NAJWYŻSZA IZBA KONTROLI
Delegatura w Białymstoku

LBI.411.001.05.2017
R/17/001

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	R/17/001 – 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/38/2017 z 2 marca 2017 r. Paweł Tołwiński – starszy inspektor kontroli państwowej, upoważnienie do kontroli nr LBI/44/2017 z 28 marca 2017 r. (dowód: akta kontroli str. 1-4)
Jednostka kontrolowana	Gminny Ośrodek Pomocy Społecznej w Rudce, 17-132 Rudka, ul Brańska 13 (dalej: GOPS lub Ośrodek)
Kierownik jednostki kontrolowanej	Halina Boratyńska, kierownik Ośrodka[1] (dowód: akta kontroli str. 5)

II. Ocena kontrolowanej działalności[2]

Ocena ogólna

Ośrodek w okresie objętym kontrolą[3], nie podejmował wszystkich działań wymaganych przepisami prawa oraz regulacjami wewnętrznymi, zmierzających do zapewnienia ochrony posiadanych zasobów informacyjnych, co obniżało poziom ich bezpieczeństwa.

Uzasadnienie oceny ogólnej

Zarządzanie informacjami określonymi w ustawie z dnia 29 sierpnia 1997 r. o ochronie danych osobowych[4] (dalej: uodo) oraz zarządzanie bezpieczeństwem, o którym mowa w rozporządzeniu Rady Ministrów z dnia 12 kwietnia 2012 r. w sprawie Krajowych Ram Interoperacyjności, minimalnych wymagań dla rejestrów publicznych i wymiany informacji w postaci elektronicznej oraz minimalnych wymagań dla systemów teleinformatycznych[5] (dalej: rozporządzenie KRI) było nierzetelne, bowiem:

- nie dopełniono obowiązku zgłoszenia zmian w rejestrze prowadzonym przez GIODO[6],
- w załączniku do Polityki Bezpieczeństwa (dalej: PB) zamieszczono nierzetelne informacje o prowadzonych zbiorach danych osobowych,
- obowiązująca do 24 listopada 2016 r. PB[7] nie zawierała części wymaganych elementów,
- nierzetelnie prowadzono ewidencję osób upoważnionych do przetwarzania danych, w której nie wykazano pracowników Powiatowego Urzędu Pracy w Bielsku Podlaskim (dalej: PUP) upoważnionych przez kierownika GOPS do przetwarzania danych osobowych,
- nie zobowiązano do zachowania poufności podmiotów i osób świadczących pomoc w zakresie usuwania awarii sprzętu komputerowego wykorzystywanego od przetwarzania danych osobowych w Ośrodku,
- nie przeprowadzano inwentaryzacji składników sprzętu komputerowego i zainstalowanego na nim oprogramowania,

---

1 Od 24 listopada 1993 r.

2 Najwyższa Izba Kontroli stosuje 3-stopniową skalę ocen: pozytywna, pozytywna mimo stwierdzonych nieprawidłowości, negatywna. Jeżeli sformułowanie oceny ogólnej według proponowanej skali byłoby nadmiernie utrudnione albo taka ocena nie dawałaby prawdziwego obrazu funkcjonowania kontrolowanej jednostki w zakresie objętym kontrolą, stosuje się ocenę opisową bądź uzupełnia ocenę ogólną o dodatkowe objaśnienie.

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

4 Dz. U. 2016 r. poz. 922.

5 Dz. U. z 2016 r. poz. 113, ze zm.

6 Generalnego Inspektora Ochrony Danych Osobowych.

7 Wprowadzona zarządzeniem kierownika GOPS z 15 stycznia 2007 r.

– wszystkim użytkownikom komputerów nadano uprawnienia administratora w systemie operacyjny tych urządzeń,
– nie sporządzano kopii danych przetwarzanych w Ośrodku z częstotliwością określoną w przyjętych regulacjach wewnętrznych,
– korzystano z łącza internetowego Urzędu Gminy w Rudce, które nie zapewniało możliwości szyfrowania danych przesyłanych w sieci publicznej, a zatem właściwej ich ochrony.

III. Opis ustalonego stanu faktycznego

1. Dokumentacja i procedury dotyczące ochrony danych

Opis stanu faktycznego

1.1. Dokumentacja dotycząca ochrony danych osobowych

Zadania z zakresu pomocy społecznej w Gminie Rudka realizował Gminny Ośrodek Pomocy Społecznej w Rudce, w którym (według stanu na 6 marca 2017 r.) zatrudniano cztery osoby, tj. kierownika, dwóch pracowników socjalnych oraz pracownika wykonującego obowiązki głównej księgowej i referenta ds. świadczeń rodzinnych. Zgodnie z § 4 ust. 2 Regulaminu organizacyjnego GOPS[8], administratorem danych osobowych był kierownik GOPS. (dowód: akta kontroli str. 6-30)

Do dnia kontroli nie skorzystano z możliwości powołania Administratora Bezpieczeństwa Informacji (dalej: ABI), o którym mowa w art. 36a ust. 1 uodo. Kierownik Ośrodka wyjaśniła, że „(…) budżet gminy Rudka objęty jest planem naprawczym", a w związku z tym „(…) brak jest środków na zatrudnienie". Dodała też, że planowane jest utworzenie wspólnego stanowiska ABI do obsługi Ośrodka i Urzędu Gminy. (dowód: akta kontroli str. 32)

W GOPS prowadzono ewidencję osób upoważnionych do przetwarzania danych osobowych, zawierającą wszystkie elementy określone w art. 39 ust. 1 uodo. Z ewidencji wynika, że upoważnienia te nadano[9] wszystkim trzem pracownikom Ośrodka uczestniczącym w procesie przetwarzania danych osobowych w stopniu adekwatnym do zadań wynikających z ich zakresów obowiązków. Nie uwzględniono jednak trzech pracowników PUP, których upoważniono do przetwarzania danych osobowych beneficjentów Ośrodka, udostępnianych na platformie SEPI[10], co opisano w punkcie 2 wystąpienia pokontrolnego. (dowód: akta kontroli str. 45, 60-62, 268)

Kierownik GOPS wyjaśniła, że upoważnienia nadano pracownikom bezpośrednio po ich zatrudnieniu i przeszkoleniu, tj. odpowiednio w latach 2007, 2012 i 2013, zaś data obecnych upoważnień jest tożsama z datą aktualizacji PB. (dowód: akta kontroli str. 36, 63-65)

Ośrodek (w listopadzie 2016 roku) dokonał analizy poufności, integralności i rozliczalności systemów informatycznych pod kątem zagrożeń i ryzyka, co opisano w punkcie 4 wystąpienia. W załączniku nr 7 do ww. dokumentu opisano procedurę kontroli podatności systemu, w której określono zakres przedmiotowy i podmiotowy badań oraz metodykę prowadzenia czynności kontrolnych. Od 24 listopada 2016 r.[11] do 16 marca 2017 r. w GOPS nie przeprowadzano kontroli w sposób określony ww. załączniku.
(dowód: akta kontroli str. 83-84)

Kierownik Ośrodka wyjaśniła, że spiętrzenie obowiązków w końcu roku uniemożliwiło przeprowadzenie takiej kontroli, która planowana jest do przeprowadzenia w najbliższym czasie. (dowód: akta kontroli str. 31-38)

W załączniku do PB zawarto wykaz 20 zbiorów danych prowadzonych w Ośrodku w wersji papierowej i elektronicznej, przy czym zbiór danych „Zespół interdyscyplinarny" ujęto dwukrotnie. Informacje o aktualności prowadzonych zbiorów przedstawiono w punkcie

[8] Wprowadzony zarządzeniem Nr 1/2013 kierownika Gminnego Ośrodka Pomocy Społecznej z dnia 31 stycznia 2013 r.
[9] W dniu 24 listopada 2016 r.
[10] Samorządowa Elektroniczna Platforma Informacyjna (dalej: SEPI).
[11] Data zatwierdzenia dokumentu „Analizy poufności, integralności i rozliczalności systemów pod kątem zagrożeń i ryzyka".

2 wystąpienia. Wykaz ten (do dnia kontroli) nie został zaktualizowany o nowy zbiór danych przetwarzanych w GOPS, dotyczący „Wsparcia kobiet w ciąży i rodzin Za życiem", co opisano w dalszej części wystąpienia, w sekcji „Ustalone nieprawidłowości".

(dowód: akta kontroli str. 47-48)

W rejestrze zbiorów danych[12], prowadzonym przez GIODO, ujęto siedem zbiorów zawierających dane osób korzystających ze świadczeń pomocy społecznej w gminie Rudka. Według stanu na 8 marca 2017 r. administratorem ww. danych w jednym przypadku był kierownik GOPS (dotyczyło to zbioru „Świadczenia wychowawcze 500 plus[13]"), a zgromadzonych w sześciu zbiorach[14] – Wójt Gminy Rudka (cztery zbiory zarejestrowano w 2001 roku i dwa w 2011 roku). Do dnia kontroli nie występowano z wnioskami o wprowadzenie zmian w rejestrze. Do GIODO 15 czerwca 2016 r. i 3 marca 2017 r. przesłano wnioski zgłoszeniowe dotyczące zbiorów odpowiednio: „Karta Dużej Rodziny" i „Wsparcie kobiet w ciąży i rodzin Za życiem", które do dnia kontroli NIK nie zostały umieszczone w rejestrze, chociaż wnioski w tych sprawach sporządzono w formie określonej w art. 41 ust. 1 uodo. Do 30 marca 2017 r. GIODO nie odmówił rejestracji i nie wydał decyzji o wyrejestrowaniu zbiorów Ośrodka. Spośród zbiorów wyszczególnionych w załączniku do PB (do dnia kontroli) nie zgłoszono do GIODO zbioru „Ewidencja korespondencji" prowadzonego w wersji elektronicznej. Przyczyny niezaktualizowania w PB wykazu zbiorów danych oraz nie zgłoszenia do GIODO jednego zbioru, opisano w dalszej części wystąpienia, w sekcji „Ustalone nieprawidłowości".

(dowód: akta kontroli str. 88-184)

W realizacji bieżących zadań Ośrodek wykorzystywał trzy systemy dziedzinowe firmy Top Team TT Sp. z o.o. z siedzibą w Warszawie (dalej: TOP TEAM), obsługujące obszary: Pomoc społeczna[15], Świadczenia rodzinne[16] i Fundusz Alimentacyjny[17]. W kwietniu 2016 roku ww. firma dostarczyła aplikację „Świadczenia wychowawcze" do obsługi wypłat w ramach Programu 500 plus. Programy dziedzinowe GOPS (od 28 marca 2014 r.) powiązane były z platformą komunikacyjną Centralnego Systemu Informatycznego Zabezpieczenia Społecznego Emp@tia (dalej: CSIZS). Ośrodek korzystał też z oprogramowania interfejsowego[18] „Płatnik", a operacje finansowo-księgowe obsługiwał moduł oprogramowania „Księgowość Budżetowa", którego głównym użytkownikiem był Urząd Gminy w Rudce. GOPS korzystał też z systemu „Elektroniczne Zarządzanie Dokumentami" (dalej: EZD) służącego do wewnętrznego obiegu i archiwizowania dokumentów wytworzonych w formie elektronicznej. Na podstawie umowy PUP od 1 stycznia 2014 r. udostępniał Ośrodkowi dane osobowe w systemie SEPI, w celu przeglądania, utrwalania papierowego i archiwizowania. Szczegóły dotyczące funkcjonalności poszczególnych systemów opisano w punkcie 2 wystąpienia.

(dowód: akta kontroli str. 230-244, 246-284, 292-313)

W Ośrodku nie powołano Administratora Systemów Informatycznych odpowiedzialnego za zapewnienie bezpieczeństwa i ciągłość działania systemów informatycznych oraz sprawne realizowanie procedur tworzenia kopii zapasowych. Kierownik Ośrodka wyjaśniła, że administratora tego nie powołano ze względu na brak środków ten cel. Dodała, że planowane jest zatrudnienie osoby, która będzie obsługiwać Urząd Gminy i Ośrodek. Wyjaśniła też, że nadzór nad programami dziedzinowymi prowadzi zewnętrzna firma TOP TEAM, która odpowiada za bezpieczeństwo systemu informatycznego, ciągłość jego działania oraz sprawne realizowanie procedur tworzenia kopii zapasowych. W ramach

---

12 https://egiodo.giodo.gov.pl/search_basic.dhtml.

13 Zbiór zarejestrowany 23 listopada 2016 r.

14 Rejestr świadczeniobiorców Gminnego Ośrodka Pomocy Społecznej (nr księgi 044413), Rejestr zasiłków dla kombatantów (nr księgi 044417), Rejestr zasiłków rodzinnych i pielęgnacyjnych (nr księgi 044414), Ewidencja osób pobierających dodatki mieszkaniowe (nr księgi 034683), Rejestr osób dotkniętych przemocą w rodzinie i osób stosujących przemoc w rodzinie (nr księgi 102136), Rejestr świadczeniobiorców z zakresu świadczeń z funduszu alimentacyjnego (nr księgi 103521).

15 Wersja oprogramowania GP-1.03-04 eksploatowana od 6 grudnia 2002 r.

16 Wersja oprogramowania G-1.01-2-01 eksploatowana od 26 kwietnia 2004 r.

17 Wersja oprogramowania TT-Alimenty 6.0.1 eksploatowana od 10 października 2008 r.

18 Oprogramowanie umożliwiające łączenie i wymianę danych w komunikacji pomiędzy systemami teleinformatycznymi.

umowy, co miesiąc opłacano faktury za nadzór nad programem. Istniała też możliwość zdalnego łączenia się z informatykiem TOP TEAM. Kierownik GOPS dodała, że w 2016 roku nie wystąpiły techniczne awarie komputerów. Wskazała też, że w przypadku zaistnienia takich okoliczności naprawę zleci wyspecjalizowanej firmie, która zrealizuje ją na miejscu w Ośrodku. (dowód: akta kontroli str. 38)

Z umów[19] z firmą TOP TEAM wynika, że Ośrodek zobowiązany jest eksploatować oprogramowanie zgodnie z dokumentacją użytkowania oraz niezwłocznie informować o wszystkich zaistniałych usterkach. GOPS nie posiadał dokumentacji potwierdzającej informowanie o takich przypadkach. Za świadczone usługi wypłacano zryczałtowane wynagrodzenie wg. ustalonych stawek (aktualizowanych aneksami do umów). Od 1 stycznia 2016 r. do 28 lutego 2017 r. ww. firmie zapłacono 4.501 zł.

(dowód: akta kontroli str. 185, 292-313)

Kierownik Ośrodka wyjaśniła, że usterki systemów dziedzinowych zgłaszano telefonicznie, natomiast ich usunięcie bądź naprawa wykonywana była za pomocą zdalnego połączenia, co szerzej opisano w pkt 3 wystąpienia. (dowód: akta kontroli str. 31-38)

Dwóch pracowników socjalnych GOPS zostało przeszkolonych w zakresie przetwarzania informacji. Osoby te odbyły szkolenia: „Praktyczne wykorzystanie nowoczesnych systemów teleinformatycznych (ICT) w zakresie zarządzania dokumentami i sprawami”[20] oraz „System wymiany informacji o dłużnikach, jako wsparcie dla gmin w walce z dłużnikami alimentacyjnymi”[21]. (dowód: akta kontroli str. 186-190)

Kierownik Ośrodka wyjaśniła, że w zakresie ochrony danych, pracowników przeszkolono bezpośrednio przed zatrudnieniem. Dodała, że podczas wdrażania systemów dostawcy oprócz szkolenia w zakresie obsługi programów, zwracali uwagę na sposób ochrony i przetwarzania danych. Wyjaśniła również, że pomimo zgłoszenia (28 marca 2014 r.) do chwili obecnej nikt nie został przeszkolony w zakresie obsługi portalu Emp@tia. Dodała, że w marcu 2017 roku zgłoszono dwóch pracowników do przeszkolenia w zakresie „Przeprowadzanie wywiadów środowiskowych w formie elektronicznej. Obsługa, działanie systemu TOP TEAM na terminalach mobilnych”. (dowód: akta kontroli str. 191-195)

Zgodnie z § 10 umowy Nr 7/2013 w sprawie udostępniania danych osobowych[22], inspektor PUP 10 marca 2017 r. skontrolowała w Ośrodku prawidłowość zabezpieczenia danych osobowych udostępnianych za pośrednictwem SEPI. Z protokołu wynika, że nieprawidłowości w tym zakresie nie stwierdzono. (dowód: akta kontroli str. 196)

W okresie objętym kontrolą Wojewoda Podlaski (na podstawie art. 25 ust. 1 pkt 3 lit. a ustawy z dnia 17 lutego 2005 r. o informatyzacji podmiotów realizujących zadania publiczne[23]) nie kontrolował w Ośrodku działania systemów teleinformatycznych oraz rejestrów publicznych, które używano do realizacji zadań zleconych z zakresu administracji rządowej (np. przy przyznaniu i wypłacie świadczeń z funduszu alimentacyjnego[24], udzielaniu świadczeń wychowawczych[25], nadawaniu uprawnień wynikających z Karty Dużej Rodziny[26], itp.).

---

[19] Umowy zawarte 1 marca 2008 r., 10 października 2008 r. i 1 kwietnia 2016 r. pomiędzy GOPS a TOP TEAM na sprawowanie nadzoru autorskiego uproszczonego odpowiednio nad programami „Świadczenia Rodzinne”, „TT-Fundusz Alimentacyjny”, „Świadczenia Wychowawcze (500 plus)”.

[20] Szkolenie odbyło się od 2 do 12 kwietnia 2007 r.

[21] Szkolenie odbyło się 4 marca 2009 r.

[22] Umowa zawarta w listopadzie 2013 roku.

[23] Dz. U. z 2014 r. poz. 1114, ze zm.

[24] Zgodnie z art. 31 ust. 1 ustawy z dnia 7 września 2007 r. o pomocy osobom uprawnionym do alimentów (Dz. U. z 2017 r. poz. 489), przyznanie i wyplata świadczeń z funduszu alimentacyjnego oraz podejmowanie działań wobec dłużników jest zadaniem zleconym gminie z zakresu administracji rządowej, finansowanym w formie dotacji celowej z budżetu państwa.

[25] Zgodnie z art. 29 ustawy z dnia 11 lutego 2016 r. o pomocy państwa w wychowaniu dzieci (Dz. U. z 2016 r. poz. 195, ze zm.), realizowanie zadań z zakresu świadczenia wychowawczego jest zadaniem zleconym z zakresu administracji rządowej. Świadczenie wychowawcze i koszty jego obsługi są finansowane w formie dotacji celowej z budżetu państwa.

[26] Zgodnie z art. 29 ustawy z dnia 5 grudnia 2014 r. o Karcie Dużej Rodziny (Dz. U. z 2016 r. poz. 785, ze zm.), realizacja zadań związanych z przyznaniem Karty należy do zadań z zakresu administracji rządowej. Koszt realizacji ustawy jest finansowany z budżetu państwa.

W teczce 051 „Skargi i wnioski" rejestru EZD nie odnotowano skarg dotyczących nieuprawnionego ujawnienia danych osobowych. (dowód: akta kontroli str. 197)

Ustalone nieprawidłowości

W działalności kontrolowanej jednostki w przedstawionym wyżej zakresie stwierdzono nieprawidłowość, polegającą na niezgłoszeniu GIODO zmiany oznaczenia administratora danych przetwarzanych w Ośrodku. W sześciu spośród siedmiu zarejestrowanych zbiorów[27] zgłoszono Wójta Gminy Rudka jako administratora danych osób korzystających z pomocy społecznej w GOPS. Zgodnie art. 7 pkt 4 uodo, administratorem danych jest jednak jednostka organizacyjna, która decyduje o celach i środkach przetwarzania danych osobowych. W myśl 41 ust. 2 uodo, każda zmiana informacji powinna być zgłoszona GIODO w terminie 30 dni od dnia dokonania zmiany w zbiorze danych.

Wójt Gminy Rudka wyjaśnił, że zgłaszając wnioski GIODO uważano, iż Gmina jest administratorem danych wszystkich jednostek organizacyjnych, w tym także GOPS. Dodał, iż w związku z brakiem świadomości popełnionego błędu nie dokonano aktualizacji.

Kierownik Ośrodka wyjaśniła, że: „Od początku utworzenia GOPS i UG nie było wyraźnej rozdzielczości między tymi instytucjami. Wszystkie działania były podejmowane w ścisłej współpracy z Gminą. Wcześniej zgłoszone zbiory przez Gminę w wyniku przeprowadzonej konsultacji w Wójtem zostaną poddane korekcie". (dowód: akta kontroli str. 31-38, 198-199)

1.2. Dokumentacja dotycząca warunków technicznych i organizacyjnych, jakim powinny odpowiadać urządzenia i systemy informatyczne

Opis stanu faktycznego

Do 24 listopada 2016 r. w Ośrodku obowiązywała PB[28], która nie zawierała elementów określonych w § 4 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[29] (dalej: rozporządzenie MSWiA). Nie uwzględniała ona pełnego wykazu zbioru danych przetwarzanych w GOPS (wyszczególniono cztery zbiory), nie definiowała sposobu przepływu danych pomiędzy poszczególnymi systemami (pomimo korzystania z możliwości pobierania informacji za pośrednictwem SEPI, portalu Emp@tia oraz EZD Urzędu Gminy w Rudce). Nie określała też rozwiązań organizacyjnych związanych z możliwością przetwarzania danych na mobilnym urządzeniu (tj. tablecie dostarczonym do Ośrodka[30] w ramach realizacji projektu Emp@tia – „Platforma komunikacyjna obszaru zabezpieczenia społecznego"). Wprawdzie zaktualizowana PB[31] odpowiadała wymogom § 4 rozporządzenia MSWiA, w tym wskazywała miejsce, przetwarzania danych oraz sposób ich zabezpieczeń, to jednak do 16 marca 2017 r.:

- w wykazie zbiorów zamieszczonym w PB nie uwzględniono zbioru „Wsparcie kobiet w ciąży i rodzin Za życiem",
- zamieszczono w niej nieadekwatne opisy danych gromadzonych w zbiorach[32] w stosunku do przetwarzanych w systemie (np. w opisie zbioru „Ewidencja klientów pomocy społecznej" wskazano na 35 różnych rodzajów danych spośród 54 wymaganych przez system TT-Pomoc, w opisie zbioru „Świadczenia wychowawcze 500 plus" wskazano na 14 rodzajów danych spośród 42 wymaganych w systemie, a w opisie zbioru „Fundusz Alimentacyjny" podano 24 rodzaje danych z 35 wymaganych w systemie),

[27] Cztery zarejestrowano w 2001 roku i dwa w 2011 roku.

[28] Wprowadzona zarządzeniem kierownika GOPS z 15 stycznia 2007 r.

[29] Dz. U. Nr 100, poz. 1024, ze zm.

[30] Na podstawie umowy użyczenia Nr 25/20/EMP/2013, zawartej 23 grudnia 2013 r. pomiędzy Ministerstwem Pracy i Polityki Społecznej a GOPS. Według § 1 ust. 2 wartość tabletu wynosi 1.469,28 zł.

[31] Wprowadzona zarządzeniem nr 2/2016 kierownika GOPS z dnia 24 listopada 2016 r.

[32] Zgodnie z § 4 pkt 3 rozporządzenia dla każdego zidentyfikowanego zbioru danych powinien być wskazany opis jego struktury i zakres informacji w nim gromadzonych. Opisy poszczególnych pól informacyjnych w strukturze zbioru danych powinny jednoznacznie wskazywać, jakie kategorie danych są w nich przechowywane. Opis pola danych, gdy możliwa jest niejednoznaczna interpretacja jego zawartości, powinien wskazywać kategorię danych, ale również format jej zapisu i/lub znaczenie określone w danym kontekście.

– PB nie określała sposobu przepływu danych[33] pomiędzy wewnętrznymi systemami Ośrodka oraz zewnętrznymi, chociaż korzystano z informacji pobieranych za pośrednictwem platformy Emp@tia, SEPI, EZD Urzędu Gminy Rudka. Zawierała jedynie zapisy „ewidencja papierowa – wydruk danych" lub „brak przepływu", co opisano w dalszej części wystąpienia pokontrolnego, w sekcji „Ustalone nieprawidłowości".

(dowód: akta kontroli str. 39-62)

W Instrukcji Zarządzania Systemem Informatycznym[34] (dalej: IZSI), sporządzonej zgodnie z wymogami § 5 ww. rozporządzenia MSWiA, określono „wysoki" poziom bezpieczeństwa przetwarzania danych osobowych w systemach informatycznych Ośrodka (ze względu na połączenie komputerów z siecią publiczną). Badanie sposobu przetwarzania danych za pomocą programów „Świadczenia rodzinne „i „TT-Pomoc" wykazało, że witryny internetowe tych programów (generowane za pomocą przeglądarki internetowej Mozilla Firefox) umożliwiające dostęp do tych programów, nie obsługują szyfrowania, co opisano w pkt 4 wystąpienia pokontrolnego. (dowód: akta kontroli str. 56-59, 212, 216-218,221)

Systemy informatyczne przetwarzające dane osobowe w Ośrodku zapewniały realizację wymogów określonych w § 7 ust. 3 rozporządzenia MSWiA, tj. umożliwiały sporządzenie i wydrukowanie raportu zawierającego w powszechnie zrozumiałej formie informacje dotyczące m.in. daty pierwszego wprowadzenia danych osobowych i identyfikatora użytkownika wprowadzającego dane do systemu. (dowód: akta kontroli str. 200-205)

Ustalone nieprawidłowości

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

1. W obowiązującej do 24 listopada 2016 r. PB nie zamieszczono pełnego wykazu zbioru danych przetwarzanych w GOPS, nie zdefiniowano sposobu przepływu danych pomiędzy poszczególnymi systemami oraz nie ustalono rozwiązań organizacyjnych związanych z możliwością przetwarzania danych na mobilnym urządzeniu, co było niezgodne z wymogami § 4 pkt 2, 4 i 5 rozporządzenia MSWiA.
2. Obowiązująca w czasie kontroli PB zawierała nieadekwatne opisy danych gromadzonych w zbiorach oraz nie określała sposobu przepływu danych pomiędzy systemami, co było sprzeczne z § 4 pkt 3 i 4 rozporządzenia MSWiA.

   Kierownik Ośrodka wyjaśniła, że wynikało to z nieuwzględniania w całości informacji zawartych w tych systemach, co w najbliższym czasie zostanie uzupełnione.

   (dowód: akta kontroli str. 39-62, 206-207)

Ocena cząstkowa

Ośrodek posiadał wymaganą dokumentację opisującą procedury ochrony danych, jednak przyjęte w niej rozwiązania nie w pełni odpowiadały wymogom określonym w § 4 rozporządzenia MSWiA. Nie dopełniono też obowiązku zgłoszenia do GIODO zmian w oznaczeniu podmiotu będącego administratorem danych przetwarzanych w Ośrodku oraz potrzeby aktualizacji prowadzonych rejestrów w zakresie wykreślenia nieprowadzonych zbiorów, zarejestrowania nowych oraz uzupełnienia informacji o podmiotach przetwarzających dane.

[33] Przepływ danych jest to sposób współpracy pomiędzy różnymi systemami informatycznymi oraz relacje, jakie istnieją pomiędzy danymi zgromadzonymi w zbiorach, do przetwarzania których systemy te są wykorzystywane. Sposób przepływu wskazuje na zakres przesyłanych danych, podmiotu lub kategorii podmiotów, do których są one przekazywane oraz ogólnych informacji na temat sposobów ich przesyłania (Internet, poczta elektroniczna, inne rozwiązania).

[34] Instrukcja zawiera: [1] procedurę nadawania uprawnień do przetwarzania danych i rejestrowania tych uprawnień w systemie informatycznym oraz wskazanie osoby odpowiedzialnej za te czynności, [2] stosowane metody i środki uwierzytelnienia, [3] procedurę rozpoczęcia, zawieszenia i zakończenia pracy przeznaczone dla użytkowników systemu, [4] procedurę tworzenia kopii zapasowych zbiorów danych oraz programów i narzędzi programowych służących do ich przetwarzania, [5] sposób, miejsce i okres przechowywania elektronicznych nośników informacji zawierających dane osobowe oraz kopii zapasowych, [6] sposób zabezpieczenia systemu informatycznego przed działalnością oprogramowania, którego celem jest uzyskanie nieuprawnionego dostępu do systemu informatycznego, [7] procedurę wykonywania przeglądów i konserwacji systemów oraz nośników informacji

2. Zakres przetwarzanych zasobów informacyjnych

Opis stanu faktycznego

Według stanu na 8 marca 2017 r. Ośrodek dysponował trzema informatycznymi systemami dziedzinowymi[35], tj.:

- „TT-Pomoc", służącym do realizacji zdań z zakresu pomocy społecznej[36], w tym ewidencjonowania klientów pomocy społecznej, rejestracji wniosków, wprowadzania danych z wywiadów środowiskowych, tworzenia decyzji, rejestracji pracy socjalnej, tworzenia: list wypłat zasiłków, sprawozdań, wydruków zbiorczych, zaświadczeń,
- „Świadczenia Rodzinne" za pomocą tego programu rejestrowano wnioski, wydawano decyzje, naliczano świadczenia[37] oraz tworzono listy wypłat, sprawozdania, wydawano zaświadczenia,
- „Fundusz Alimentacyjny", służący do rejestracji wierzycieli, sporządzania listy dłużników, rejestracji wniosków, wydawania decyzji, ewidencji długu, tworzenia list wypłat świadczeń alimentacyjnych oraz tworzenia sprawozdań.

Ośrodek uzyskał też dostęp do baz danych upublicznianych na portalu Emp@tia, w celu weryfikacji informacji lub pobierania niezbędnych danych osobowych. W programach (firmy TOP TEAM) zainstalowano funkcjonalność automatycznie łączącą z ww. portalem (bez potrzeby uwierzytelniania użytkownika). Umożliwiała ona pobranie informacji z systemów obsługujących Urzędy Skarbowe, Zakład Ubezpieczeń Społecznych, Powszechny Elektroniczny System Ewidencji Ludności, Elektroniczny Krajowy System Monitoringu Orzekania o Niepełnosprawności, Krajowy Rejestr Sądowy, Centralną Bazę Beneficjentów, Centralną Ewidencję Informacji o Działalności Gospodarczej (dalej: CEIDG). Za pośrednictwem ww. portalu istniała też możliwość zgłaszania dłużników do Krajowego Rejestru Długów BIG S.A i Rejestru dłużników ERIF.

Ośrodek dysponował programem interfejsowym „Płatnik", który zapewniał pełną obsługę dokumentów ubezpieczeniowych i wymianę informacji z ZUS klientów Ośrodka, w tym: automatyczne wykorzystanie danych do przygotowania dokumentów ubezpieczeniowych, weryfikację dokumentów ubezpieczeniowych oraz przygotowanie raportu o wynikach weryfikacji, wyliczanie wartości w poszczególnych dokumentach rozliczeniowych, wyświetlanie zawartości elektronicznych dokumentów ubezpieczeniowych, drukowanie dokumentów zgłoszeniowych i rozliczeniowych, drukowanie przelewów bankowych i dokumentów wpłaty, przygotowywanie przelewów bankowych w formie pliku tekstowego, automatyczne tworzenie i drukowanie raportów miesięcznych i rocznych dla ubezpieczonego, wysyłkę i potwierdzenie zestawów dokumentów, itp. Korzystano też z programu „Księgowość budżetowa" z modułem Kadry i Płace – służącym do ewidencjonowania przebiegu operacji gospodarczych w Ośrodku, obsługi zatrudniania pracowników oraz ich wynagradzania, a także sporządzania sprawozdawczości budżetowej.
(dowód: akta kontroli str. 208-244, 292-313)

Za pośrednictwem strony Internetowej https://kdr.mpips.gov.pl/start/, Ośrodek posiadał też dostęp do Systemu Informatycznego Karty Dużej Rodziny (dalej: SI KDR), służącego do rejestracji i obsługi wniosków, wydawania decyzji odmownych, zamówienia, odbioru i zarządzania kartami, złożenia i zarządzania reklamacjami oraz tworzenia sprawozdań.

---

[35] Programy te posiadają świadectwa zgodności, o których mowa w § 6 ust. 2 rozporządzenia Ministra Pracy i Polityki Społecznej z dnia 2 listopada 2007 r. w sprawie systemów teleinformatycznych stosowanych w jednostkach organizacyjnych pomocy społecznej (Dz. U. Nr 216, poz. 1609).

[36] Realizacja zadań polega na wypłacie zasiłków: okresowych, stałych, celowych, celowych specjalnych, udzielania pomocy w zakresie dożywiania, w tym wypłaty świadczeń na zakup żywności, kierowania do domów pomocy społecznej, sprawiania pogrzebów, świadczenie usług opiekuńczych, opłacania składek na ubezpieczenie zdrowotne.

[37] Świadczenia rodzinne związane są z wypłatą: [1] zasiłków pielęgnacyjnych, [2] świadczeń pielęgnacyjnych, [3] specjalnych zasiłków opiekuńczych, [4] zasiłków dla opiekuna, [5] świadczenia rodzicielskiego, [6] świadczenia wychowawczego 500 plus, [7] jednorazowej zapomogi w tytułu urodzenia dziecka, [8] zasiłków rodzinnych wraz z następującymi dodatkami: z tytułu urodzenia dziecka, opieki nad dzieckiem w okresie korzystania z urlopu wychowawczego, samotnego wychowania dziecka, wychowywania dziecka w rodzinie wielodzietnej, kształcenia i rehabilitacji dziecka niepełnosprawnego, rozpoczęcia roku szkolnego, podjęcia przez dziecko nauki w szkole poza miejscem zamieszkania, z tego: na częściowe pokrycie wydatków związanych z zamieszkiwaniem w miejscowości, w której znajduje się siedziba szkoły oraz na pokrycie wydatków związanych z zapewnieniem dziecku możliwości dojazdu z miejsca zamieszkania do miejscowości, w której znajduje się siedziba szkoły.

W tym systemie funkcjonowała skrzynka odbiorcza za pośrednictwem, której można było odbierać wnioski złożone w formie elektronicznej. Ośrodek dysponował też systemem EZD, który pozyskano w związku z przystąpieniem Gminy Rudka do realizacji Projektu „Wdrażanie elektronicznych usług dla ludności województwa podlaskiego", realizowanego w ramach Regionalnego Programu Operacyjnego Województwa Podlaskiego. W Ośrodku użyczony moduł tej aplikacji służył do wewnętrznej obsługi kancelaryjnej, tj. rejestracji dokumentów, ewidencji, obiegu korespondencji przychodzącej, zakładania i prowadzenia spraw. Umożliwiał też korzystanie z poczty elektronicznej.

(dowód: akta kontroli str. 208-244, 292-313)

Powyższe systemy umożliwiały gromadzenie danych w zbiorach prowadzonych w formie elektronicznej i papierowej. Spośród 20 zbiorów danych ujętych w wykazie, stanowiącym załącznik do PB, GIODO zgłoszono do zarejestrowania dziewięć, co opisano w pkt 1 niniejszego wystąpienia. Analiza aktualności zbiorów Ośrodka wykazała, że:

- spośród dziewięciu zgłoszonych zbiorów, nie prowadzono dwóch („Rejestr zasiłków dla kombatantów" oraz „Ewidencja osób pobierających dodatki mieszkaniowe"; odpowiednio księgi Nr 044417 i Nr 034683) i do 22 marca 2017 r. nie wystąpiono o ich wykreślenie,
- spośród 20 zbiorów ujętych ww. wykazie, nie prowadzono czterech,
- w wykazie dwukrotnie ujęto zbiór „Zespół interdyscyplinarny", który pod nazwą „Rejestr osób dotkniętych przemocą w rodzinie i osób stosujących przemoc w rodzinie" 5 października 2011 r. zarejestrowano w GIODO,
- nie zgłoszono GIODO zbioru danych przetwarzanych w systemie EZD,
- zakres przetwarzanych danych w czterech zbiorach[38] (spośród siedmiu zarejestrowanych) był zgodny z wnioskiem zgłoszeniowym do GIODO i był niezbędny do realizacji zadań z zakresu pomocy społecznej, przypisanych poszczególnym pracownikom Ośrodka,
- w zgłoszeniach do GIODO o rejestrację zbiorów „Karta Dużej Rodziny", „Świadczenia wychowawcze" oraz „Wsparcie kobiet w ciąży i rodzin Za życiem" wskazano, że będą przetwarzane następujące dane: imiona rodziców, miejsce urodzenia, miejsce pracy, wykształcenie. Przepisy regulujące obsługę tych świadczeń nie wymagają jednak takich danych. Nie wykazano natomiast pełnego, wymaganego zakresu danych.

Wymienione wyżej kwestie opisano też w dalszej części wystąpienia pokontrolnego, w sekcji „Ustalone nieprawidłowości". (dowód: akta kontroli str. 245)

Na podstawie umowy Nr 6/2011/SEPI w sprawie powierzenia przetwarzania danych osobowych, zawartej 14 grudnia 2011 r. z dyrektorem PUP[39], Ośrodek posiadał dostęp do bazy danych osobowych przetwarzanych na platformie SEPI. W załączniku nr 2 do umowy wyszczególniono zakres danych wzajemnie wymienianych. Do ich przetwarzania upoważniono dwóch pracowników Ośrodka i trzech z PUP, których nie ujęto w ewidencji upoważnionych prowadzonej w GOPS, co opisano w dalszej części wystąpienia w sekcji „Ustalone nieprawidłowości". (dowód: akta kontroli str. 39-53, 259, 276-291)

Kierownik GOPS 22 lutego 2017 r. zawarła też z firmą Sygnity S.A. z siedzibą w Warszawie umowę powierzenia przetwarzania danych osobowych. Z § 1 pkt 2 ww. umowy wynika, że podstawą jej zawarcia był fakt świadczenia przez ww. firmę usług na rzecz PUP. W umowie wskazano, że zawarto ją „(…) w celu zapewnienia bezpieczeństwa danych osobowych przetwarzanych w Systemie informatycznym" (§ 2 pkt 5 umowy). Zgodnie z § 10 umowy Ośrodek wyraził zgodę na przetwarzanie danych osobowych beneficjentów przez pięciu podwykonawców wykazanych w załączniku Nr 1 do umowy. Zakres udostępnianych danych wyszczególniono w załączniku Nr 2. Obejmował on 12 różnych informacji o beneficjentach pomocy społecznej i 20 informacji o osobach korzystających ze świadczeń

[38] „Rejestr świadczeniobiorców Gminnego Ośrodka Pomocy Społecznej", „Rejestr zasiłków rodzinnych i pielęgnacyjnych", „Rejestr osób dotkniętych przemocą w rodzinie i osób stosujących przemoc w rodzinie", „Rejestr świadczeniobiorców z zakresu świadczeń z funduszu alimentacyjnego",

[39] Kolejna umowa obowiązuje od 1 stycznia 2014 r.

rodzinnych. Do dnia kontroli NIK kierownik GOPS nie zgłosił do GIODO zmian w celu ujawnienia informacji o fakcie powierzenia przetwarzania danych dla PUP i firmy Sygnity S.A., co opisano w dalszej części wystąpienia pokontrolnego, w sekcji „Ustalone nieprawidłowości". (dowód: akta kontroli str. 246-284)

Do 30 marca 2017 r. nie zgłoszono GIODO zbioru „Ewidencja korespondencji", prowadzonego w GOPS (w wersji elektronicznej za pomocą programu EZD, który otrzymano z Urzędu Gminy w Rudce w grudniu 2014 roku), co opisano poniżej, w sekcji „Ustalone nieprawidłowości".

Ustalone nieprawidłowości

W działalności kontrolowanej jednostki w przedstawionym zakresie stwierdzono następujące nieprawidłowości:

1. Nie poinformowano GIODO o zaprzestaniu przetwarzania danych w dwóch zarejestrowanych zbiorach danych osobowych: „Ewidencja osób pobierających dodatki mieszkaniowe" i „Rejestr zasiłków dla kombatantów", w celu uzyskania decyzji o wykreśleniu tych zbiorów, czym naruszono art. 44a pkt 1 uodo.

   Kierownik Ośrodka wyjaśniła, że administratorem tych danych jest Wójt Gminy Rudka i w najbliższym czasie nastąpi korekta. (dowód: akta kontroli str. 88, 285-291)

2. Nie zgłoszono GIODO do rejestracji zbioru „Ewidencja korespondencji", przetwarzanego w Ośrodku za pomocą modułu EZD, wbrew art. 40 ust. uodo.

   Kierownik Ośrodka wyjaśniła, że zbioru tego nie zgłaszano, gdyż jest on prowadzony za pomocą modułu EZD, przekazanego z Urzędu. Uważano, że jest on jego administratorem. (dowód: akta kontroli str. 47-48, 88, 285-291)

3. W zgłoszeniach rejestracyjnych zbiorów: „Karta Dużej Rodziny", „Świadczenia wychowawcze" oraz „Wsparcie kobiet w ciąży i rodzin Za życiem" nie wykazano pełnego zakresu danych w nich gromadzonych, przewidzianego w obowiązujących przepisach[40], co było sprzeczne z art. 41 uodo.

   Kierownik Ośrodka wyjaśniła, że: „(…) rutynowo jak w poprzednich latach zaznaczyliśmy informacje, nie zwracając uwagi na niezbędność określoną w przepisach".
   (dowód: akta kontroli str. 153-174, 285-291)

4. Nie zgłoszono do GIODO aktualizacji zbioru „Rejestr świadczeniobiorców Gminnego Ośrodka Pomocy Społecznej" (nr księgi 044413) w zakresie powierzenia, na podstawie art. 31 ust. 1 uodo, przetwarzania danych osobowych PUP i firmie Sygnity S.A. Wymóg zgłoszenia do GIODO faktu powierzania przetwarzania danych w zbiorze wynika z art. 41 ust. 1 i 2 powołanej ustawy. Ponadto w prowadzonej przez Ośrodek ewidencji osób upoważnionych do przetwarzania danych osobowych, wbrew przepisom art. 39 ust. 1 uodo, nie ujęto informacji o trzech pracownikach PUP, którym Kierownik GOPS udzieliła upoważnienia do przetwarzania danych osobowych pochodzących z Ośrodka, w systemie SEPI.

   Kierownik Ośrodka wyjaśniła, że było to wynikiem przeoczenia. Wskazała też, że firmie tej nie przekazywano jeszcze żadnych danych.

   Oględziny wykazały, że w marcu 2017 roku za pośrednictwem portalu SEPI (obsługiwanego przez firmę Signity S.A.) przekazane zostały dane dotyczące świadczeń wypłaconych we wskazanym miesiącu przez GOPS.
   (dowód: akta kontroli str. 39-53, 259, 276-291)

5. W wykazie, stanowiącym załącznik do PB, ujęto cztery zbiory (tj. „Ewidencja zamówień publicznych", „Ewidencja dodatków energetycznych", „Ewidencja dodatków

[40] Art. 21 ust. 1 ustawy o Karcie Dużej Rodziny oraz w kwestionariuszach wniosków określonych odpowiednio: w załącznikach do rozporządzenia Ministra Rodziny, Pracy i Polityki Społecznej z dnia 18 lutego 2016 r. w sprawie sposobu i trybu postępowania w sprawach o świadczenie wychowawcze (Dz. U. z 2016 r. poz. 214) i w załączniku do rozporządzenia Ministra Rodziny, Pracy i Polityki Społecznej z dnia 21 grudnia 2016 r. w sprawie wzoru wniosku o jednorazowe świadczenie z tytułu urodzenia się dziecka, u którego zdiagnozowano ciężkie i nieodwracalne upośledzenie albo nieuleczalną chorobę zagrażającą życiu, które powstały w prenatalnym okresie rozwoju dziecka lub w czasie porodu (Dz. U. z 2016 r. poz. 2234).

mieszkaniowych", „Podania o pracę"), które nie były prowadzone w Ośrodku oraz dwukrotnie wykazano zbiór „Zespół interdyscyplinarny".

Kierownik Ośrodka wyjaśniła, że zbiory te omyłkowo zostały przepisane ze starej Polityki. (dowód: akta kontroli str. 47-48, 88, 285-291)

Uwagi dotyczące badanej działalności

Najwyższa Izba Kontroli zwraca uwagę, że dobrą praktyką byłaby aktualizacja zbioru „Rejestr świadczeniobiorców Gminnego Ośrodka Pomocy Społecznej", w zakresie wskazania pięciu podmiotów, którym w myśl umowy zawartej 22 lutego 2017 r. dokonano podpowierzenia przetwarzania danych osobowych. (dowód: akta kontroli str. 269-275)

Ocena cząstkowa

Zakres przetwarzanych danych w czterech zbiorach (spośród siedmiu) był zgodny z wnioskiem zgłoszeniowym do GIODO i był niezbędny w realizacji zadań z zakresu pomocy społecznej. Natomiast w zgłoszeniach rejestracyjnych zbiorów: „Karta Dużej Rodziny", „Świadczenia wychowawcze" oraz „Wsparcie kobiet w ciąży i rodzin Za życiem" nie wykazano pełnego zakresu danych w nich gromadzonych. Ponadto GIODO nie zgłoszono do zarejestrowania zbioru elektronicznego „Ewidencja korespondencji", w którym dane przetwarzano od ponad dwóch lat. Nie wywiązano się też z obowiązku poinformowania GIODO o zaprzestaniu przetwarzania danych w dwóch zarejestrowanych zbiorach oraz potrzebie ujawnienia w „Rejestrze świadczeniobiorców Gminnego Ośrodka Pomocy Społecznej" podmiotów, którym powierzono przetwarzanie danych.

3. Sposób przechowywania oraz fizycznego zabezpieczenia danych

Opis stanu faktycznego

Z wykazu, stanowiącego załącznik do PB wynika, że 20 zbiorów danych osobowych prowadzono w wersji papierowej, w tym dziewięć również z wykorzystaniem systemów elektronicznych. W rzeczywistości w formie elektronicznej prowadzono siedem zbiorów, gdyż Ośrodek od 2001 roku nie wykonywał zadań związanych z wypłatą zasiłków dla kombatantów, a od lipca 2011 roku – dodatków mieszkaniowych. Do 30 marca 2017 r. nie wnioskowano do GIODO o wykreślenie z rejestru ww. zbiorów (co opisano w punkcie 2 wystąpienia pokontrolnego).

Ośrodek zajmował dwa pokoje w budynku Urzędu Gminy w Rudce, które:

- były zabezpieczone drzwiami zwykłymi, zamykanymi na klucz,
- w oknach pomieszczeń nie było zainstalowanych krat, rolet lub folii antywłamaniowej,
- pokoje nie były wyposażone w system alarmowy przeciwwłamaniowy i nie były objęte systemem przeciwpożarowym (wyposażono je w dwie gaśnice proszkowe) oraz systemem kontroli dostępu i monitoringu z zastosowaniem kamer przemysłowych, a także nie były nadzorowane przez służbę ochrony.

W pokoju zajmowanym przez dwóch pracowników socjalnych i główną księgową zorganizowano miejsce do obsługi interesantów, którego usytuowanie wykluczało możliwość odczytania danych z ekranów komputerów zainstalowanych na stanowiskach roboczych. Analiza zastosowanych zabezpieczeń na komputerach Ośrodka wykazała, że:

- dostęp do systemów operacyjnych komputerów, na których przetwarzano dane osobowe był zabezpieczony indywidualnym loginem i hasłem o ilości i konfiguracji znaków zgodnej z wymogiem określonym w pkt IV ppkt 2 IZSI (hasło zawiera co najmniej 8 znaków, małe i wielkie litery, cyfry lub znaki specjalne),
- systemy operacyjne wyposażono w funkcjonalność wymuszającą zmianę haseł co 30 dni (istniała też możliwość zmiany hasła dostępowego w zależności od potrzeb użytkownika),
- zastosowany był mechanizm automatycznej blokady dostępu do systemu w przypadku dłuższej nieaktywności użytkownika, wymuszający potrzebę ponownego jego uwierzytelnienia,
- każdemu użytkownikowi nadano uprawnienia administratora systemu operacyjnego, co opisano w dalszej części wystąpienia w sekcji „Ustalone nieprawidłowości".

(dowód: akta kontroli str. 208-229, 314-315)

Kierownik Ośrodka nie upoważniała osób niebędących pracownikami GOPS do dostępu do danych osobowych przetwarzanych przez Ośrodek, z wyjątkiem trzech pracowników PUP, którzy korzystali poprzez portal internetowy https://sepi.sygnity.pl z informacji automatycznie przekazywanych na platformę SEPI. (dowód: akta kontroli str. 268)

W Ośrodku nie przeprowadzano inwentaryzacji zasobów informatycznych w celu ustalenia specyfikacji technicznej każdej ze stacji roboczych oraz zainstalowanych wersji oprogramowania. Konieczności takiej nie określono też w IZSI, co opisano w dalszej części wystąpienia pokontrolnego, w sekcji „Ustalone nieprawidłowości". W Ośrodku nie stwierdzono wykorzystywania urządzeń informatycznych niebędących własnością GOPS.
(dowód: akta kontroli str. 208-229, 317-321)

Od 1 stycznia 2016 r. do 30 marca 2017 r. na nośnikach CD-R; pięciokrotnie[41] tworzono kopie zapasowe danych przetwarzanych w systemach: TT-Fundusz alimentacyjny i TT-Pomoc oraz dwukrotnie w systemach „Płatnik" (odpowiednio: 3 czerwca 2016 r. i 15 marca 2017 r.) i TT-Świadczenia rodzinne (14 czerwca 2016 r. i 3 marca 2017 r.). Kopii tych nie testowano, a częstotliwość ich sporządzania nie odpowiadała wymogom określonym w IZSI. Nie sporządzano natomiast kopii danych przetwarzanych w systemach EZD, „Księgowość budżetowa" oraz SEPI. Na dwóch komputerach korzystano z funkcjonalność TT-BACKUP, służącej do tworzenia okresowych baz danych na dysku lokalnym, przetwarzanych w systemach TT-Świadczenia alimentacyjne oraz TT-Świadczenia rodzinne, co opisano w dalszej części wystąpienia pokontrolnego, w sekcji „Ustalone nieprawidłowości". (dowód: akta kontroli str. 317-321)

W IZSI określono procedurę likwidacji urządzeń, dysków i innych nośników informacji (do 30 marca 2017 r. przypadki takie nie wystąpiły). Ośrodek był wyposażony w niszczarkę do dokumentów papierowych oraz urządzenia UPS (do każdego komputera) na wypadek wystąpienia braku zasilania. Ośrodek nie posiadał procedury postępowania w przypadku długotrwałego braku zasilania. Pracownicy nie korzystali ze służbowych urządzeń informatycznych poza Ośrodkiem, chociaż możliwość tak istniała, w związku z przekazaniem z Ministerstwa Pracy i Polityki Socjalnej terminala mobilnego ACER TMB 113E. (dowód: akta kontroli str. 322-329)

Pomieszczenia GOPS sprzątane były przez pracownicę Urzędu Gminy, która czynności wykonywała w godzinach pracy GOPS i w obecności pracowników Ośrodka.

GOPS nie posiadał dokumentacji potwierdzającej wykonywanie przeglądów technicznych i konserwacji systemów oraz nośników informacji służących do przetwarzania danych, co opisano w dalszej części wystąpienia pokontrolnego, w sekcji „Ustalone nieprawidłowości". Ośrodek nie podpisywał umów na świadczenie usług w zakresie usuwania usterek i awarii sprzętu komputerowego wykorzystywanego do przetwarzania danych. Awarie były usuwane na prośbę Kierownika GOPS przez pracowników firmy TOP TEAM, która prowadziła serwis systemów dziedzinowych wykorzystywanych w Ośrodku (pomoc zdalna i w siedzibie GOPS), a w przypadku systemu „Księgowość Budżetowa" przez pracowników firmy Nanocom, która prowadziła serwis systemu Info System, wykorzystywanego w Urzędzie Gminy w Rudce (pomoc zdalna i w siedzibie GOPS), zaś w odniesieniu do systemu EZD – przez Sekretarza Gminy. Żadnego z ww. podmiotów nie zobowiązano do zachowania poufności w odniesieniu do danych osobowych przetwarzanych w GOPS, z którymi mogą mieć styczność w trakcie usuwania awarii, co opisano poniżej, w sekcji „Ustalone nieprawidłowości".
(dowód: akta kontroli str. 38, 316)

Ustalone nieprawidłowości

W działalności kontrolowanej jednostki w przedstawionym zakresie stwierdzono następujące nieprawidłowości:

1. Nie przeprowadzano inwentaryzacji zasobów informatycznych Ośrodka, czym naruszono § 20 ust. 2 pkt 2 rozporządzenia KRI. Zgodnie z powołanym przepisem kierownik powinien zapewnić utrzymywanie aktualności inwentaryzacji sprzętu

[41] Odpowiednio: 8 kwietnia, 15 kwietnia i 22 lipca 2016 r. oraz 7 lutego i 3 marca 2017 r.

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).

Kierownik Ośrodka wyjaśniła, że: „Nie mamy zatrudnionego pracownika, który byłby w stanie taką usługę wykonać. Urządzenia te były inwentaryzowane zgodnie z ustawą z dnia 29 września 1994 r. o rachunkowości"[42]. (dowód: akta kontroli str. 330-331)

2. Nie sporządzano kopii danych przetwarzanych w Ośrodku z częstotliwością określoną w rozdziale IV pkt 3 IZSI (tj. nie rzadziej niż raz na tydzień). W 2016 roku w zależności od rodzaju aplikacji kopie takie sporządzono jedynie dwu lub pięciokrotnie. Ponadto sporządzanie kopii na dyskach lokalnych komputerów za pomocą funkcjonalności TT-BCKUP nie zapewniło im ochrony w przypadku trwałego uszkodzenia urządzenia.

   Kierownik Ośrodka wyjaśniła, że: „W związku z natłokiem pracy bieżącej nie sporządzamy kopii danych przetwarzanych w systemach informatycznych z częstotliwością określoną w instrukcji Zarządzania Systemem Informatycznym. Posiadamy program TT-BACKUP, który raz w tygodniu, w piątek wykonuje automatycznie kopie bazy danych". (dowód: akta kontroli str. 314-315, 330-331)

3. Nie wykonywano przeglądów technicznych i konserwacji systemów oraz nośników informacji służących do przetwarzania danych, co sprzeczne było z § 5 IZSI, zobowiązującym kierownika do wykonywania tych czynności co 30 dni i co najmniej raz w roku, w sposób generalny.

   Kierownik Ośrodka wyjaśniła, że czynności tych nie wykonywano „(…) ponieważ nie mamy zatrudnionej osoby wykwalifikowanej w tym zakresie".
   (dowód: akta kontroli str. 314-315, 330-331)

4. W Ośrodku wszystkim użytkownikom komputerów wykorzystywanych do przetwarzania danych osobowych nadano uprawnienia administratora systemu operacyjnego. Pozwalało to na możliwość samodzielnego instalowania przez użytkownika nieautoryzowanego oprogramowania, co potwierdza stwierdzony w trakcie oględzin przypadek zainstalowania na jednym z komputerów programu do rozliczania PIT za 2016 rok. Kierownik ośrodka wyjaśniła, że: „Każdy pracownik jest samodzielnym administratorem oprogramowania. Wgrane oprogramowanie na komputerze służyło jako dodatkowa forma pomocy w ramach pracy socjalnej dla klientów Ośrodka pomocy społecznej, w celu rozliczania podatku PIT". (dowód: akta kontroli str. 208-210, 330-331)

5. Nie zobowiązano podmiotów i osób (tj. pracowników firmy TOP TEAM i Nanocom oraz Sekretarza Gminy), świadczących pomoc w zakresie usuwania awarii sprzętu komputerowego wykorzystywanego od przetwarzania danych osobowych w Ośrodku, do zachowania poufności danych osobowych, z którymi mogli mieć styczność podczas wykonywania tych czynności. Stosownie do przepisu art. 37 uodo, do przetwarzania danych mogą być dopuszczone wyłącznie osoby posiadające upoważnienie administratora danych. Kierownik GOPS wyjaśniła, nie zobowiązywano ww. podmiotów do zachowania poufności, gdyż *„…w 2016 roku nie wystąpiły techniczne awarie komputerów, które wymagałyby interwencji…".* (dowód: akta kontroli str. 34-38, 316)

Ocena cząstkowa

Najwyższa Izba Kontroli ocenia negatywnie zabezpieczenie systemów informatycznych. Techniczne warunki pasywnej asekuracji jedynie w minimalnym stopniu ograniczały skutki ewentualnych zagrożeń związanych z kradzieżą lub pożarem. Na obniżenie poziomu bezpieczeństwa danych wpływać mogło również nadanie wszystkim użytkownikom komputerów uprawnień administratora oraz niezobowiązanie do zachowania poufności podmiotów i osób, którym powierzono usuwanie awarii sprzętu komputerowego. W Ośrodku nie spełniono też szeregu wymogów przewidzianych w rozporządzeniu KRI, dotyczących zinwentaryzowania składników sprzętu komputerowego i zainstalowanego na nim oprogramowania (w celu odtworzenia) oraz okresowego kontrolowania ich stanu

[42] Dz. U. z 2016 r. poz. 1047 ze zm.

technicznego w celu rozpoznania zagrożeń. Nie przestrzegano też postanowień IZSI dotyczących częstotliwości tworzenia kopii danych przetwarzanych w systemach informatycznych.

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

Opis stanu faktycznego

Zgodnie z wymogiem określonym § 20 ust. 2 pkt 14 rozporządzenia KRI, w Ośrodku dokonano analizy poufności, integralności i rozliczalności systemów informatycznych pod kątem zagrożeń i ryzyka. W wyniku analizy:

- zdiagnozowano 19 potencjalnych zagrożeń utraty poufności danych przetwarzanych w systemach informatycznych (związanych np. z: nieuprawnionym dostępem do pomieszczeń, ujawnieniem haseł dostępowych, utratą nośnika zawierającego dane osobowe, pokonaniem zabezpieczeń fizycznych lub programowych, podglądem, podsłuchem, pożarem itp.),
- wskazano na sposoby poprawy bezpieczeństwa, tj. ograniczenie kręgu osób przetwarzających dane wyłącznie do upoważnionych, zabezpieczenie pomieszczeń systemem antywłamaniowym oraz przestrzeganie instrukcji przeciwpożarowej,
- zalecono rygorystyczne przestrzeganie przepisów w zakresie ochrony danych osobowych oraz postanowień PB i IZSI. (dowód: akta kontroli str. 81)

Zagadnienie dotyczące przestrzegania zasad korzystania z systemów, których administratorem danych nie był kierownik Ośrodka opisano w pkt 1.1 niniejszego wystąpienia.

Analiza uprawnień nadanych pracownikom GOPS wykazała, że wszyscy posiadali osobisty login i hasło, umożliwiające prace w tych systemach. Zakres udzielonych upoważnień do wykonywanych obowiązków opisano w pkt. 1.2 niniejszego wystąpienia. W okresie objętym kontrolą nie zwalniano pracowników, przez co nie wdrażano procedury odebrania uprawnień dostępowych.

Ośrodek korzystał z usług Internetowych za pośrednictwem modemu zainstalowanego w Urzędzie Gminy w Rudce. Z informacji przekazanej przez Sekretarza Urzędu wynika, że:

- modem DSL i przełącznik sieciowy SWITCH udostępniające usługi Internetowe zabezpieczono urządzeniem podtrzymującym pracę w przypadku zaniku napięcia,
- łącze, z którego korzysta GOPS jest łączem z publicznym adresem IP, nie jest łączem dedykowanym, do którego dostęp wymaga hasła,
- zabezpieczenie typu firewall (automatycznie aktualizowane) jest zainstalowane na przełączniku sieciowym – jest to jedyne zabezpieczenie, które można ulokować na urządzeniu udostępniającym Internet,
- nie ma technicznej możliwości selekcji wiadomości typu SPAM i plików zawierających szkodliwe oprogramowanie,
- nie ma technicznych możliwości zapisywania logów systemowych usług sieciowych udostępnianych Ośrodkowi,
- nie odnotowano prób nieautoryzowanego dostępu do sieci komputerowej, z której korzysta Urząd i GOPS. (dowód: akta kontroli str. 332-334)

Oględziny komputerów Ośrodka wykazały, że na stronach witryn internetowych wykorzystywanych do obsługi programów dziedzinowych firmy TOP TEAM zamieszczone były komunikaty „Połączenie nie jest bezpieczne”, „Pobierana strona www nie obsługuje szyfrowania danych”, „Informacje przesyłane przez sieć Internet bez uprzedniego szyfrowania mogą zostać odczytane przez inne osoby”. Natomiast strona Internetowa systemu IS KDR oznakowana była jako „Bezpieczna”, a w przypadku korzystania ze stron

Internetowych systemu „Płatnik" automatycznie pojawiał się komunikat o aktywnym zabezpieczeniu danych za pomocą oprogramowania AVAST.

(dowód: akta kontroli str. 212, 216-218, 221)

Na trzech komputerach zainstalowano system operacyjny Windows 7, a na jednym system Windows 10 Pro. Na trzech spośród czterech komputerów nie stwierdzono zainstalowanych nielicencjonowanych programów. Na jednym zainstalowano oprogramowanie do rozliczania deklaracji podatkowych PIT za 2016 rok, co opisano w poprzednim punkcie wystąpienia w sekcji „Ustalone nieprawidłowości". Do ochrony systemów używany był program antywirusowy AVAST Professional AntiVirus. (dowód: akta kontroli str. 213, 221)

Kierownik Ośrodka wyjaśniła, że nie wystąpiły przypadki wykrycia nieautoryzowanych działań związanych z przetwarzaniem informacji. Nie zaszła też konieczność odtwarzania zbioru danych z kopii bezpieczeństwa. Na komputerach Ośrodka zainstalowany był program antywirusowy aktualizujący się automatycznie. (dowód: akta kontroli str. 330-331)

Płatności elektronicznie Ośrodek realizował na podstawie umowy Nr 20/16 o świadczenie usługi systemu bankowości internetowej eCorpoNet, zawartej 17 października 2016 r. z Bankiem Spółdzielczym w Brańsku. Przelewy realizowano po złożeniu podpisu elektronicznego przez dwóch pracowników, którym PWPW-Sigillum PCCE S.A. w Warszawie wystawiło certyfikaty, zgodnie z umową o świadczenie usług certyfikacyjnych, zawartą 29 maja 2015 r. (dowód: akta kontroli str. 335-347)

W 2016 roku na zapewnienie bezpieczeństwa przetwarzania danych wydatkowano 126,57 zł za przedłużenie licencji użytkowania programu antywirusowego AVAST na jednym komputerze. Na pozostałych trzech nie upłynął jeszcze trzyletni okres ważności uprawnień. (dowód: akta kontroli str. 348-349)

Ustalone nieprawidłowości

W działalności kontrolowanej jednostki w przedstawionym zakresie stwierdzono nieprawidłowość, polegającą na niezapewnieniu wysokiego stopnia bezpieczeństwa przetwarzania danych określonego w IZSI. Dane przesyłane przez sieć Internet (przetwarzane w systemach dziedzinowych firmy TOP TEAM) nie były szyfrowane. Stanowiło to naruszenie § 6 ust. 4 rozporządzenia MSWiA oraz postanowień zawartych w części „C" załącznika do ww. rozporządzenia.

Kierownik Ośrodka wyjaśniła, że oprogramowanie zostało zainstalowane przez firmę TOP TEAM, która sprawuje nadzór w ramach umowy i nie są jej znane przyczyny wyświetlania komunikatów, iż połączenia nie są bezpieczne.

(dowód: akta kontroli str. 206-229)

Ocena cząstkowa

W GOPS dokonano analizy poufności, integralności i rozliczalności systemów informatycznych, w efekcie czego zidentyfikowano zagrożenia i ryzyka oraz przestrzegano zasad uwierzytelniania użytkowników systemów informatycznych. Przekazywanie jednak nieszyfrowanych danych w sieci publicznej Internet nie zapewniało im bezpieczeństwa. Były bowiem ogólnodostępne, a zatem mogły być odczytane przez nieupoważnionych.

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 o Najwyższej Izbie Kontroli[43], wnosi o:

1. Prawidłowe, zgodne z art. 7 pkt 4 uodo, określenie administratora sześciu zbiorów danych, prowadzonych przez GOPS i zgłoszenie ww. zmiany do GIODO.
2. Terminowe zgłaszanie GIODO zmian w zakresie danych osobowych przetwarzanych w Ośrodku w zarejestrowanych zbiorach, stosownie do art. 41 ust. 2 uodo oraz

[43] Ustawa z dnia 23 grudnia 1994 r. o Najwyższej Izbie Kontroli (Dz. U. z 2017 r. poz. 524). Ustawa zwana dalej: „ustawą o NIK".

zgłoszenie zaprzestania przetwarzania danych w dwóch zbiorach, w celu uzyskania decyzji o ich wykreśleniu z rejestru, stosownie do art. 44a pkt 1 uodo.

3. Zaktualizowanie PB Ośrodka w zakresie sposobu przepływu informacji między systemami przetwarzającymi dane osobowe oraz o wykaz wszystkich zbiorów wraz z opisem ich struktury, stosownie do § 4 pkt 3 i 4 rozporządzenia MSWiA.
4. Przeprowadzanie inwentaryzacji sprzętu informatycznego i nośników informacji przetwarzanych w Ośrodku oraz dokonywanie ich okresowych przeglądów i konserwacji, w celu wykonania kontroli określonej w § 20 ust. 2 pkt 12 lit. h rozporządzenia KRI.
5. Wykonywanie kopii bezpieczeństwa danych przetwarzanych z częstotliwością określoną w IZSI oraz odebranie użytkownikom uprawnień administratora systemu operacyjnego w komputerach wykorzystywanych do przetwarzania danych.
6. Zobowiązanie podmiotów i osób świadczących pomoc w zakresie usuwania awarii sprzętu komputerowego, do zachowania poufności w odniesieniu do danych osobowych znajdujących się na urządzeniach Ośrodka.
7. Podjęcie działań w celu zapewnienia wysokiego poziomu bezpieczeństwa przesyłu danych za pośrednictwem publicznej sieci Internet, do której włączone są komputery Ośrodka, w sposób określony w załączniku do rozporządzenia MSWiA oraz zgodnie z wymogiem § 20 ust. 2 pkt 12 lit. d rozporządzenia KRI.

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 wykonania uwag i 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 28 kwietnia 2017 r.

Kontroler Marek Zapolski doradca ekonomiczny	DYREKTOR DELEGATURY Najwyższej Izby Kontroli w Białymstoku z up. WICEDYREKTOR Robert Skwarko
..... *podpis*	..... *podpis*