, 146, 172-174)

2.2. Administrator Danych Osobowych[24] w MGOPS nie powołał ABI, mimo że w Instrukcji (§ 5 i 6) określił dla tej funkcji obowiązki m.in.: dokonywania przeglądów technicznych sprzętu informatycznego oraz dbałość o jego dobry stan techniczny, zalecenie dokonywania przeglądów okresowych co 30 dni oraz przeglądów generalnych raz na rok, niezwłoczne powiadomienie ADO w przypadku stwierdzenia usterki. Była Kierownik Ośrodka wyjaśniła: „*W MGOPS nie skorzystano z możliwości wyznaczenia Administratora Bezpieczeństwa Informacji ze względu na braki kadrowe. Pracownicy socjalni zgodnie z ustawą o pomocy społecznej nie mogą pełnić innych funkcji. Pracownicy prowadzący świadczenia rodzinne, świadczenia wychowawcze i fundusz alimentacyjny oraz główny księgowy są nadmiernie obciążeni obowiązkami.*" (dowód: akta kontroli str. 172-174, 229-239)

2.3. W myśl przepisu art. 36b ustawy o ochronie danych osobowych w przypadku niewyznaczenia ABI, zadania określone w art. 36a ust 2 pkt 1 tej ustawy, z wyłączeniem obowiązku sporządzania sprawozdania, realizuje ADO. Pomimo to Kierownik MGOPS, jako administrator danych osobowych, w 2016 roku opracowała niekompletną dokumentację opisującą sposób przetwarzania danych osobowych, środki techniczne i organizacyjne zapewniające ich ochronę oraz nie wprowadziła niezbędnych aktualizacji. Nieskuteczny był również nadzór nad przestrzeganiem zasad w nich określonych, co szerzej opisano w dalszej części wystąpienia pokontrolnego, w sekcji „Ustalone nieprawidłowości".

(dowód: akta kontroli str. 22-100)

W okresie objętym kontrolą osoby upoważnione do przetwarzania danych osobowych i nowo zatrudnieni pracownicy nie zostali zapoznani z przepisami o ochronie takich danych, co szerzej opisano w dalszej części wystąpienia pokontrolnego, w sekcji „Ustalone nieprawidłowości". (dowód: akta kontroli str. 229-239)

2.4. W MGOPS, mimo wymogu określonego w art. 39 ust. 1 ustawy o ochronie danych osobowych, do 1 stycznia 2018 r. nie prowadzono ewidencji osób upoważnionych do przetwarzania danych osobowych, natomiast założona 2 stycznia 2018 r. ewidencja była niekompletna, co szerzej opisano w sekcji „Ustalone nieprawidłowości".

(dowód: akta kontroli str. 22-81)

Zakres upoważnień wszystkich pracowników MGOPS do przetwarzania danych w systemach informatycznych był zgodny z realizowanymi przez nich zadaniami

[24] Zwany dalej „ADO".

i w przypadku ośmiu z dziesięciu osób wynikał z ich zakresu obowiązków. Pozostałe dwa przypadki szerzej opisano w sekcji „Ustalone nieprawidłowości."
(dowód: akta kontroli str. 39-48, 73-81, 150-151,250-277)

Ponadto nie wywiązano się z obowiązków określonych w umowie[25] na korzystanie z Samorządowej Elektronicznej Platformy Informacyjnej[26], administrowanej przez Powiatowy Urząd Pracy w Sokółce. W umowie tej strony zobowiązały się do zachowania w tajemnicy danych osobowych beneficjentów oraz ich zabezpieczenia zgodnie z zasadami określonymi w ustawie o ochronie danych osobowych oraz udzielenia upoważnień do przetwarzania danych osobowych. Upoważnienia te zostały udzielone z opóźnieniem, co szerzej opisano w sekcji „Ustalone nieprawidłowości." (dowód: akta kontroli str. 185-214)

2.5. W MGOPS nie opracowywano procedur wewnętrznych dotyczących ochrony danych osobowych, poza Polityką bezpieczeństwa[27] i Instrukcją. (dowód: akta kontroli str. 172-174)

2.6. Była Kierownik MGOPS nie powołała administratora systemów informatycznych Ośrodka, mimo że w regulacjach wewnętrznych wskazała szereg zadań dla osoby pełniącej tę funkcję. (dowód: akta kontroli str. 89-100, 175-177)

2.7. W okresie objętym kontrolą w MGOPS 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. 172-174)

2.8. Do stycznia 2018 roku żaden (z dziesięciu) pracowników MGOPS zaangażowanych w proces przetwarzania informacji nie brał udziału w szkoleniach z zakresu ochrony danych osobowych. W związku ze zmianą przepisów o ochronie danych osobowych z dniem 1 maja 2018 r. planowane jest przeszkolenie w kwietniu 2018 roku wszystkich pracowników Ośrodka. Szerzej problem szkoleń z tematyki ochrony danych osobowych opisano w dalszej części wystąpienia pokontrolnego, w sekcji „Ustalone nieprawidłowości".
(dowód: akta kontroli str. 82-83,145, 172-174, 178-180)

2.9. W okresie objętym kontrolą w Ośrodku nie były przeprowadzane zewnętrzne kontrole w zakresie bezpieczeństwa danych osobowych. Nie wpływały również do MGOPS skargi związane z nieuprawnionymi przypadkami ujawnienia danych osobowych.
(dowód: akta kontroli str. 172-174)

2.10. W MGOPS dokumentacja związaną z przetwarzaniem danych osobowych, tj. Polityka bezpieczeństwa oraz Instrukcja, zostały wprowadzone po raz pierwszy 22 sierpnia 2016 r. oraz zaktualizowane 2 stycznia 2018 r.[28]

Obowiązująca do 1 stycznia 2018 r. Polityka bezpieczeństwa spośród elementów wymaganych przepisem § 4 rozporządzenia w sprawie dokumentacji i warunków technicznych zawierała jedynie określenie środków technicznych i organizacyjnych niezbędnych dla zapewnienia poufności, integralności i rozliczalności przetwarzanych danych.

Instrukcja obowiązująca w tym okresie zawierała natomiast elementy określone w § 5 pkt 2, 3 i 5 – 8 rozporządzenia w sprawie dokumentacji i warunków technicznych, tj. m.in.: stosowane metody i środki uwierzytelnienia oraz procedur związanych z ich zarządzaniem i użytkowaniem, procedury rozpoczęcia, zawieszenia i zakończenia pracy przeznaczonych dla użytkowników systemów, sposób, miejsce i okres przechowywania elektronicznych nośników informacji zawierających dane osobowe oraz kopii zapasowych zbiorów danych, programów i narzędzi programowych służących do ich przetwarzania. Wskazywała sposób zabezpieczenia systemu informatycznego przed awariami zasilania oraz ochrony przed działalnością oprogramowania, którego celem jest uzyskanie nieuprawnionego dostępu do systemu informatycznego. Określała sposób realizacji

[25] Umowa zawarta 16 października 2013 r. pomiędzy Kierownikiem MGOPS a Dyrektorem Powiatowego Urzędu Pracy w Sokółce.
[26] Dalej: „SEPI".
[27] Zarządzenie nr 4 /2016 Kierownika Miejsko-Gminnego Ośrodka Pomocy Społecznej w Suchowoli z dnia 22 sierpnia 2016 r. w sprawie wprowadzenia „Polityki bezpieczeństwa w MGOPS".
[28] Zarządzenie 1/2018 Kierownika Miejsko-Gminnego Ośrodka Pomocy Społecznej w Suchowoli z dnia 2 stycznia 2018 r.

wymogów, o których mowa w § 7 ust. 1 pkt 4 rozporządzenia w sprawie dokumentacji oraz warunków technicznych, a także procedury wykonywania przeglądów i konserwacji systemów oraz nośników informacji służących do przetwarzania danych.

W Instrukcji poziom bezpieczeństwa przetwarzania danych osobowych w systemach informatycznych MGOPS, zgodnie z § 6 rozporządzenia w sprawie dokumentacji oraz warunków technicznych, określono jako wysoki (§ 2 Instrukcji), ponieważ wszystkie osiem komputerów, na których przetwarzano dane osobowe było połączonych z siecią publiczną.

Dokumenty te nie zawierały natomiast elementów określonych w § 4 pkt 1 – 4 oraz zawierały niekompletne informacje wymagane przepisem § 5 pkt 1 i 4 rozporządzenia w sprawie dokumentacji oraz warunków technicznych.

Wprowadzona 2 stycznia 2018 r. aktualizacja dokumentacji wewnętrznej obejmowała jedynie Politykę Bezpieczeństwa, którą uzupełniono o elementy wymagane przepisem § 4 pkt 1 i 2 rozporządzenia w sprawie dokumentacji oraz warunków technicznych. Ponadto określono w niej opis struktury zbiorów danych wskazujący zawartość poszczególnych pól informacyjnych, jednak bez określenia powiązań między nimi oraz sposobu przepływu danych pomiędzy poszczególnymi systemami, co szerzej opisano w dalszej części wystąpienia pokontrolnego, w sekcji „Ustalone nieprawidłowości".

Nie wywiązano się również z obowiązku – wynikającego z § 2 pkt 15 w związku z § 20 ust. 1 rozporządzenia KRI – wdrożenia regulacji wewnętrznych stanowiących politykę bezpieczeństwa informacji, co szerzej opisano w dalszej części wystąpienia pokontrolnego, w sekcji „Ustalone nieprawidłowości". (dowód: akta kontroli str. 22-48, 84-88, 175-177)

Ustalone nieprawidłowości

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

1. Ośrodek nie zgłosił do rejestracji GIODO pięciu (z siedmiu) przetwarzanych zbiorów danych osobowych, tj. Pomoc społeczna, Dodatki mieszkaniowe, Świadczenia rodzinne, Fundusz alimentacyjny (funkcjonujących w MGOPS na 1 stycznia 2016 r.), Ustawa o wsparciu kobiet w ciąży i ich rodzin „Za życiem" (z 4 listopada 2016 r.[29]), mimo takiego wymogu wynikającego z art. 40 ustawy o ochronie danych osobowych.
(dowód: akta kontroli str. 10-15,146)

   Była Kierownik MOPS wyjaśniła: *„MGOPS, będący Administratorem Danych Osobowych, nie zarejestrował pięciu z siedmiu przetwarzanych zbiorów danych osobowych z powodu zbyt dużej liczby obowiązków nałożonych na ośrodek oraz braków kadrowych i braku dostatecznych umiejętności."* (dowód: akta kontroli str. 229-239)

2. W latach 2016 – 2018 (do 5 stycznia) w MGOPS 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.
(dowód: akta kontroli str. 172-174)

   Była Kierownik MGOPS wyjaśniła, że audytu nie przeprowadzono, *„ponieważ nie miałam świadomości o konieczności"* jego przeprowadzania.
(dowód: akta kontroli str. 229-239)

3. Do 16 stycznia 2018 r. żaden (z dziesięciu) pracowników MGOPS przetwarzających dane osobowe nie uczestniczył w szkoleniach dotyczących zagadnień związanych z ochroną danych osobowych oraz bezpieczeństwem informacji. Takie szkolenie odbyło się dopiero w styczniu 2018 roku, tj. w trakcie kontroli NIK. Obowiązek zapewnienia szkoleń osobom zaangażowanym w proces przetwarzania informacji, z uwzględnieniem zagrożenia jej bezpieczeństwa, skutków naruszenia zasad bezpieczeństwa, konsekwencji prawnych i środków zapewniających jej bezpieczeństwo, ustalono w § 20 ust. 2 pkt 6 rozporządzenia KRI. (dowód: akta kontroli str. 145, 172-174, 178-180)

   Była Kierownik MOPS wyjaśniła, że: *„takie szkolenia były zaplanowane na IV kwartał 2017 r., jednak nie zostały wykonane z powodu braków finansowych."*
(dowód: akta kontroli str. 229-239)

[29] Obowiązującej od 1 stycznia 2017 r.

4. W MGOPS, mimo wymogu określonego w art. 39 ust. 1 ustawy o ochronie danych osobowych, do 1 stycznia 2018 r. nie prowadzono ewidencji osób upoważnionych do przetwarzania danych osobowych. Od 2 stycznia 2018 r. ewidencja ta była zaś niekompletna, gdyż nie zawierała identyfikatorów osób upoważnionych do przetwarzania danych osobowych w systemach, wbrew wymogom określonym w art. 39 ust. 1 pkt 3 ustawy o ochronie danych osobowych. Ponadto nie ujęto w niej informacji o dziewięciu pracownikach Powiatowego Urzędu Pracy w Sokółce, którym wydano upoważnienia 29 maja 2017 r.[30] (dowód: akta kontroli str. 22-83)

   Była Kierownik MOPS wyjaśniła, że: *„(...) Nie zdawałam sprawy o tak dużej ważności tego dokumentu. Został on sporządzony w oparciu o wzorcową instrukcję i z powodu przeoczenia, nie zostały w niej uzupełnione następujące elementy".*
   (dowód: akta kontroli str. 229-239)

   Kierownik MGOPS wyjaśniła, że: *„Pierwszego dnia roboczego, po objęciu stanowiska Kierownika MGOPS zorientowałam się, że Polityka bezpieczeństwa nie posiada wielu informacji. Pilnie ją uzupełniłam o dane, które były w mojej kompetencji. Nie wpisałam do rejestru osób upoważnionych do przetwarzania danych osobowych dziewięciu pracowników PUP w Sokółce, ponieważ nie miałam świadomości, że takie upoważnienia zostały wydane. Dopiero w późniejszym terminie odnalazłam umowę z PUP i zauważyłam swoje przeoczenie, co niezwłocznie zamierzam uwzględnić w najbliższej aktualizacji Polityki bezpieczeństwa".* (dowód: akta kontroli str. 243-244)

5. Polityka bezpieczeństwa obowiązująca od 22 sierpnia 2016 r. do 1 stycznia 2018 r. nie zawierała elementów przewidzianych w § 4 pkt 1 – 4 rozporządzenia w sprawie dokumentacji oraz warunków technicznych, tj.: aktualnego wykazu budynków, pomieszczeń, w którym przetwarzano dane osobowe, wykazu zbiorów danych osobowych wraz ze wskazaniem programów zastosowanych do przetwarzania tych danych, opisu struktury zbiorów danych, wskazującego zawartość poszczególnych pól informacyjnych, powiązań między nimi, sposobu przepływu danych pomiędzy poszczególnymi systemami. (dowód: akta kontroli str. 22-48)

   Była Kierownik MGOPS wyjaśniła: *„Nie zdawałam sprawy o tak dużej ważności tego dokumentu. Został on sporządzony w oparciu o wzorcową instrukcję i z powodu przeoczenia, nie zostały w niej uzupełnione następujące elementy."*
   (dowód: akta kontroli str. 229-239)

   Obowiązująca od 22 sierpnia 2016 r. Instrukcja nie wskazywała osoby odpowiedzialnej za nadawanie i rejestrowanie uprawnień do przetwarzania danych w systemach informatycznych, a także nie wskazywała programów i narzędzi programowych do przetwarzania kopii zbiorów danych, wymaganych § 5 odpowiednio pkt 1 i pkt 4 rozporządzenia w sprawie dokumentacji oraz warunków technicznych.

   Była Kierownik MGOPS wyjaśniła: *„(...) ponieważ nie było osoby posiadającej kompetencje wyznaczonej do tego zadania."* (dowód: akta kontroli str. 84-88, 229-239)

   Ponadto przyjęta 2 stycznia 2018 r. aktualizacja Polityki bezpieczeństwa wprowadziła w jej treści jedynie część wymaganych elementów, przez co w dalszym ciągu dokument ten zawierał niekompletny opis struktury zbiorów danych, wskazujący zawartość poszczególnych pól informacyjnych, ale bez wskazania powiązań między nimi oraz nie określono w nim sposobu przepływu danych pomiędzy poszczególnymi systemami. Elementy te są wymagane przepisem § 4 pkt 3 i 4 rozporządzenia w sprawie dokumentacji oraz warunków technicznych. (dowód: akta kontroli str. 49-81)

   Kierownik MOPS wyjaśniła, że: *„Niekompletny opis struktury zbiorów danych nie wykazuje powiązań między nimi oraz brak sposobu przepływu danych pomiędzy poszczególnymi systemami spowodowany jest zbyt krótkim czasem od objęcia stanowiska Kierownika niepozwalającym na jego weryfikację. Błędy zostaną poprawione w najbliższym czasie."* (dowód: akta kontroli str. 223-226)

[30] Na podstawie umowy zawartej 16 października 2013 r. między MGOPS i Powiatowym Urzędem Pracy w Sokółce.

Wyżej wymienione braki w przyjętej dokumentacji wewnętrznej powodowały, że regulacje składające się na politykę bezpieczeństwa informacji, określoną w § 2 pkt 15 rozporządzenia KRI, nie odpowiadały wymogom § 20 ust. 1 ww. rozporządzenia.

6. Dwóm spośród dziesięciu osób przetwarzających dane osobowe w MGOPS nie nadano upoważnień do przetwarzania danych osobowych w zbiorze o nazwie: Ustawa o wsparciu kobiet w ciąży i ich rodzin „Za życiem" (prowadzonego z wykorzystaniem programu „Amazis"), mimo że osoby te przetwarzały dane w tym zbiorze od 2017 roku do zakończenia kontroli. Było to niezgodne z art. 37 ustawy o ochronie danych osobowych, w myśl którego do przetwarzania danych mogą być dopuszczone wyłącznie osoby posiadające upoważnienie nadane przez administratora danych.
(dowód: akta kontroli str. 22-81, 145, 147-149, 162-163)

Kierownik MGOPS wyjaśniła: *„Ww. osobom nie nadano uprawnień z powodu przeoczenia. Ustawa Za życiem odnosi się do bardzo wąskiej grupy społecznej. W naszym Ośrodku w 2017 roku był rozpatrzony jeden wniosek w oparciu o tę ustawę. W najbliższym czasie upoważnienia zostaną nadane."*
(dowód: akta kontroli str. 245-246)

7. MGOPS upoważniło dziewięciu pracowników Powiatowego Urzędu Pracy w Sokółce do przetwarzania danych osobowych dopiero 29 maja 2017 r., tj. z opóźnieniem ponad trzech lat i siedmiu miesięcy w stosunku do postanowień § 3 pkt. 2 umowy zawartej 16 października 2013 r. między MGOPS i Powiatowym Urzędem Pracy w Sokółce. Ośrodek wystawił ww. upoważnienia dopiero po otrzymaniu monitu od Powiatowego Urzędu Pracy w Sokółce, skierowanego w wyniku przeprowadzonych sprawdzeń ABI w Sokółce. (dowód: akta kontroli str. 185-214)

Była Kierownik MGOPS wyjaśniła, że: *„Pracowników Powiatowego Urzędu Pracy w Sokółce, upoważniono do przetwarzania danych osobowych dopiero 29 maja 2017 r., ponieważ we wcześniejszym okresie nie miałam świadomości o konieczności takiego upoważnienia."* (dowód: akta kontroli str. 229-239)

Ocena cząstkowa

Najwyższa Izba Kontroli ocenia negatywnie opracowanie i wdrożenie dokumentacji oraz procedur ochrony danych i zgłaszanie rejestracji zbiorów do GIODO.

3. Sposób przechowywania oraz zabezpieczenia danych

Opis stanu faktycznego

3.1. Zgodnie z przyjętą w Ośrodku Polityką bezpieczeństwa, wszystkie pomieszczenia stanowiące obszar przetwarzania danych oraz szafy, w których gromadzono dane w wersji papierowej, zamykane były na klucz. W trakcie przeprowadzonych oględzin stwierdzono, że urządzenia sieciowe były zabezpieczone przed fizyczną ingerencją osób do tego nieupoważnionych z racji umieszczenia ich w szafce, do której dostęp był ograniczony. Na pierwszej kondygnacji budynku oraz w archiwum umieszczono gaśnice. W Ośrodku nie zainstalowano monitoringu wizyjnego, systemu przeciwpożarowego ani alarmowego. Okna nie posiadały zabezpieczeń antywłamaniowych oraz krat metalowych.
(dowód: akta kontroli str. 164-166)

W MGOPS nie sformalizowano „polityki kluczy", która określałaby podstawowe zasady postępowania z kluczami do pomieszczeń Urzędu, w których przetwarzane były dane osobowe. Klucze do szaf po zakończeniu pracy były gromadzone w oznaczonym pudełku i przekazywane Kierownikowi MGOPS, który je zamykał w szafce na kucz.
(dowód: akta kontroli str.164-166, 171)

3.2. W Urzędzie nie prowadzono rejestru zasobów informatycznych, co szerzej opisano w dalszej części wystąpienia pokontrolnego, w sekcji „Ustalone nieprawidłowości".
(dowód: akta kontroli str. 18-21, 172-174)

3.3. W okresie objętym kontrolą w Ośrodku nie dokonywano likwidacji lub naprawy sprzętu będącego nośnikiem danych. (dowód: akta kontroli str. 215-222)

3.4. W Urzędzie niszczenie dokumentów odbywało się za pomocą niszczarek, co było zgodne z wewnętrznymi regulacjami. MGOPS nie korzystał z usług firm zewnętrznych w tym zakresie. (dowód: akta kontroli str. 164-166, 172-174)

3.5. W § 2 pkt V. Instrukcji MGOPS przewidziano użytkowanie komputerów przenośnych z zachowaniem szczególnej ostrożności, w tym ze stosowaniem haseł dostępu do komputera oraz szyfrowania plików, w których przetwarzano dane osobowe.

Biegły w dziedzinie bezpieczeństwa systemów informatycznych stwierdził, że zdalny dostęp do zasobów nie funkcjonował, co szerzej omówiono w pkt 1.6 niniejszego wystąpienia pokontrolnego. (dowód: akta kontroli str. 18-21, 84-88)

3.6. Sprzątanie pomieszczeń, w których przetwarzano dane osobowe odbywało się w godzinach pracy MGOPS[31], co było to zgodne z Instrukcją. Wskazano tam bowiem, że przebywanie osób nieuprawnionych do dostępu do danych osobowych w pomieszczeniach znajdujących się wewnątrz obszaru przetwarzania tych danych jest dopuszczalne w obecności osoby upoważnionej do przetwarzania danych osobowych.
(dowód: akta kontroli str. 172-174)

3.7. W MGOPS nie dokonywano przeglądów technicznych sprzętu informatycznego, co szerzej opisano w sekcji „Ustalone nieprawidłowości". (dowód: akta kontroli str. 229-239)

3.8. Wszystkie komputery wykorzystywane przez pracowników MGOPS zostały zabezpieczone przed utratą zasilania, za pomocą zasilaczy awaryjnych UPS. W Urzędzie nie opracowano natomiast rozwiązań na wypadek wystąpienia sytuacji nadzwyczajnych, np. awarii, długotrwałego braku zasilania, procedur dotyczących przywracania systemów po awarii oraz planu ciągłości działania umożliwiającego kontynuację wykonywania zadań publicznych, co szerzej opisane zostało w dalszej części wystąpienia pokontrolnego, w sekcji „Uwagi dotyczące badanej działalności". Ośrodek nie posiadał dodatkowego źródła zasilania na wypadek długotrwałych przerw w dostawie prądu.
(dowód: akta kontroli str. 152-163, 229-239)

3.9. W MGOPS w latach 2016 – 2017 nie wystąpiły przypadki fizycznej utraty danych.
(dowód: akta kontroli str. 172-174, 215-222)

Ustalone nieprawidłowości

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

1. W MGOPS – wbrew wymogom § 20 ust. 2 pkt 2 rozporządzenia KRI – nie gromadzono bieżących informacji w zakresie inwentaryzacji sprzętu i oprogramowania służącego do przetwarzania informacji obejmujących ich rodzaj i konfigurację.
(dowód: akta kontroli str. 172-174)

   Była Kierownik MGOPS wyjaśniła: „(...) *nie gromadzono bieżących informacji w zakresie inwentaryzacji sprzętu i oprogramowania służącego do przetwarzania informacji obejmujących ich rodzaj i konfigurację, ponieważ we wskazanym okresie nie było zatrudnionego informatyka.* (dowód: akta kontroli str. 240-242)

2. W MGOPS nie dokonywano przeglądów technicznych sprzętu informatycznego w celu dbałości o ich dobry stan techniczny, do czego zobowiązano Administratora Bezpieczeństwa Informacji (którego nie powołano) – § 5 Instrukcji. Zalecono dokonywanie przeglądów okresowych co 30 dni oraz generalnych – raz na rok, a w przypadku stwierdzenia usterek technicznych niezwłoczne powiadomienie ADO.
(dowód: akta kontroli str. 84-88, 175-177)

   Była Kierownik MGOPS wyjaśniła: „*W okresie 2016 – 2017 nie dokonywano przeglądów okresowych co 30 dni oraz rocznych co rok, wymaganych wprowadzoną w MGOPS Instrukcją, ponieważ zbyt dużo obowiązków nałożonych na MGOPS oraz braki kadrowe uniemożliwiały wykonywanie tych zada* (dowód: akta kontroli str. 229-239)

Uwagi dotyczące badanej działalności

Najwyższa Izba Kontroli zwraca uwagę na potrzebę opracowania planu ciągłości działania MGOPS na wypadek wystąpienia np. długotrwałego braku zasilania, który umożliwiałby kontynuację wykonywania zadań. Plan ten powinien określić systemy i aplikacje o znaczeniu krytycznym oraz wszystkie podporządkowane lub powiązane plany. Istotne jest, aby plany te były jasno udokumentowane, przekazane pracownikom i aktualizowane w celu odzwierciedlenia bieżącej działalności Ośrodka.

[31] W dni robocze w godz. 7^{30} do godz. 15^{30}.

Ocena cząstkowa

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

4. Przetwarzanie zasobów informacyjnych zgodnych z zakresem działalności jednostki kontrolowanej

4.1. Dane osobowe w MGOPS przetwarzane były w siedmiu zbiorach danych, prowadzonych w wersji elektronicznej oraz papierowej.

Opis stanu faktycznego

Do końca 2017 roku MGOPS nie prowadził wykazu zbiorów danych osobowych wraz ze wskazaniem programów zastosowanych do ich przetwarzania, stanowiącego element obowiązującej wówczas Polityki bezpieczeństwa, co szerzej opisano w sekcji „Ustalone nieprawidłowości", w punkcie 2 wystąpienia pokontrolnego. Wykaz ten został opracowany wraz z aktualizacją Polityki bezpieczeństwa wprowadzoną 2 stycznia 2018 r.

(dowód: akta kontroli str. 22-81)

4.2. W okresie objętym kontrolą nie dokonywano aktualizacji zbioru danych zgłoszonego przez MGOPS do rejestracji GIODO, mimo zaistnienia takiej okoliczności, co szerzej opisano w dalszej części niniejszego wystąpienia, w sekcji „Ustalone nieprawidłowości".

(dowód: akta kontroli str. 10-15, 69-72, 152-163,172-174)

4.3. We wszystkich zbiorach danych prowadzonych w MGOPS zakres gromadzonych i przetwarzanych danych był niezbędny do realizacji zadań, dla których zbiory były prowadzone. (dowód: akta kontroli str. 39-48, 73-81,150-151, 250-277)

4.4. Ośrodek korzystał z trzech zewnętrznych elektronicznych źródeł danych, których administratorami były podmioty zewnętrzne, tj. SEPI, Systemu informatycznego Karta Dużej Rodziny oraz platformy wymiany informacji Emp@tia, tj. portalu prowadzonego przez Ministerstwo Rodziny Pracy i Polityki Społecznej służącemu m.in. do pozyskiwania i wymiany informacji o klientach MGOPS pomiędzy jednostkami pomocy społecznej. W przypadku SEPI strony umowy zobowiązały się do zachowania w tajemnicy danych osobowych beneficjentów oraz ich zabezpieczenia zgodnie z zasadami określonymi w ustawie o ochronie danych osobowych. Uzyskanie dostępu do tych zbiorów nie wymagało spełnienia przez Ośrodek specjalnych warunków takich, jak np. stworzenie wydzielonego łącza internetowego czy budowy określonej struktury sieci.

(dowód: akta kontroli str. 139-144,185-201)

Ustalone nieprawidłowości

W działalności kontrolowanej jednostki w przedstawionym wyżej zakresie stwierdzono nieprawidłowość polegającą na braku w zgłoszeniu rejestracyjnym do GIODO[32] informacji o przetwarzanym w zbiorze numerze konta bankowego. 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 danych gromadzonych w zbiorze. (dowód: akta kontroli str. 10-15, 69-72, 152-163,172-174)

Kierownik MGOPS wyjaśniła: *„ Funkcję Kierownika MGOPS pełnię od 2 stycznia 2018 r. Był to zbyt krótki okres, żeby zapoznać się ze wszystkimi dokumentami, w tym zgłoszeniem do GIODO. W najbliższym czasie planuję zgłosić aktualizację. Wydaje mi się, że niezgłoszenie konta bankowego nastąpiło przez omyłkę."*

(dowód: akta kontroli str. 245-246)

Ocena cząstkowa

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

[32] Dotyczącym zbioru danych osobowych „Świadczenia wychowawcze – Program 500+".

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[33] wnosi o:

1. Nadanie użytkownikom komputerów uprawnień w systemach operacyjnych odpowiadających ich zakresom obowiązków.
2. Zapewnienie minimalnej długości, złożoności oraz zmiany – nie rzadziej niż co 30 dni – haseł dostępu do systemów operacyjnych, stosownie do § 2 pkt IV.2 Instrukcji.
3. Zaprzestanie używania bezpłatnego konta pocztowego, które nie gwarantuje zabezpieczenia informacji przed jej ujawnieniem nieuprawnionej osobie, modyfikacją, usunięciem lub zniszczeniem.
4. Analizowanie i zabezpieczenie przed modyfikacją lub zniszczeniem logów systemów operacyjnych komputerów wykorzystywanych w MGOPS.
5. Przestrzeganie zasad i procedur dotyczących tworzenia i przechowywania kopii zapasowych baz danych, określonych w § 2 pkt IV.3 Instrukcji.
6. Przeprowadzanie okresowych analiz utraty integralności, dostępności lub poufności informacji, o których mowa § 20 ust. 2 pkt 3 rozporządzenia KRI.
7. Zgłoszenie GIODO do rejestracji pięciu zbiorów danych osobowych przetwarzanych w MGOPS oraz zgłoszenie aktualizacji zakresu danych przetwarzanych w zarejestrowanym zbiorze.
8. Utrzymywanie aktualności inwentaryzacji sprzętu i oprogramowania służącego do przetwarzania informacji obejmującej ich rodzaj i konfigurację oraz przeprowadzania corocznych audytów wewnętrznych z zakresu bezpieczeństwa informacji, zgodnie z § 20 ust. 2 pkt. 2 i 14 rozporządzenia KRI.
9. Wskazanie w ewidencji osób upoważnionych do przetwarzania danych osobowych elementów określonych w art. 39 ust. 1 pkt 3 ustawy o ochronie danych osobowych oraz ujęcie w niej pracowników Powiatowego Urzędu Pracy w Sokółce, upoważnionych przez Kierownika MGOPS.
10. Aktualizację Polityki bezpieczeństwa oraz Instrukcji, w tym uzupełnienie ich stosownie do wymogów § 20 ust. 1 rozporządzenia KRI oraz § 4 pkt 3 i 4 i § 5 pkt 1 i 4 rozporządzenia w sprawie dokumentacji oraz warunków technicznych.
11. Nadanie dwóm osobom upoważnień do przetwarzania danych osobowych w zbiorze o nazwie: Ustawa o wsparciu kobiet w ciąży i ich rodzin „Za życiem".
12. Zlecanie przeglądów technicznych sprzętu informatycznego, zgodnie z § 5 Instrukcji.
13. Udzielenie zdalnego dostępu do zasobów sieciowych firmie serwisującej składniki systemu pod pełną kontrolą administratora systemu.

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.

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

Obowiązek poinformowania NIK o sposobie wykorzystania uwag i wykonania wniosków

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

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

Białystok, dnia 26 lutego 2018 r.

Kontroler
Joanna Muszyńska
specjalista kontroli państwowej

.....
podpis

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

.....
podpis