NAJWYŻSZA IZBA KONTROLI
Delegatura w Olsztynie

LOL. 411.5.7.2023

Beata Ostrzycka
Dyrektor
Samodzielnego Gminnego Zakładu Opieki
Zdrowotnej w Dywitach
ul. Jeżynowa 16
11-001 Dywity

WYSTĄPIENIE POKONTROLNE

I/23/003 Ochrona danych pacjentów przed cyberatakami w podmiotach leczniczych na terenie województwa warmińsko-mazurskiego

NAJWYŻSZA IZBA KONTROLI
Delegatura w Olsztynie
ul. Artyleryjska 3e, 10-165 Olsztyn
T +48 89 678 82 00, F +48 89 678 82 30
lol@nik.gov.pl

I. Dane identyfikacyjne

Jednostka kontrolowana

Samodzielny Gminny Zakład Opieki Zdrowotnej w Dywitach, ul. Jeżynowa 16, 11-001 Dywity (dalej: SGZOZ lub Przychodnia).

Kierownik jednostki kontrolowanej

Beata Ostrzycka, Dyrektor, od 1 września 2018 r.

Zakres przedmiotowy kontroli

1. Działania związane z przygotowaniem technicznym i organizacyjnym dotyczącym przetwarzania i ochrony danych pacjentów przed cyberatakami.
2. Funkcjonowanie przyjętych rozwiązań i ich wpływ na ochronę danych pacjentów przed cyberatakami.

Okres objęty kontrolą

Lata 2020-2023 (I półrocze) z uwzględnieniem okresów wcześniejszych i późniejszych, jeśli miało to wpływ na realizowanie zadania.

Podstawa prawna podjęcia kontroli

Art. 2 ust. 2 ustawy z dnia 23 grudnia 1994 r. o Najwyższej Izbie Kontroli[1].

Jednostka przeprowadzająca kontrolę

Najwyższa Izba Kontroli
Delegatura w Olsztynie

Kontrolerzy

1. Bartosz Kościukiewicz, główny specjalista kontroli państwowej, upoważnienie do kontroli nr LOL/14/2024 z 12 stycznia 2024 r.
2. Emilia Wasilewska, starszy inspektor kontroli państwowej, upoważnienie do kontroli nr LOL/15/2024 z 12 stycznia 2024 r.

(akta kontroli str. 1-34)

II. Ocena ogólna[2] kontrolowanej działalności

OCENA OGÓLNA

W Przychodni podjęto działania na rzecz zapewnienia bezpieczeństwa informacji, w tym danych pacjentów. Odpowiednie rozwiązania organizacyjne i techniczne w tym zakresie wprowadzono jednakże dopiero wraz z przyjęciem 1 stycznia 2023 r. nowego Systemu Zarządzania Bezpieczeństwem Informacji (dalej: SZBI), a także wyznaczeniem w listopadzie 2022 r. inspektora danych osobowych (dalej: IOD).

W SGZOZ prawidłowo przypisano odpowiedzialność za bezpieczeństwo informacji określając w wewnętrznych regulacjach zadania administratora danych osobowych (dalej: ADO) i IOD. Obowiązki IOD były zgodne z ustawowymi wymogami, jednocześnie wyznaczona do pełnienia tej funkcji osoba posiadała odpowiednie kwalifikacje.

Nie w pełni jednak realizowano wymagania dotyczące zapewnienia bezpieczeństwa informacji, w tym danych pacjentów, określone w obowiązujących w SGZOZ regulacjach wewnętrznych lub w przepisach prawa. W toku kontroli ustalono bowiem, że np. nie zablokowano możliwości podłączenia nośnika pamięci do poddanym oględzinom stacji roboczych, a niektóre stanowiska komputerowe nie miały aktualnego oprogramowania antywirusowego. Przez okres ponad czterech lat

[1] Dz. U. z 2022 r. poz. 623, dalej: ustawa o NIK.

[2] Najwyższa Izba Kontroli formułuje ocenę ogólną jako ocenę pozytywną, ocenę negatywną albo ocenę w formie opisowej.

Przychodnia korzystała z poczty elektronicznej założonej na komercyjnej domenie bez zawarcia umowy powierzenia przetwarzania danych osobowych.

Należy podkreślić, że stwierdzone w toku kontroli NIK nieprawidłowości zostały usunięte jeszcze przed zakończeniem kontroli.

III. Opis ustalonego stanu faktycznego oraz oceny cząstkowe[3] kontrolowanej działalności

OBSZAR

1. Działania związane z przygotowaniem technicznym i organizacyjnym dotyczącym przetwarzania i ochrony danych pacjentów przed cyberatakami

Opis stanu faktycznego

1.1. W okresie objętym kontrolą w SGZOZ obowiązywały kolejno dwie regulacje wewnętrzne w zakresie bezpieczeństwa informacji stanowiące SZBI. Pierwsza z nich – Polityka bezpieczeństwa informacji oraz Instrukcja zarządzania systemem informatycznym służącym do przetwarzania danych osobowych[4] – obejmowała okres od 25 maja 2018 r. do 31 grudnia 2022 r. Uregulowania te z dniem 1 stycznia 2023 r. zostały zastąpione Polityką ochrony danych osobowych, Polityką retencji danych osobowych, Procedurą użytkowania poczty elektronicznej oraz Regulaminem monitoringu[5]. Wewnętrzne przepisy SGZOZ z 2018 r. określały m.in.: zakres danych osobowych przetwarzanych w Przychodni, zadania ADO i IOD, środki techniczne i organizacyjne niezbędne dla zapewnienia poufności, integralności i rozliczalności przetwarzanych danych oraz procedury: nadawania uprawnień do przetwarzania danych i rejestrowania tych uprawnień w systemie informatycznym, tworzenia kopii zapasowych zbiorów danych oraz programów i narzędzi programowych służących do ich przetwarzania. Przepisy wewnętrzne obowiązujące od 2023 r. określały natomiast m.in. rolę i odpowiedzialność związane z ochroną danych osobowych, sposoby realizacji zasady integralności i poufności oraz przejrzystości, jak również procedurę zgłaszania naruszeń ochrony danych osobowych. Pracownicy Przychodni zostali zapoznani z ww. procedurami, a fakt ten potwierdzono poprzez złożenie pisemnych oświadczeń.

(akta kontroli str. 35-36, 42-43, 63-312)

1.2. W ww. regulacjach określono zakres odpowiedzialności za bezpieczeństwo informacji i przypisano ją ADO[6] i IOD. Polityka bezpieczeństwa informacji z 2018 r. określała zadania ADO, którymi było m.in.: czuwanie nad stosowaniem i przestrzeganiem w Przychodni przepisów Rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE[7] i ustawy z dnia 10 maja 2018 r. o ochronie danych osobowych[8] oraz nadzorowanie pracy IOD, jak również podejmowanie stosownych działań w przypadku wykrycia nieuprawnionego dostępu do bazy danych lub naruszenia zabezpieczenia danych znajdujących się w systemie informatycznym. W Polityce ochrony danych osobowych obowiązującej od 2023 r. określono m.in. zapewnienie środków technicznych i organizacyjnych do osiągnięcia celów tej polityki.

---

[3] Oceny cząstkowe to oceny działalności w poszczególnych obszarach badań kontrolnych. Ocena cząstkowa może być sformułowana jako ocena pozytywna, ocena negatywna albo ocena w formie opisowej.

[4] Wprowadzone zarządzeniami Dyrektora SGZOZ nr: 2/2018 i 2.1/2018 z 24 maja 2018 r.

[5] Wprowadzone zarządzeniami Dyrektora SGZOZ nr: 13/2022, 14/2022, 15/2022 i 16/2022 z 30 grudnia 2022 r.

[6] W okresie objętym kontrolą funkcję ADO pełniła Dyrektor SGZOZ.

[7] Dz. Urz. UE L 119 z 4 maja 2016 r., str. 1 (dalej: RODO).

[8] Dz. U. z 2019 r. poz. 1781 (dalej: ustawa o ochronie danych osobowych).

W całym okresie objętym kontrolą zadania IOD obejmowały m.in.: zapoznawanie pracowników i współpracowników SGZOZ z przepisami RODO i ustawy o ochronie danych osobowych oraz informowanie o zagrożeniach bezpieczeństwa danych osobowych, monitorowanie przestrzegania przepisów prawa o ochronie danych osobowych, ocenianie skutków naruszeń ochrony danych osobowych, jak również prowadzenie audytów stanu ochrony danych osobowych (szerzej opisano w punkcie 1.4.).

(akta kontroli str. 63-126)

1.3. W Polityce bezpieczeństwa informacji z 2018 r. nie określono zasad zarządzania incydentami związanymi z bezpieczeństwem informacji, o których mowa w § 20 ust. 3 rozporządzenia Rady Ministrów z dnia 12 kwietnia 2012 r. w sprawie krajowych ram interoperacyjności, minimalnych wymagań dla rejestrów publicznych i wymiany informacji w postaci elektronicznej oraz minimalnych wymagań dla systemów teleinformatycznych[9] oraz w punkcie A.16.1 Polskiej Normy (opisano w sekcji „Stwierdzone nieprawidłowości"). Procedura zgłaszania naruszeń ochrony danych osobowych została ujęta w Polityce ochrony danych osobowych obowiązującej od 2023 r. Określono w niej katalog okoliczności mogących prowadzić do naruszenia ochrony przetwarzanych danych osobowych oraz sposób reagowania.

(akta kontroli str. 63-126, 344, 484-486)

1.4. W okresie objętym kontrolą[10] w SGZOZ nie było wyznaczonego IOD (opisano w sekcji „Stwierdzone nieprawidłowości"). Został on wyznaczony z dniem 1 listopada 2022 r. Jego kwalifikacje zawodowe zostały zweryfikowane przez Dyrektor Przychodni na podstawie otrzymanej dokumentacji. Stosownie do art. 37 ust. 7 RODO, dokonano zawiadomienia organu nadzorującego o danych kontaktowych IOD.

W regulacjach wewnętrznych SGZOZ przypisano zadania IOD odpowiadające czynnościom określonym w art. 39 RODO, tj.:

- informowanie administratora, podmiotu przetwarzającego oraz pracowników, którzy przetwarzają dane osobowe, o obowiązkach spoczywających na nich na mocy RODO oraz innych przepisów Unii Europejskiej lub państw członkowskich o ochronie danych i doradzanie im w tej sprawie,
- monitorowanie przestrzegania RODO, innych przepisów Unii Europejskiej lub państw członkowskich o ochronie danych oraz polityk administratora lub podmiotu przetwarzającego w dziedzinie ochrony danych osobowych, w tym podziału obowiązków, działań zwiększających świadomość, szkoleń personelu uczestniczącego w operacjach przetwarzania oraz powiązanych z tym audytów,
- udzielanie na żądanie zaleceń co do oceny skutków dla ochrony danych oraz monitorowania jej wykonania zgodnie z art. 35 RODO,
- współpracę z organem nadzorczym,
- pełnienie funkcji punktu kontaktowego dla organu nadzorczego w kwestiach związanych z przetwarzaniem, w tym z uprzednimi konsultacjami, o których mowa w art. 36 RODO oraz w stosownych przypadkach prowadzenia konsultacji we wszelkich innych sprawach.

(akta kontroli str. 63-126, 341-407, 470-472)

1.5. W latach 2020-2023 w SGZOZ, w zakresie związanym z wejściem w życie RODO oraz bezpieczeństwa danych, przeszkoleni zostali wszyscy pracownicy, których forma oraz okres zatrudnienia tego wymagał[11]. Przeprowadzono w tym czasie sześć

[9] Dz. U. z 2017 r. poz. 2247, dalej: rozporządzenie KRI.
[10] Do 31 października 2022 r.
[11] Dotyczyło to 45 pracowników.

szkoleń skierowanych do pracowników medycznych i niemedycznych, zatrudnionych zarówno na umowę o pracę oraz na podstawie umów cywilnoprawnych. Szkolenia te zostały przeprowadzone przez IOD, a ich tematyka objęła m.in. zagadnienia ochrony danych osobowych i przepisów z nią związanych oraz zasad ich przetwarzania.

(akta kontroli str. 339-352)

1.6. SGZOZ nie występował o wsparcie na dofinansowanie inwestycji poprawiających bezpieczeństwo infrastruktury teleinformatycznej.

(akta kontroli str. 44)

Stwierdzone nieprawidłowości

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

1. SZBI, na który składały się regulacje wewnętrzne obejmujące Politykę bezpieczeństwa informacji oraz Instrukcję zarządzania systemem informatycznym służącym do przetwarzania danych osobowych, obowiązujące w okresie od 25 maja 2018 r. do 31 grudnia 2022 r., nie został opracowany na podstawie Polskiej Normy PN-ISO/IEC 27001. Było to niezgodne z § 20 ust. 3 rozporządzenia KRI. W SZBI nie określono bowiem m.in. warunków umożliwiających wywiązanie się z wymagań określonych w § 20 ust. 2 pkt 13 tego rozporządzenia, tj. nie określono zasad zarządzania incydentami związanymi z bezpieczeństwem informacji. Przywołany przepis stanowił, że zarządzanie bezpieczeństwem informacji realizowane jest w szczególności przez zapewnienie przez kierownictwo podmiotu publicznego warunków umożliwiających realizację i egzekwowanie bezzwłocznego zgłaszania incydentów naruszenia bezpieczeństwa informacji w określony i z góry ustalony sposób, umożliwiający szybkie podjęcie działań korygujących. Ponadto w punkcie A.16.1 Polskiej Normy wskazano, że jednym z celów SZBI jest zapewnienie spójnego i skutecznego podejścia do zarządzania incydentami związanymi z bezpieczeństwem informacji, z uwzględnieniem informowania o zdarzeniach i słabościach.

   Dyrektor wyjaśniła, że wewnętrzne regulacje SGZOZ z 2018 r. w tym zakresie nie zawierały zasad zarządzania incydentami związanymi z bezpieczeństwem informacji, gdyż był to początek ich funkcjonowania. Nowe regulacje, obowiązujące od 2023 r. już określają te zasady. Dyrektor wyjaśniła, że nie wiedziała dlaczego regulacje wewnętrzne SGZOZ z 2018 r. nie zostały opracowane na podstawie Polskiej Normy.

   (akta kontroli str. 63-126, 344, 484-486)

2. W okresie objętym kontrolą[12] w SGZOZ nie wyznaczono IOD, co było niezgodne z art. 37 ust. 1 RODO.

   Dyrektor Przychodni wyjaśniła, że została zapewniona przez informatyka zatrudnionego na podstawie umowy serwisowej, że skoro on posiada wyznaczonego IOD w ramach swojej działalności, to jednocześnie SGZOZ też posiada wyznaczonego IOD.

   NIK nie podziela powyższych wyjaśnień, bowiem wspomniana wyżej umowa serwisowa w swoim zakresie przedmiotowym nie wskazywała, że wykonawca zapewnia w ramach tej umowy osobę do pełnienia funkcji IOD w Przychodni. SGZOZ nie zawarł również osobnej umowy w ww. okresie, której przedmiotem byłoby pełnienie funkcji IOD. Ponadto Dyrektor Przychodni wyjaśniła, że nie było

[12] Do 31 października 2022 r.

jej znane imię i nazwisko IOD, o którym została zapewniona przez ww. informatyka i że IOD ten nigdy nie pojawił się osobiście w siedzibie SGZOZ.

(akta kontroli str. 63-126, 341-407, 470-472)

OCENA CZĄSTKOWA

W okresie objętym kontrolą w SGZOZ zostały stworzone odpowiednie rozwiązania organizacyjne w ramach przyjętego SZBI obejmującego m.in. Politykę ochrony danych osobowych, Politykę retencji danych osobowych, Procedurę użytkowania poczty elektronicznej oraz Regulamin monitoringu. Wyznaczony IOD posiadał odpowiednie kwalifikacje, a zadania mu przypisane były zgodne z ustawowymi wymogami. Niektóre jednak z działań podjętych w Przychodni w okresie objętym kontrolą w zakresie stworzenia warunków bezpieczeństwa informacji, w tym ochrony danych, odbyły się niezgodnie z obowiązującymi przepisami. W szczególności dotyczyło to opracowania SZBI obowiązującego do końca 2022 r., w którym nie uwzględniono zasad zarządzania incydentami związanymi z bezpieczeństwem informacji oraz wyznaczenia ww. IOD dopiero z dniem 1 listopada 2022 r.

OBSZAR

2. Funkcjonowanie przyjętych rozwiązań i ich wpływ na ochronę danych pacjentów przed cyberatakami

Opis stanu faktycznego

2.1. W SGZOZ w okresie objętym kontrolą funkcjonowało sześć systemów informatycznych. Służyły one do m.in. obsługi Przychodni, prowadzenia ewidencji dokumentów elektronicznych oraz zarządzania obiegiem informacji.

(akta kontroli str. 46)

2.2. Wszyscy pracownicy niemedyczni zatrudnieni w Przychodni w okresie objętym kontrolą posiadali upoważnienia do przetwarzania danych w zakresie niezbędnym do wykonywania swoich obowiązków służbowych.

(akta kontroli str. 84-87, 255-264, 439-440)

2.3. Analiza nadanych uprawnień dostępu do systemu informatycznego Przychodni oraz upoważnień do przetwarzania danych osobowych przeprowadzona na próbie 24 z 38 pracowników medycznych[13] wykazała m.in. że:

- posiadali oni wydane przez ADO stosowne upoważnienia do przetwarzania danych osobowych,
- mieli dostęp do danych medycznych wyłącznie w zakresie wskazanym w upoważnieniu,
- przetwarzali oni dane w programie służącym do obsługi Przychodni w ramach wykonywanych przez siebie obowiązków.

(akta kontroli str. 255-264, 313-340, 439-440)

2.4. W wyniku analizy rejestru ostatnich logowań 11 byłych pracowników medycznych SGZOZ ustalono, że w systemie informatycznym było odnotowane logowanie jednego z nich po dniu zakończenia okresu jego zatrudnienia (opisano w sekcji „Stwierdzone nieprawidłowości").

(akta kontroli str. 453-464)

2.5. W wyniku oględzin przeprowadzonych w toku kontroli NIK w siedzibie SGZOZ i jego filii w Tuławkach ustalono m.in., że:

- w przypadku jednej stacji roboczej (na pięć poddanych oględzinom) nie został zainstalowany program antywirusowy, a w innej – baza wirusów nie była aktualna na dzień przeprowadzonych oględzin,

[13] Tj. lekarzy, pielęgniarek i fizjoterapeutów.

– żadna z poddanych oględzinom stacji roboczych nie posiadała fizycznej blokady uniemożliwiającej podłączenie nośnika pamięci, jak również nie zablokowano ich w systemie Windows,
– w ustawieniach systemu do obsługi Przychodni w zakładce „Opcje ogólne" w pozycji „Bezpieczeństwo" przy pozycji minimalnej długości hasła znajdowała się wartość „0", zaś przy pozycji „poziom bezpieczeństwa" znajdowała się wartość „1" (opisano w sekcji „Stwierdzone nieprawidłowości").

(akta kontroli str. 465-469)

2.6. W okresie objętym kontrolą w Przychodni nie odnotowano naruszeń w zakresie bezpieczeństwa danych.

(akta kontroli str. 45)

2.7. W dniu 5 lutego 2024 r. założono, celem użytkowania przez Przychodnię, skrzynki pocztowe w domenie sgzozdywity.pl. W okresie od 1 stycznia 2020 r. do 4 lutego 2024 r. SGZOZ nie miał zawartej umowy powierzenia przetwarzania danych osobowych, w związku z korzystaniem z domeny zewnętrznej dla adresów mailowych: sgzozdywity@(...), receptydywity@(...), pelnomocnik.sgzozdywity@(...) (opisano w sekcji „Stwierdzone nieprawidłowości").

(akta kontroli str. 14-29, 35-36, 50- 52, 487-504)

Stwierdzone nieprawidłowości

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

1. Nie zapewniono skutecznego mechanizmu odbierania byłym pracownikom uprawnień dostępu do systemu informatycznego, służącego do obsługi Przychodni, po zakończeniu z nimi stosunku pracy. Działanie to było nierzetelne bowiem zapisy art. 29 oraz art. 32 ust. 4 RODO nakładają na ADO obowiązek podejmowania działań w celu zapewnienia, by każda osoba fizyczna mająca dostęp do danych osobowych, przetwarzała je wyłącznie na podstawie upoważnienia ADO i na jego polecenie. Brak ww. skutecznego mechanizmu umożliwił zalogowanie się jednemu[14] z 11 byłych pracowników do systemu KS-SOMED w dniu 4 maja 2022 r., mimo że umowa o pracę została zakończona 21 kwietnia 2022 r. i w tym samym dniu wygaszono jego upoważnienie do przetwarzania danych osobowych.

   Dyrektor wyjaśniła, że nie wie dlaczego doszło do tego logowania.

   W toku kontroli NIK w SGZOZ opracowano i wprowadzono działania naprawcze obejmujące m.in. podniesienie poziomu bezpieczeństwa w programie KS-SOMED obejmujące wymuszanie zmiany hasła po upływie określonego czasu.

   (akta kontroli str. 84-87, 439-441, 453-464, 484-504)

2. Przeprowadzone przez NIK w dniu 6 lutego 2024 r. oględziny pięciu stanowisk komputerowych wykazały niezgodność z niektórymi postanowieniami SZBI. Dotyczyło to m.in. braku oprogramowania antywirusowego na jednej stacji roboczej oraz braku aktualnej bazy wirusów na kolejnej stacji, a także niezablokowania (fizycznego lub systemowego) portów USB na wszystkich pięciu stanowiskach. Ustalono również, że ustawienia wartości poziomu zabezpieczeń dostępu do systemu obsługi Przychodni posiadały wartości minimalne.

   W sprawie tej Dyrektor wyjaśniła, że w ramach pełnionego przez nią nadzoru otrzymała od IOD Raport z oceny zgodności działalności podmiotu z wymogami z zakresu ochrony danych osobowych w SGZOZ z 28 grudnia 2023 r. W Raporcie

[14] Pracownik medyczny, któremu udzielono upoważnienia do przetwarzania danych osobowych 1 lutego 2022 r. i odebrano je 21 kwietnia 2022 r.

nie wykazano niezgodności w przedmiotowym zakresie, nie sformułowano również rekomendacji.

W toku kontroli NIK w SGZOZ opracowano i wprowadzono działania naprawcze obejmujące m.in. wymianę starych komputerów na nowe z nowym i aktualnym oprogramowaniem antywirusowym, wyznaczenie komputerów, na których mają pozostać aktywne porty USB w celach archiwizacji zdjęć i dokumentacji medycznej oraz zwiększono poziom bezpieczeństwa w programie KS-SOMED, a osoby upoważnione do jego obsługi zmieniły swoje hasła na hasła posiadające wymaganą liczbę znaków.

(akta kontroli str. 465-483, 487-504)

3. W okresie od 1 stycznia 2020 r. do 4 lutego 2024 r. SGZOZ nie zawarł umowy powierzenia przetwarzania danych osobowych, w związku z korzystaniem z domeny zewnętrznej dla adresów mailowych: sgzozdywity@(...), receptydywity@(...), pelnomocnik.sgzozdywity@(...), co było niezgodne z art. 28 ust. 1 i 3 RODO. Przepisy te stanowiły m.in., że jeżeli przetwarzanie danych miało być dokonywane w imieniu administratora, to musiał on korzystać wyłącznie z usług takich podmiotów przetwarzających, które zapewniały wystarczające gwarancje wdrożenia odpowiednich środków technicznych i organizacyjnych, by przetwarzanie spełniało wymogi RODO i chroniło prawa osób, których dane dotyczą. Ponadto przetwarzanie przez podmiot przetwarzający odbywało się na podstawie umowy lub innego instrumentu prawnego, które podlegały prawu Unii Europejskiej lub prawu państwa członkowskiego i wiązały podmiot przetwarzający i administratora.

   W sprawie tej Dyrektor wyjaśniła, że przyczyną powyższej nieprawidłowości było jej przekonanie o poprawności działań SGZOZ w tym zakresie oparte na rekomendacji informatyków, którzy wskazali jej domenę (…).com, jako domenę posiadają zabezpieczenia w zakresie spełnienia obowiązku RODO oraz że zapewnia ona ochronę również przed wyciekiem danych. Dyrektor podała, że informatycy SGZOZ poinformowali ją, że nie ma konieczności zawierania z (…).com umów powierzenia przetwarzania danych i nie weryfikowała tych informacji.

   (akta kontroli str. 14-29, 35-36, 50-52, 487-504)

OCENA CZĄSTKOWA

Pracownicy Przychodni posiadali upoważnienia do danych adekwatne do wykonywanych obowiązków. Pracownicy medyczni ponadto korzystali z systemów informatycznych w zakresie odpowiadającym zakresowi upoważnień. Zapewnienie bezpieczeństwa informacji, w tym danych pacjentów w niektórych przypadkach odbywało się jednak w sposób odbiegający od wymagań określonych w obowiązujących w SGZOZ regulacjach wewnętrznych lub w przepisach prawa. Stwierdzono bowiem, że w sposób nieskuteczny odbierano byłym pracownikom uprawnienia dostępu do systemów informatycznych, jak również nie zapewniono aktualnego oprogramowania antywirusowego czy zablokowania portów USB. Ponadto przez okres ponad czterech lat Przychodnia korzystała z poczty elektronicznej założonej na komercyjnej domenie bez zawarcia umowy powierzenia przetwarzania danych osobowych. W ocenie NIK powyższy stan wskazuje, że nadzór nad przestrzeganiem przez pracowników SGZOZ zasad określonych w SZBI nie był w pełni skuteczny.

IV. Uwagi i wnioski

Wnioski

Najwyższa Izba Kontroli w wyniku kontroli nie formułuje uwag. W związku z usunięciem w toku kontroli stwierdzonych nieprawidłowości lub ich ustaniem, NIK nie formułuje również wniosków.

V. Pozostałe informacje i pouczenia

Wystąpienie pokontrolne zostało sporządzone w dwóch egzemplarzach; jeden dla kierownika 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 Olsztynie. Prawo zgłaszania zastrzeżeń, zgodnie z art. 61b ust. 2 ustawy o NIK, nie przysługuje do wystąpienia pokontrolnego zmienionego zgodnie z treścią uchwały w sprawie zastrzeżeń.

Olsztyn, 29 marca 2024 r.

Emilia Wasilewska
Starszy inspektor kontroli państwowej

.....
podpis

Najwyższa Izba Kontroli
Delegatura w Olsztynie
Dyrektor
z up. Piotr Wanic
Wicedyrektor

.....
podpis