NAJWYŻSZA IZBA KONTROLI
Delegatura w Lublinie

LLU.410.003.02.2019

**Pan Piotr Dreher**
**Dyrektor Szpitala Neuropsychiatrycznego**
**Prof. Mieczysława Kaczyńskiego**
**SP ZOZ w Lublinie**

# WYSTĄPIENIE POKONTROLNE

P/19/063 - Wdrożenie przez podmioty lecznicze regulacji dotyczących ochrony danych osobowych

NAJWYŻSZA IZBA KONTROLI
Delegatura w Lublinie
ul. Okopowa 7, 20-022 Lublin
T +48 81 461 31 20, F +48 81 461 31 11
llu@nik.gov.pl
Adres korespondencyjny: Skr. poczt. P-112, 20-001 Lublin 1

# I. Dane identyfikacyjne

Jednostka kontrolowana

Szpital Neuropsychiatryczny im. Prof. Mieczysława Kaczyńskiego, Samodzielny Publiczny Zakład Opieki Zdrowotnej, ul. Abramowicka 2, 20-442 Lublin (dalej: *Szpital* lub *SPZOZ*)

Kierownik jednostki kontrolowanej

Piotr Dreher, Dyrektor od dnia 22 marca 2018 r.

Zakres przedmiotowy kontroli

1. Opracowanie wymaganej dokumentacji oraz procedur związanych z ochroną przetwarzanych danych osobowych.
2. Zapewnienie prawidłowego przetwarzania i ochrony danych osobowych.

Okres objęty kontrolą

Od 25 maja 2018 r. do dnia zakończenia czynności kontrolnych, a także działania sprzed tego okresu, mające związek z zagadnieniami będącymi przedmiotem kontroli.

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 Lublinie

Kontrolerzy

1. Agnieszka Bury, doradca prawny, upoważnienie do kontroli nr LLU/32/2019 z 1 lutego 2019 r.
2. Monika Cieniuch, starszy inspektor kontroli państwowej, upoważnienie do kontroli nr LLU/33/2019 z 1 lutego 2019 r.

(akta kontroli, str. 1-4)

# II. Ocena ogólna[2] kontrolowanej działalności

**OCENA OGÓLNA**

Najwyższa Izba Kontroli negatywnie ocenia przygotowanie Szpitala do wdrożenia niezbędnych regulacji dotyczących ochrony danych osobowych oraz podjęte przez Szpital działania w celu zapewnienia przetwarzania danych osobowych w sposób zgodny z obowiązującymi przepisami.

Uzasadnienie oceny ogólnej

Stwierdzono bowiem nieprawidłowości, polegające m.in. na:

- przekazaniu z naruszeniem art. 5 ust. 1 lit. c RODO[3]. podmiotowi świadczącemu usługi serwisowe danych osobowych dwóch pacjentów Szpitala, w tym danych medycznych jednego z nich, co nie było konieczne do przeprowadzenia procesu obsługi zgłoszenia serwisowego,
- niedostosowaniu regulacji wewnętrznych do przepisów RODO oraz nieprzeszkoleniu ponad połowy pracowników Szpitala z zakresu ochrony danych osobowych i danych medycznych,

[1] Dz. U. z 2019 r. poz. 489, dalej: ustawa o NIK.

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

[3] Rozporządzenie 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 (Dz. Urz. UE L 119 z 4 maja 2016 r., str. 1).

- niezapewnieniu jednej osobie personelu właściwych uprawnień w systemach operacyjnych, a także niezastosowaniu w czterech przypadkach środków uwierzytelniających podczas rozpoczynania pracy (loginu i hasła), co było niezgodne z § 20 ust. 2 pkt 4, pkt 7 lit. a i pkt 12 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[4],
- odebraniu z opóźnieniem byłym pracownikom uprawnień w systemie wykorzystywanym do przetwarzania danych medycznych, co było sprzeczne z przepisem § 20 ust. 2 pkt 5 rozporządzenia KRI,
- przechowywaniu materiałów łatwopalnych oraz niewykorzystywanego sprzętu komputerowego w serwerowni oraz pomieszczeniu, w którym znajdowały się kopie bezpieczeństwa baz danych Szpitala.

# III. Opis ustalonego stanu faktycznego oraz oceny cząstkowe[5] kontrolowanej działalności

OBSZAR

## 1. Opracowanie wymaganej dokumentacji oraz procedur związanych z ochroną przetwarzanych danych osobowych

Opis stanu faktycznego

**1.1.** Wywiązując się z obowiązku określonego w art. 8 ustawy z dnia 10 maja 2018 r. o ochronie danych osobowych[6] w związku z art. 37 RODO, Dyrektor Szpitala z dniem 18 maja 2018 r. wyznaczył Inspektora Ochrony Danych Osobowych (dalej: IODO). Na stanowisko to powołany został pracownik zatrudniony dotychczas w Szpitalu jako inspektor ds. zamówień publicznych[7]. Posiadał wykształcenie magisterskie z zakresu administracji, licencjackie z zakresu politologii oraz ukończył studia podyplomowe z zakresu zamówień publicznych. IODO odbył szkolenie na temat: *Wszystko o RODO - jak się przygotować?* (9 marca 2018 r.), a w dniu 13 czerwca 2018 r. szkolenie: *Wdrożenie RODO w jednostkach obszaru ochrony zdrowia*, a także dotyczące narzędzi informatycznych w zarządzaniu w ochronie zdrowia, rozwoju zdolności analitycznych i audytu wewnętrznego pracowników sektora ochrony zdrowia[8]. Z dniem wyznaczenia na inspektora ochrony danych osobowych złożył ponadto oświadczenie, że posiada wiedzę fachową na temat prawa i praktyk w dziedzinie ochrony danych osobowych oraz wypełniania zadań określonych na tym stanowisku. Wykształcenie i doświadczenie IODO spełniały wymogi art. 37 ust. 5 RODO. Zawiadomienie o wyznaczeniu IODO przekazane zostało do Prezesa Urzędu Ochrony Danych Osobowych w dniu 5 lipca 2018 r., tj. z opóźnieniem wynoszącym 32 dni. Przekazane zawiadomienie zawierało wszystkie elementy określone art. 10 ust. 1 i 3 ustawy o ochronie danych osobowych. Dane IODO oraz sposób i formę kontaktu udostępniono na stronie internetowej Szpitala, zgodnie z wymogiem art. 37 ust. 7 RODO.

[4] Dz. U. z 2017 r. poz. 2247. Rozporządzenie zwane dalej: rozporządzeniem KRI.

[5] 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.

[6] Dz. U. poz. 1000 ze zm.

[7] Tj. w okresie od 09.12.2015 r. do 31.07.2017 r. i od 10.01.2018 r. do 17.05.2018 r., a w okresie od 01.08.2017 r. do 09.01.2018 r. jako inspektor ds. administracji.

[8] Szkolenie w dniach 21-22.10.2017 r.

W § 5 ust. 10 pkt 7 Regulaminu organizacyjnego Szpitala[9], wskazano stanowisko IODO jako samodzielne stanowisko pracy oraz w § 42 ust. 1 pkt 1.7 określono jego podstawowe zadania. W zakresie obowiązków pracownika pełniącego funkcję IODO wskazano wszystkie zadania określone w art. 39 RODO. Umożliwiono mu wykonywanie obowiązków w sposób niezależny, stosownie do art. 38 ust. 3 tego rozporządzenia. Samodzielne stanowisko IODO, podległe bezpośrednio Dyrektorowi Szpitala, zostało wyodrębnione w strukturze organizacyjnej SPZOZ 20 czerwca 2018 r. w związku ze zmianą regulaminu organizacyjnego[10].

Szpital nie został uznany za operatora usługi kluczowej, o którym mowa w art. 5 ust. 1 ustawy z dnia 5 lipca 2018 r. o krajowym systemie cyberbezpieczeństwa[11]. W Szpitalu dotychczas nie powołano wewnętrznych struktur odpowiedzialnych za cyberbezpieczeństwo określonych w art. 14 tej ustawy.

(akta kontroli, str. 6-64, 179-182)

**1.2.** W Szpitalu obowiązywała *Polityka Bezpieczeństwa* oraz *Instrukcja Zarządzania Systemem Informatycznym służącym do postępowania przy przetwarzaniu danych osobowych oraz postępowania w sytuacji naruszenia ochrony danych osobowych* (dalej: IZSI) wprowadzone zarządzeniem Dyrektora Szpitala Nr 129/2016 z dnia 28 grudnia 2016 r. *Polityka Bezpieczeństwa* zawierała podstawowe zasady, wytyczne i wymagania, zgodnie z którymi powinny być zarządzane, zabezpieczane i udostępniane aktywa informacyjne i materialne Szpitala, a także: [1] wykaz budynków i pomieszczeń tworzących obszar, w którym przetwarzane są dane osobowe, [2] wykaz zbiorów danych osobowych wraz ze wskazaniem programów zastosowanych do przetwarzania tych danych, [3] opis struktury zbiorów danych, [4] sposób przepływu danych między systemami, [5] środki techniczne i organizacyjne niezbędne dla zapewnienia poufności, integralności i rozliczalności przetwarzanych danych. W IZSI określono m.in. [1] obowiązki w ramach przetwarzania danych w systemie informatycznym: Administratora Danych Osobowych (dalej: ADO), Administratora Bezpieczeństwa Informacji (dalej: ABI), Administratora Systemów Informatycznych (dalej: ASI), osoby upoważnionej lub użytkownika systemu informatycznego do korzystania z poszczególnych systemów, [2] zasady wydawania upoważnień i przyznawania dostępu do systemu informatycznego, [3] zasady eksploatacji systemu informatycznego, [4] wymagania sprzętowo-organizacyjne w zakresie ochrony przetwarzania danych osobowych, [5] zastosowane środki programowe, sprzętowe, informatyczne i telekomunikacyjne do przetwarzania danych osobowych, [6] postępowanie w przypadku naruszenia ochrony danych osobowych, [7] zasady udostępniania danych osobowych. Załącznikami do IZSI były wzory: [1] oświadczenia o zapoznaniu się z przepisami dotyczącymi ochrony danych osobowych; [2] upoważnienia pracownika do przetwarzania danych osobowych; [3] wniosku o utworzenie konta i nadanie uprawnień użytkownika dostępu do systemu informatycznego; [4] upoważnienia pracownika do przetwarzania danych osobowych (zmiana zakresu przetwarzania danych osobowych); [5] ewidencji osób uprawnionych do przetwarzania danych osobowych oraz procedury: [1] określająca postępowanie na wypadek awarii w wyniku, próby lub faktu niepowołanego naruszenia ochrony danych osobowych w systemie informatycznym; [2] postępowania z urządzeniami, dyskami lub innymi

[9] Zarządzenie Dyrektora Szpitala Nr 46/2014 z dnia 27 czerwca 2014 r. w sprawie Regulaminu organizacyjnego Szpitala Neuropsychiatrycznego SPZOZ w Lublinie, ujednolicone zarządzeniem wewnętrznym nr 192/2018 z dnia 5 października 2018 r.

[10] Stanowisko IODO wprowadzono do Regulaminu organizacyjnego zarządzeniem wewnętrznym Dyrektora Szpitala nr 113/2018 z dnia 20 czerwca 2018 r.

[11] Dz. U. poz. 1560.

informatycznymi nośnikami zawierającymi dane osobowe, przeznaczonymi do naprawy bądź likwidacji; [3] zasady tworzenia kopii zapasowych i archiwalnych.
Polityka Bezpieczeństwa oraz IZSI nie zostały zaktualizowane. Jako podstawę prawną opracowania tej Instrukcji i Polityki podano przepisy dotyczące ochrony danych osobowych w brzmieniu obowiązującym przed 25 maja 2018 r.[12] W dokumentach tych nie uwzględniono również zmian organizacyjnych wprowadzonych w Szpitalu w związku z wejściem w życie przepisów RODO tj. w zakresie zniesienia funkcji ABI oraz powołania IODO. Zostało to szerzej opisane w dalszej części wystąpienia, w sekcji *Stwierdzone nieprawidłowości*.

Dostęp do Polityki Bezpieczeństwa oraz IZSI za pośrednictwem wewnętrznej sieci intranet mieli wszyscy pracownicy korzystający ze służbowych komputerów. Pracownicy, którzy otrzymali upoważnienia do przetwarzania danych osobowych podpisywali oświadczenie (potwierdzenie) zapoznania się z przepisami dotyczącymi ochrony danych osobowych oraz zobowiązywali się do ich przestrzegania. Kierownicy (przełożeni) danej komórki organizacyjnej byli zobowiązani do zapoznania nowo zatrudnionych pracowników z tymi regulacjami. W przypadku oświadczeń składanych po 25 maja 2018 r., zawierały one zaktualizowaną podstawę prawną (rozporządzenie RODO). Wzór tych oświadczeń nie wynikał z uregulowań wewnętrznych.

(akta kontroli str. 65-115, 587)

Ponadto, w ramach Systemu Zarządzania Jakością[13] opracowano szereg procedur, w tym dotyczących ochrony danych osobowych, regulujących m.in.: [1] nadzór nad dokumentami - dokumentacją medyczną; [2] zasady gromadzenia danych i przetwarzania informacji; [3] zasady bezpieczeństwa informacji medycznej oraz sposób postepowania w sytuacjach krytycznych; [4] zasady dokonywania wpisów i autoryzacja dokumentacji medycznej w wersji elektronicznej; [5] zabezpieczenie papierowej wersji dokumentacji medycznej; [6] przechowywanie archiwalnej dokumentacji medycznej; [7] zasady dostępu do sieci rozległej dla pracowników i pacjentów szpitala; [8] utrzymanie infrastruktury informatycznej.

(akta kontroli str. 116-127)

**1.3.** W Szpitalu od 25 maja do 27 czerwca 2018 r. nie prowadzono rejestru czynności przetwarzania danych, wymaganego art. 30 ust. 1 RODO, co szerzej opisano w dalszej części wystąpienia, w sekcji *Stwierdzone nieprawidłowości.* Według oświadczenia Dyrektora Szpitala, rejestr prowadzony był przez IODO od 28 czerwca 2018 r.[14] w formie elektronicznej. Zawierał wszystkie informacje wymagane w art. 30 ust. 1 RODO, tj.: [1] nazwę i dane kontaktowe administratora oraz IODO, [2] czynności przetwarzania, [3] cel i podstawę prawną przetwarzania, [4] opis kategorii osób, których dane dotyczą, [5] opis kategorii danych osobowych, [6] kategorie odbiorców, którym dane osobowe zastały lub zostaną ujawnione, [7] planowy termin usunięcia danych, [8] ogólny opis technicznych i organizacyjnych środków bezpieczeństwa. W wyniku analizy zapisów rejestru stwierdzono, że nie zawierał on wszystkich czynności przetwarzania danych dokonywanych w Szpitalu. Między innymi, nie wymieniono w nim czynności związanych z przetwarzaniem danych osobowych pacjentów Szpitala (oprócz realizacji recept), jak również nie uwzględniono wszystkich czynności wskazanych w informacjach złożonych do

[12] Ustawa z dnia 29 sierpnia 1997 r. o ochronie danych osobowych (Dz. U. z 2016 r. poz. 922, ze zm.) oraz rozporządzenie 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 (Dz. U. Nr 100, poz. 1024.).

[13] Zarządzeniem Dyrektora Szpitala z dnia 07.11.2018 r. nr 259/2018 *w sprawie aktualizacji Księgi jakości i Katalogu procedur* (wg normy PN-EN ISO 9001:2015).

[14] Rejestr prowadzony był w formie elektronicznej, nie odnotowano w nim daty jego sporządzenia.

IODO przez kierowników poszczególnych oddziałów Szpitala w odpowiedzi na pismo IODO z dnia 21 maja 2018 r. Zgodnie z wyjaśnieniami Dyrektora SPZOZ, rejestr był aktualizowany pod kątem apteki szpitalnej w lutym 2019. Aktualizacja nastąpiła w trybie roboczym, po wymianie poglądów i ustaleniu czynności przetwarzania danych z kierownik apteki[15].

(akta kontroli str. 128-175, 586-590, 605-606)

**1.4.** W Szpitalu przeprowadzono jedną analizę ryzyka przetwarzania danych osobowych, określoną w art. 32 RODO (w dniu 18 lutego 2019 r.)[16]. Na podstawie przeprowadzonej analizy IODO opracował rejestr ryzyk, w którym określił osiem obszarów/grup procesów związanych z przetwarzaniem danych osobowych wraz ze wskazaniem zagrożeń związanych z tymi procesami oraz poziomem ich istotności. Ocenił również stopień zapewnienia bezpieczeństwa tych procesów w stosunku do stwierdzonych ryzyk. Dla każdego procesu opracowana została redukcję ryzyka poprzez zastosowanie odpowiedniego planu działania, np. poprzez szkolenia personelu, szyfrowanie danych, aktualizację procedur, prowadzenie regularnej wymiany oraz przeglądów infrastruktury technicznej (lub: wymianę oraz przegląd infrastruktury technicznej). Żadnego z ryzyk nie określono jako krytyczne. W dwóch przypadkach zalecono monitorowanie ryzyka: [1] w zaznaczonym obszarze *ochrony danych osobowych w Szpitalu*, ryzyko: wycieku danych osobowych na zewnątrz, udostępnienia danych medycznych osobom nieuprawnionym, świadomego lub nieświadomego udostępnienia danych wrażliwych, włamania do sieci IT, ataków złośliwym oprogramowaniem oraz [2] w obszarze *prowadzenia dokumentacji psychologicznej* – ryzyko ujawnienia osobom z zewnątrz protokołów z badań psychologicznych. W pozostałych obszarach określono ryzyka na poziomie akceptowalnym.

(akta kontroli str. 176-178)

**1.5.** W ZOZ nie została wykonana ocena skutków dla ochronnych danych[17], o której mowa w art. 35 RODO. Obowiązek wykonania tej oceny dotyczy bowiem planowanych operacji przetwarzania dla ochrony danych osobowych przed rozpoczęciem ich przetwarzania, a Szpital, wraz z wejściem w życie RODO, nie rozpoczął przetwarzania nowych kategorii danych, w szczególności z użyciem nowych technologii. Również Prezes UODO w komunikacie[18] wydanym na podstawie art. 35 ust. 4 RODO, wśród rodzajów operacji przetwarzania danych osobowych wymagających oceny skutków przetwarzania dla ich ochrony, nie wskazał danych medycznych przetwarzanych w szpitalach, jako wymagających przeprowadzenia takiej oceny. Pojedyncza (bieżąca) ocena operacji wiążących się z wysokim ryzykiem jest również fakultatywna, przy czym Grupa Robocza Art. 29 ds. Ochrony Danych[19] zdecydowanie zalecała dokonanie DPIA dla operacji przetwarzania już trwających przed 25 maja 2018 r.[20] oraz w przypadkach, gdy nie jest jasne, czy wymagana jest DPIA, ponieważ jest ona „przydatnym narzędziem, które może pomóc administratorom danych w zapewnieniu zgodności z prawem ochrony danych". IODO wyjaśnił, że ocena skutków dla ochrony danych nie mogła

[15] Szpital nie dysponuje dokumentami wskazującymi na daty aktualizacji rejestru.
[16] Zgodnie z wyjaśnieniami Dyrektora Szpitala -na dokumencie brak jest daty sporządzenia.
[17] Dalej: DPIA.
[18] Komunikat Prezesa Urzędu Ochrony Danych Osobowych z dnia 17 sierpnia 2018 r. w sprawie wykazu rodzajów operacji przetwarzania danych osobowych wymagających oceny skutków przetwarzania dla ich ochrony (M. P. poz. 827).
[19] Grupa Robocza została powołana na mocy art. 29 dyrektywy 95/46/WE. Była ona niezależnym organem doradczym w zakresie ochrony danych i prywatności. Zadania grupy określone są w art. 30 dyrektywy 95/46/WE oraz art. 15 dyrektywy 2002/58/WE.
[20] Dokument pt.: Wytyczne dotyczące oceny skutków dla ochrony danych (DPIA) oraz ustalenia, czy przetwarzanie „z dużym prawdopodobieństwem może powodować wysokie ryzyko", do celów rozporządzenia 2016/679 https://www.giodo.gov.pl/1520281/id_art/9957/j/pl.

zostać przeprowadzona, ponieważ *zgodnie z art. 35 ust. 4 ww. rozporządzenia, organ nadzorczy ustanowił i podał do publicznej wiadomości wykaz rodzajów operacji przetwarzania podlegających wymogowi dokonania oceny skutków przetwarzania dla ich ochrony dopiero 17 sierpnia 2018 r. (MP 2018 poz. 827). Rozporządzenie zaś weszło w życie 25 maja 2018 r. Najpóźniej w II połowie 2019 r. Szpital rozpocznie korzystanie z rozwiązań technologicznych stosowanych podczas przetwarzania dokumentacji medycznej w postaci elektronicznej, zgodnie z rekomendacjami Centrum Systemów Informacyjnych Ochrony Zdrowia, przed pełnym wdrożeniem ocena skutków zostanie przeprowadzona w myśl komunikatu Prezesa Urzędu Ochrony Danych Osobowych. Szpital przetwarza dane pacjentów wyłącznie w celu świadczenia usług medycznych, odbiorcami danych osobowych są wyłącznie podmioty uprawnione do uzyskania danych osobowych na podstawie przepisów prawa, dane nie podlegają zautomatyzowanemu przetwarzaniu, w tym profilowaniu z użyciem nowych technologii.*

(akta kontroli str. 269-273)

**1.6.** Jednym z zadań IODO, w myśl art. 39 ust. 1 lit. b RODO, było prowadzenie szkoleń dla personelu uczestniczącego w operacjach przetwarzania danych. IODO zorganizował 17 szkoleń w terminach od 23 maja 2018 r. do 18 marca 2019 r. Łącznie przeszkolono 478 pracowników Szpitala, tj. 49,7%. Szkoleniami objęto: zastępcę dyrektora ds. pielęgniarstwa, lekarzy, pielęgniarki/pielęgniarzy, rehabilitantów i fizjoterapeutów, terapeutów, psychologów, logopedów, sekretarki medyczne, laborantów, pracowników administracyjnych i spraw pracowniczych, aptekarzy, informatyka, a także pracowników działu technicznego (tokarz, elektryk, murarz, stolarz, hydraulik) oraz salowe.
Tematyka szkoleń pracowników obejmowała omówienie m.in. następujących zagadnień: [1] najważniejsze pojęcia i definicje RODO, [2] prawa i obowiązki SN ZOZ, [3] prawa i obowiązki pacjentów, [4] proces naboru i rekrutacji zgodnie z RODO, [5] zakres obowiązywania RODO w SN ZOZ, [6] praktyczne zasady RODO, [7] dostęp do danych pacjentów, [8] tajemnica lekarska, tajemnica zawodu zgodnie z RODO, [9] sposób postępowania z pacjentami zgodnie z RODO, ze szczególnym uwzględnieniem prawa do poszanowania godności i intymności w czasie udzielania świadczeń zdrowotnych, [10] rejestracja pacjentów zgodnie z RODO, [11] wprowadzenie i omówienie statusu studentów/praktykantów/stażystów w SPZOZ, zgodnie z zasadami RODO, [12] omówienie praktyk związanych z ochroną danych osobowych (m.in. polityka czystego biurka, logowanie do systemu, zabezpieczanie danych osobowych w komunikacji wewnętrznej).

(akta kontroli str. 187-267)

**1.7.** Szpital w okresie objętym kontrolą nie stosował kodeksu dobrych praktyk ani medycznego kodeksu branżowego. Dyrektor Szpitala wyjaśnił, że *Kodeks dobrych praktyk nie jest normą narzucaną w drodze ustawowej lub innych przepisów obowiązujących powszechnie, lecz ustanawiany jest przez samych przedsiębiorców lub ich zrzeszenia.* Odnośnie do *Kodeksu postępowania dla sektora ochrony zdrowia,* Dyrektor wyjaśnił, że *w dniu 13 listopada 2018 r. Polska Federacja Szpitali - organizacja pracodawców złożyła do Urzędu Ochrony Danych Osobowych wniosek o zatwierdzenie tego kodeksu postępowania wydanego zgodnie z art. 40 RODO i dotyczącego podmiotów wykonujących działalność leczniczą i podmiotów przetwarzających. Do dnia dzisiejszego Prezes Urzędu Ochrony Danych Osobowych nie określiła swojego stanowiska w sprawie. Sprawa znajduje się w toku. Nie jest znana również spodziewana data decyzji dot. złożonego projektu. Wobec powyższego, w chwili obecnej w SN ZOZ nie stosuje się regulacji w nim zawartych.*

Szpital posiada natomiast *Kodeks Etyki Szpitala Neuropsychiatrycznego* wprowadzony Zarządzeniem Wewnętrznym Nr 73/2012 przez Dyrektora Szpitala Neuropsychiatrycznego w dniu 16 maja 2012 r. Kodeks ten stanowił zbiór wartości i zasad, którymi powinni się kierować pracownicy podczas wykonywania zadań służbowych w miejscu pracy, a także poza nim. Celem Kodeksu była poprawa jakości udzielanych świadczeń oraz zwiększenia zaufania pacjentów i ich rodzin do personelu medycznego i wsparcie pracowników w realizowaniu standardów etycznego postępowania.

(akta kontroli str. 179-186)

Stwierdzone nieprawidłowości

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

1. O wyznaczeniu IDOO w dniu 18 maja 2018 r. Dyrektor Szpitala zawiadomił Prezesa Urzędu Ochrony Danych Osobowych dopiero w dniu 5 lipca 2018 r. tj. z opóźnieniem wynoszącym 32 dni w stosunku do terminu określonego w art. 10 ust. 1 u.o.d.o., zgodnie z którym termin na dokonanie zawiadomienia wynosi 14 dni od dnia wyznaczenia inspektora ochrony danych.

   Dyrektor SPZOZ wyjaśnił, że w okresie przejściowym, bezpośrednio po wejściu w życie ustawy o ochronie danych osobowych, zostały przewidziane różne terminy na dopełnienie obowiązku zgłoszenia Inspektora Ochrony Danych Osobowych. Zależały one od tego, czy dany podmiot przed 25 maja 2018 r. miał powołanego administratora bezpieczeństwa informacji (ABI), a także od tego, czy nowe przepisy nakładają na niego obowiązek wyznaczenia inspektora ochrony danych. Szpital powołał Inspektora Ochrony Danych Osobowych, korzystając z dyspozycji przepisu art. 158 ust. 1 ustawy o ochronie danych osobowych, dochowując tym samym terminów obligatoryjnych.

   NIK zauważa, że art. 158 ust. 1 ustawy o ochronie danych osobowych ustalający termin na zgłoszenie inspektora ochrony danych do dnia 1 września 2018 r., dotyczy osoby pełniącej w dniu 24 maja 2018 r. funkcję administratora bezpieczeństwa informacji, natomiast w SPZOZ na IODO powołana została osoba niepełniąca tej funkcji przed wejściem w życie RODO.

   (akta kontroli str. 269)

2. Do dnia 18 kwietnia 2019 r. nie zaktualizowano obowiązujących w Szpitalu regulacji wewnętrznych dotyczących ochrony danych osobowych, w celu dostosowania ich do przepisów RODO i ustawy o ochronie danych osobowych z dnia 10 maja 2018 r. W Szpitalu obowiązywały Polityka Bezpieczeństwa i IZSI, które nie uwzględniały części wymogów przewidzianych w RODO oraz w przepisach krajowych obowiązujących od 25 maja 2018 r., w tym m.in. dotyczących: powołania IODO w miejsce Administratora Bezpieczeństwa Informacji, prawa do sprostowania danych (art. 16 RODO), prawa do usunięcia danych (art. 17 RODO), prawa do ograniczenia przetwarzania (art. 18 RODO), obowiązku powiadamiania o sprostowaniu lub usunięciu danych osobowych, lub o ograniczeniu przetwarzania (art. 19 RODO), uwzględniania ochrony danych osobowych w fazie projektowania, domyślnej ochrony danych (art. 25 RODO), rejestrowania czynności przetwarzania (art. 30 RODO), obowiązku zgłaszania naruszenia ochrony danych osobowych organowi nadzorczemu (art. 33 RODO), prowadzenia oceny skutków dla ochrony danych osobowych (art. 35 RODO), statusu IOD w strukturach Szpitala (art. 38 RODO).

   Niezaktualizowanie regulacji wewnętrznych Szpitala stanowiło naruszenie przepisu art. 24 ust. 1 i 2 RODO, zgodnie z którym do obowiązków administratora danych osobowych należy m.in. poddawanie w razie potrzeby

przeglądom i aktualizacja przyjętych polityk ochrony danych i regulacji wewnętrznych w tym zakresie.

Dyrektor SPZOZ wyjaśnił, że opóźnienia spowodowane były faktem, iż IODO został zobowiązany do zakończenia bieżących spraw służbowych, w związku ze zmianą stanowiska oraz koniecznością przeprowadzenia procesu rekrutacji i zatrudnienia na jego miejsce nowego pracownika. Po przejściu na nowe stanowisko, IODO musiał mieć czas na wdrożenie się do nowych obowiązków. Ponadto pomiędzy listopadem 2018 r. a styczniem 2019 r. przebywał na zwolnieniu lekarskim w związku ze złamaniem. Dodał, że aktualnie w Szpitalu trwają zaawansowane prace kończące proces aktualizacji Polityki Bezpieczeństwa i IZSI.

Załączony do wyjaśnień projekt aktualizacji ww. dokumentów, jako podstawę ich opracowania przywoływał RODO oraz nową ustawę o ochronie danych osobowych, nie zawierał jednak wymienionych powyżej uregulowań wynikających z tych przepisów.

(akta kontroli str. 418, 605-606)

3. Od 25 maja do 27 czerwca 2018 r. w Szpitalu nie był prowadzony rejestr czynności przetwarzania danych osobowych, wbrew wymogom art. 30 ust. 1 RODO. Rejestr ten zaczęto prowadzić dopiero w dniu 28 czerwca 2018 r. Rejestr ten nie zawierał również wszystkich czynności przetwarzania danych dokonywanych w Szpitalu. Między innymi, nie wymieniono w nim czynności związanych z przetwarzaniem danych osobowych pacjentów Szpitala (oprócz realizacji recept), jak również nie uwzględniono wszystkich czynności wskazanych w informacjach złożonych do IODO przez kierowników poszczególnych oddziałów Szpitala.

   Dyrektor Szpitala wyjaśnił, że opóźnienia spowodowane były faktem, iż IODO został zobowiązany do zakończenia bieżących spraw służbowych, w związku ze zmianą stanowiska oraz koniecznością przeprowadzenia procesu rekrutacji i zatrudnienia na jego miejsce nowego pracownika. Po przejściu na nowe stanowisko, IODO musiał mieć czas na wdrożenie się do nowych obowiązków. Ponadto pomiędzy listopadem 2018 r. a styczniem 2019 r. przebywał na zwolnieniu lekarskim w związku ze złamaniem. RODO przewiduje, że administratorzy danych oraz podmioty przetwarzające mają obowiązek prowadzenia odpowiednio rejestru czynności lub rejestru kategorii czynności. Art. 30 RODO wskazuje ich obligatoryjne składniki, niemniej przepis ten może budzić wątpliwości co do znaczenia poszczególnych użytych w jego treści pojęć oraz sposobu wykonania tego obowiązku. UODO przedstawiło szablony rejestrów, zastrzegając jednocześnie, że nie należy traktować ich jako jedynych prawidłowych wzorów. Należy zauważyć, że RODO nie definiuje czynności przetwarzania. Określona w art. 30 RODO zawartość rejestru czynności nie wskazuje na obowiązek opisywania każdej poszczególnej czynności. Kwestie przetwarzania danych osobowych pacjentów oraz czynności sprawozdanych przez kierowników zostaną zaktualizowane w rejestrze.

   (akta kontroli str. 589, 605-606)

4. Analiza procesów przetwarzania danych osobowych wraz z ryzykami i odpowiednimi zabezpieczeniami została przeprowadzona przez IODO 18 lutego 2019 r., tj. po ponad ośmiu miesiącach od wejścia w życie RODO. Wymóg przeprowadzenia analizy wynika z art. 32 RODO, zgodnie z którym do obowiązków administratora należy wdrożenie odpowiednich środków

technicznych i organizacyjnych, aby zapewnić stopień bezpieczeństwa odpowiadający stwierdzonemu ryzyku.

Dyrektor SPZOZ wyjaśnił, że w IODO samodzielnie przeprowadził wewnętrzny przegląd zgodności z RODO na zasadzie: przepis RODO - zagadnienie-wskazówka-pytania kontrolne - ocena „tak/nie/uwagi" czy jednostka spełnia wymagania. Dodał, że *Szpital jest na etapie wdrażania elektronicznego systemu obiegu informacji i dokumentacji i po jego wdrożeniu zostaną wykonane kolejne badania*.

NIK zauważa jednak, że przedłożony *wewnętrzny przegląd kontrolny zgodności z RODO* (bez daty sporządzenia) nie został sporządzony rzetelnie, ponieważ w zakresie oceny, czy jednostka spełnia poszczególne, wymienione w nim wymagania, IODO zaznaczył jedynie: tak/nie lub uwagi, bez wskazania konkretnych rozwiązań przyjętych w Szpitalu lub skonkretyzowania, czego dotyczą uwagi.

(akta kontroli str. Wyjaśnienia z 587, 417-434)

5. Inspektor ochrony danych osobowych nie wywiązał się w pełni z wynikającego z art. 39 ust. 1 lit. b RODO obowiązku prowadzenia szkoleń dla personelu uczestniczącego w operacjach przetwarzania danych. Po wejściu w życie przepisów RODO, do dnia 18 kwietnia 2019 r. przeszkolonych zostało jedynie 478 z 961[21] pracowników Szpitala (tj. 49,7%). 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 wynika również z § 20 ust. 2 pkt 6 rozporządzenia KRI.

   IODO wyjaśnił, że *niski procent udziału w szkoleniach personelu Szpitala, wynika przede wszystkim z faktu, że część personelu pracuje w systemie zmianowo-dyżurowym, w różnych wymiarach czasu pracy, odbiegających od czasu pracy administracji. Ponadto część jest nieobecna w pracy z przyczyn losowych (zwolnienia lekarskie, choroby, rehabilitacja, urlopy rodzicielskie, szkoleniowe itp.). W miesiącach listopad 2018 – styczeń 2019 przebywałem na długim zwolnieniu lekarskim w związku ze złamaniem. Informacje dotyczące obowiązku uczestnictwa w szkoleniach w zakresie przepisów RODO, dostarczane były kierownikom komórek i oddziałów szpitalnych, komunikaty zamieszczane były także w wewnętrznym kanale informacyjnym lecznicy. Nie wszyscy zobowiązani podeszli odpowiedzialnie do realizacji szkoleń, z przyczyn ode mnie niezależnych.*

(akta kontroli str. 236-238)

**OCENA CZĄSTKOWA**

Najwyższa Izba Kontroli negatywnie ocenia działania Szpitala w zakresie opracowania wymaganej dokumentacji oraz procedur związanych z ochroną przetwarzania danych osobowych.

[21] Wg stanu na dzień 25.03.2019 r.

OBSZAR

## 2. Zapewnienie prawidłowego przetwarzania i ochrony danych osobowych

Opis stanu faktycznego

**2.1.** Oględziny trzech[22] (z sześciu) funkcjonujących w Szpitalu rejestracji wykazały, że w celu ochrony danych osobowych pacjentów wprowadzone zostały niżej wymienione rozwiązania:

- zapewniono, aby w obrębie wzroku pacjenta nie znajdowały się dokumenty zawierające dane osobowe innych pacjentów. W jednej rejestracji[23] zamontowano przesłonę pomiędzy poszczególnymi stanowiskami (dwa stanowiska). W pozostałych dwóch rejestracjach, obsługa pacjentów odbywała się przy jednym stanowisku (przy okienku[24] oraz w oddzielnym, zamykanym pomieszczeniu[25]). Pracownicy rejestracji nie wypowiadali na głos informacji zawierających dane osobowe, rejestrowali pacjenta na podstawie dowodu osobistego przekazując jedynie dane dotyczące dalszego procesu postępowania po zarejestrowaniu się do danej poradni lub gabinetu;
- w dwóch rejestracjach[26] poza informacją, że przy okienku może znajdować się tylko jedna obsługiwana osoba zamieszczoną na okienku rejestracji, wyznaczono czerwoną linię na podłodze, znajdującą się w odległości około 2 - 3 metrów od osób znajdujących się przy okienku, zapewniającą odstęp pomiędzy osobami przy okienku, a kolejnymi osobami w kolejce;
- w każdej rejestracji umieszczono pisemne informacje na temat: administratora danych osobowych, IODO wraz z jego danymi kontaktowymi, a także celów i podstaw przetwarzania danych osobowych i okresu przechowywania tych danych w Szpitalu;
- przy okienkach dwóch rejestracji[27] zamieszczono informację dla pacjentów o konieczności okazania dowodu osobistego. Identyfikacja pacjentów rejestrujących się w trakcie prowadzonych oględzin odbyła się na podstawie dowodów osobistych okazanych rejestratorce;
- wszystkie monitory znajdujące się w rejestracjach były ustawione w sposób, który uniemożliwiał osobom rejestrującym się wgląd w treści na nich wyświetlane;

(akta kontroli str. 278-299)

We wszystkich trzech objętych oględzinami gabinetach poradni specjalistycznych[28] karty pacjentów były ułożone w stosach danymi osobowymi w stronę biurka, co uniemożliwiało odczyt tych danych przez pacjentów odbywających wizytę. W czasie oględzin nie stwierdzono pozostawienia gabinetów lekarskich bez nadzoru ani opuszczania gabinetów lekarskich przez lekarzy. Nie stwierdzono pozostawienia klucza w zamkniętych drzwiach gabinetu podczas nieobecności lekarza. Pacjenci nie byli wzywani na wizytę przez lekarza, lecz wchodzili do gabinetu bezpośrednio po jego opuszczeniu przez poprzedniego pacjenta.

---

[22] Rejestracja do przychodni specjalistycznych: Poradni Zdrowia Psychicznego dla Dorosłych, Poradni Zdrowia Psychicznego dla Dzieci i Młodzieży, Poradni Psychologicznej, Poradni Neurologicznej, Poradni Rehabilitacyjnej, Poradni Chirurgii Ogólnej, Poradni Logopedycznej i Poradni Terapii Uzależnień od Substancji Psychoaktywnych, (dalej: rejestracja do przychodni specjalistycznych), Rejestracja do Zakładu Diagnostyki Obrazowej, Rejestracja do przychodni i oddziałów Wojewódzkiego Ośrodka Terapii Uzależnienia od Alkoholu i Współuzależnienia.

[23] Rejestracja do przychodni specjalistycznych.

[24] Rejestracja do Zakładu Diagnostyki Obrazowej.

[25] Rejestracja do przychodni i oddziałów Wojewódzkiego Ośrodka Terapii Uzależnienia od Alkoholu i Współuzależnienia.

[26] Rejestracja do przychodni specjalistycznych.

[27] Rejestracja do przychodni specjalistycznych.

[28] Poradnia Neurologiczna, Poradnia Zdrowia Psychicznego dla Dorosłych i Poradnia Zdrowia Psychicznego dla Dzieci i Młodzieży.

(akta kontroli str. 300-304)

Oględziny dyżurek pielęgniarskich, sal chorych oraz gabinetów lekarskich na trzech oddziałach szpitalnych[29] wykazały m.in., że:

- na oddziałach znajdowało się 28 sal chorych, dysponujących 109 łóżkami,
- wejście do dwóch oddziałów[30] było zamykane na klucz,
- na dwóch oddziałach[31] wszyscy 38 zaobserwowani pacjenci nosili na nadgarstku opaski informacyjne zawierające nazwisko i imię pacjenta (wypisane ręcznie), na Oddziale Psychiatrycznym dla Dzieci i Młodzieży żaden z pacjentów nie miał opaski identyfikacyjnej,
- na żadnym z oddziałów[32] nie umieszczono kart chorych przy łóżkach pacjentów,
- ruch chorych[33] prowadzony był w punkcie pielęgniarskim z pokojem przygotowawczym lub w gabinecie diagnostyczno-zabiegowym, w miejscu niewidocznym dla osób postronnych (w szafkach zamykanych na klucz), na jednym oddziale[34] ruch chorych prowadzony był wyłącznie w formie elektronicznej,
- na jednym z oddziałów[35] w gabinecie pielęgniarki oddziałowej i w punkcie pielęgniarskim z pokojem przygotowawczym nie przechowywano dokumentacji medycznej, na pozostałych oddziałach podręczna dokumentacja pielęgniarska przechowywana była w zamykanych na klucz szafkach,
- poddane obserwacji oddziały wyposażono w 8 komputerów, znajdujących się w gabinetach pielęgniarki oddziałowej, punktach pielęgniarskich z pokojem przygotowawczym i gabinetach diagnostyczno-zabiegowych. Dwa z nich były wyłączone, natomiast 6 było uruchomionych – stwierdzono, że na komputerze uwidoczniony był pulpit i nie był uruchomiony żaden program, w pomieszczeniu nie było obecnych żadnych osób, a pokój był zamknięty na klucz. Było to zgodne z obowiązującą w Szpitalu IZSI, zgodnie z którą komputer zalogowany do systemu nie mógł być pozostawiony w niezamkniętym pomieszczeniu.
- na komputerach w lokalizacji *pulpit* i *moje* dokumenty nie znajdowały się pliki z danymi osobowymi pacjentów,
- na oddziałach znajdowało się pięć gabinetów lekarskich, wyposażonych w 22 komputery, z których 11 było uruchomionych – lekarze pracowali na 4 z nich, a na pozostałych 7 stwierdzono, że uwidoczniony był pulpit i nie był uruchomiony żaden program,
- dokumentacja medyczna pacjentów w gabinetach lekarskich była przechowywana w szafach zamykanych na klucz, albo w zamykanych na klucz szafkach w biurkach lekarzy.
- na dwóch oddziałach[36] znajdowały się trzy gabinety przeznaczone dla psychologów, wyposażone w 4 komputery, z których 2 były uruchomione (pracowali na nich psychologowie),
- dokumentacja medyczna pacjentów w gabinetach przeznaczonych dla psychologów przechowywana była w zamykanej na klucz szafce. Jeden

[29] Oględziny przeprowadzono na Oddziale Neurologicznym, Oddziale Chorób Wewnętrznych i Oddziale Psychiatrycznym dla Dzieci i Młodzieży.
[30] Oddział Chorób Wewnętrznych i Oddział Psychiatryczny dla Dzieci i Młodzieży.
[31] Oddział Neurologiczny, Oddział Chorób Wewnętrznych. Na Oddziale Psychiatrycznym dla Dzieci i Młodzieży żaden z pacjentów nie miał opaski identyfikacyjnej.
[32] Oddział Chirurgii Onkologicznej.
[33] Ruch chorych to lista pacjentów danego oddziału wraz z numerem sali, w których przebywają pacjenci.
[34] Oddział Chorób Wewnętrznych.
[35] Oddział Chorób Wewnętrznych.
[36] Oddział Chorób Wewnętrznych i Oddział Psychiatryczny dla Dzieci i Młodzieży.

psycholog oświadczył, że nie przechowuje w gabinecie[37] żadnej dokumentacji medycznej,

– w czasie oględzin nie stwierdzono pozostawienia gabinetów lekarskich czy dyżurek pielęgniarek bez nadzoru ani opuszczania ich przez personel medyczny. Nie stwierdzono pozostawienia klucza w zamkniętych drzwiach gabinetu/dyżurki.

(akta kontroli str. 90, 305-319)

W ramach oględzin stwierdzono, że na dwóch[38] z trzech oddziałów zamontowane były kamery monitoringu wizyjnego. Na jednym oddziale[39] kamery umiejscowiono na korytarzach na parterze i piętrze budynku oraz na stołówce. Kamery rejestrowały także widok na okna budynku. Na drugim z oddziałów były dwie nieczynne kamery (zostały odłączone przez dział techniczny Szpitala). Informacja o funkcjonującym monitoringu (zawierająca m.in. dane ADO, kontakt do IODO oraz podstawę prawną przetwarzania) znajdowały się na korytarzach Szpitala na tablicach informacyjnych. W SPZOZ nie sporządzono regulaminu monitoringu. Dyrektor wyjaśnił, że mając na uwadze art. 5 ust. 1 lit. e RODO, Szpital dokłada starań, aby okres przechowywania był jak najkrótszy i nie przekraczał 3 miesięcy. Stwierdził, że obraz z kamer może być na bieżąco obserwowany przez operatora lub przechowywany w celu udokumentowania incydentów, jednak nie dłużej niż jest to konieczne do zakończenia odpowiednich czynności wyjaśniających, a dostęp do urządzeń oraz zapisu z monitoringu jest kontrolowany i możliwy, zgodnie z procedurą Q-PP 15 tylko dla osób uprawnionych (pielęgniarka, sekretarka medyczna, informatycy). W Szpitalu stosowana jest klauzula informacyjna przy pobieraniu danych za pośrednictwem monitoringu wizyjnego. Ponadto kwestia monitoringu przy stosowaniu przymusu bezpośredniego została uregulowana w procedurze Q-PP 15.

(akta kontroli str. 305-320, 449-452, 456)

**2.2.** W Szpitalu zarządzanie siecią nie odbywało się za pomocą usługi Active Directory. Dyrektor SPZOZ wyjaśnił, że Szpital w chwili obecnej jest na etapie wdrażania projektu e-zdrowie i planowane jest wdrożenie usługi Active Directory. Zarządzanie siecią w Szpitalu odbywa się z wykorzystaniem oprogramowania Lansweeper – wersja darmowa na licencji Freeware, dla którego wszystkie wymagania sieciowe ustawiane są przez autorski, dedykowany skrypt w języku powłoki shell, napisany przez informatyka Szpitala. Jako sposób uwierzytelnienia wykorzystywane jest logowanie usługi profili użytkowników do systemu Windows.

(akta kontroli str. 454-455)

Według stanu na 25 marca 2019 r. personel działów administracyjnych Szpitala liczył 69 osób. Analiza uprawnień nadanych 59 pracownikom[40] wykazała, że 8 osób (rewident zakładowy, inspektor ds. kancelarii, dwóch inspektorów ds. administracji, inspektor ds. biurowych/ZOL Somatyczny, kierownik Działu Organizacyjnego, specjalista ds. socjalnych pacjentów, inspektor ds. administracyjno-metodycznych) posiadało ograniczony dostęp do danych w programie Hipokrates[41], który pozwalał tylko na odczyt danych. Dyrektor SPZOZ wyjaśnił, że upoważnienie do przetwarzania danych medycznych zostało wydane tym osobom, ponieważ Szpital zobowiązany jest odpowiadać na zapytania upoważnionych organów ochrony prawnej (sądy, prokuratury, policja, ABW, AW, SWW, SKW itp.) Pytania dotyczą m.in. przyczyn hospitalizacji, rozpoznania i diagnozy, terminów pobytów itd. Na powyższe, projekty odpowiedzi, przygotowują upoważnieni przez administratora

[37] Gabinet psychologa na parterze budynku Oddziału Psychiatrycznego dla Dzieci i Młodzieży.
[38] Oddział Chorób Wewnętrznych i Oddział Psychiatryczny dla Dzieci i Młodzieży.
[39] Oddział Psychiatryczny dla Dzieci i Młodzieży.
[40] Nie weryfikowano dostępu pracowników Sekcji Informatyki (4 osoby) i Działu Statystyki Medycznej (6 osób).
[41] Program do obsługi ruchu pacjentów wewnątrz podmiotu leczniczego.

pracownicy. Obecnie w SN ZOZ obowiązuje „odręczny" system dekretowania pism przez dyrekcję, celem ich załatwienia przez pracowników. Po wdrożeniu (połowa 2019 r.) elektronicznego systemu obiegu dokumentacji, proces ten będzie odbywał się wyłącznie w nim. W związku z przeprowadzoną reorganizacją struktury organizacyjnej SN ZOZ, niektóre komórki otrzymały szerszy niż dotychczas zakres obowiązków i w związku z tym zaistniała konieczność nadania uprawnień.
Dostęp ten, w trzech przypadkach był przyznany na wniosek kierownika Działu Organizacyjnego zaakceptowany przez Dyrektora Szpitala, a w pięciu przypadkach na wniosek samego pracownika zaakceptowany przez administratora systemu informatycznego, co szerzej opisano w dalszej części wystąpienia, w sekcji *Stwierdzone nieprawidłowości*. Według obowiązującej w Szpitalu IZSI, dostęp do systemu informatycznego jest przyznawany przez Administratora Systemu Informatycznego i wymaga zgody Administratora Bezpieczeństwa Informacji, czyli upoważnienia pracownika do przetwarzania danych osobowych. Zgodnie z Polityką Bezpieczeństwa, Dyrektor Szpitala określa, kto z podległych mu pracowników ma mieć konto w systemie informatycznym, określa uprawnienia użytkownika i wnioskuje o zmianę tych uprawnień, a Kierownicy Sekcji wnioskują do ABI i ASI o przydział konta w systemie informatycznym dla siebie i podległych pracowników, określają konieczne uprawnienia użytkownika i wnioskują o zmianę tych uprawnień.

(akta kontroli str. 91, 187-218, 274, 325-356, 582-585, 597-598, 605-607)

**2.3.** Analiza przeprowadzona na próbie upoważnień 30 (z 285) pielęgniarek zatrudnionych w Szpitalu[42] wykazała, że wszystkie posiadały dostęp w programie Hipokrates do danych medycznych pacjentów tylko na oddziałach szpitalnych, na których świadczyły pracę. Jedna pielęgniarka nie posiadała jednak w swoich aktach osobowych potwierdzenia nadania jej przez ADO pisemnego upoważnienia do przetwarzania danych osobowych, co szerzej opisano w dalszej części wystąpienia, w sekcji *Stwierdzone nieprawidłowości*. Do przetwarzania danych osobowych nie upoważniono żadnej z 218 osób zatrudnionych na stanowiskach: salowa lub sanitariusz.

(akta kontroli str. 274, 325-344, 357-365)

**2.4.** W okresie od 25 maja 2018 r. do 25 marca 2019 r. 67 osób przestało świadczyć pracę w Szpitalu. Analiza uprawnień 30 spośród tych osób wykazała, że 21 osób w trakcie zatrudnienia miało przyznany dostęp do programu Hipokrates, 12 osobom dostęp do tego programu odebrano przed lub w dniu rozwiązania stosunku pracy, jednej osobie dostęp do programu zablokowano następnego dnia po zakończeniu zatrudnienia, 3 osoby ponownie zostały zatrudnione, natomiast 5 osobom nie odebrano dostępu do programu Hipokrates, co szerzej opisano w dalszej części wystąpienia, w sekcji *Stwierdzone nieprawidłowości*.

(akta kontroli str. 205-206, 366-369)

**2.5.** W myśl postanowień umowy serwisowej, która obowiązywała w okresie objętym kontrolą[43], Szpital obowiązany był do zgłaszania błędów w działaniu programu HIPOKRATES poprzez witrynę internetową help desk wykonawcy, a w przypadku trudności z rejestracją zgłoszenia w tej witrynie, mógł zrealizować je drogą telefoniczną. Oględziny sposobu przekazania 18 zgłoszeń serwisowych[44], związanych z błędami lub wadliwym działaniem programu HIPOKRATES wykazały m.in., że: [1] wszystkie zgłoszenia serwisowe były przekazywane przez informatyków Szpitala i w dniu oględzin miały status *zamrożony*, *zamknięty*,

[42] Dane wg. stanu na 25 marca 2019 r.

[43] Umowa nr SZNSPZOZ.-A-INF.0300-5/18 z 6 marca 2018 r., której przedmiotem było m.in. objęcie nadzorem autorskim modułów Oprogramowania Aplikacyjnego Hipokrates wraz z opieką serwisową.

[44] Zgłoszenia te Szpital przekazał od 25 maja 2018 r. do 17 kwietnia 2019 r.

*rozwiązanie tymczasowe* lub *w realizacji*; [2] dostęp do archiwalnych zgłoszeń możliwy był po dokonaniu autoryzacji (wpisaniu loginu i hasła) w serwisie internetowym do tego wykorzystywanym; [3] wszystkie zrealizowano drogą elektroniczną z wykorzystaniem serwisu internetowego, który został wymieniony w umowie serwisowej; [4] w dwóch przypadkach w zgłoszeniach (dotyczących poprawy daty przyjęcia pacjenta oraz problemu z przesłaniem zlecenia) przekazano dane osobowe pacjentów Szpitala (podano nazwisko, imię oraz pesel oraz w jednym z tych przypadków, także rodzaj wykonywanego badania pacjenta), co szerzej opisano w dalszej części wystąpienia, w sekcji *Stwierdzone nieprawidłowości*.

(akta kontroli str. 457-477, 480-495)

**2.6.** W okresie objętym kontrolą Szpital zawarł 26 umów powierzenia danych osobowych. W 17 z nich SPZOZ był podmiotem przetwarzającym, a w pozostałych 9 administratorem danych (powierzającym przetwarzanie). Szpital umowami powierzył przetwarzanie danych osobowych wykonawcom realizującym na rzecz Szpitala m.in. serwisu oprogramowania oraz usługi informatyczne. Analiza treści pięciu umów powierzenia przez Szpital przetwarzania danych osobowych innym podmiotom (tj. w zakresie obsługi serwisowej rezonansu magnetycznego i stacji diagnostycznej MR, usługi nadzoru autorskiego i serwisu systemu dla pracowni diagnostycznych, wykonywania badań tomografii komputerowej, wykonywania badań usg, dostawy i wdrożenia systemu HIS) wykazała, że zawierały one wszystkie postanowienia wymagane art. 28 ust. 3 RODO, tj. zawierały cel i zakres przetwarzanych danych osobowych oraz zapisy o: przetwarzaniu danych osobowych przez procesora wyłącznie na udokumentowane polecenie ADO, zobowiązaniu osób upoważnionych do zachowania tajemnicy, zapewnieniu przez procesora wszelkich środków technicznych i organizacyjnych w celu ochrony danych, przestrzeganiu warunków korzystania z usług innego podmiotu przetwarzającego za zgodą ADO na dalsze powierzenie, usunięciu lub zwrocie ADO wszelkich danych osobowych po zakończeniu świadczenia usług, umożliwieniu ADO lub audytorowi upoważnionemu przez ADO przeprowadzenie audytów, w tym inspekcji.

(akta kontroli str. 496-550, 593, 595-596)

**2.7.** IODO prowadził rejestr incydentów bezpieczeństwa i działań korygujących i zapobiegawczych, w którym zanotowano dwa zdarzenia. Jedno dotyczyło skargi pacjentki na używanie jej nazwiska przez pracownika Szpitala podczas wchodzenia na zabieg, drugie zdarzenie dotyczyło samoczynnego uruchomienia się czujki alarmowej przeciwdymnej w pomieszczeniu serwerowni. W obydwu przypadkach przeprowadzono postępowanie wyjaśniające i odnotowano podjęcie działań korygujących i zapobiegawczych w postaci upomnienia pracownika i jego przeszkolenia oraz przeprowadzenia audytu zabezpieczeń pomieszczenia serwerowni.

Żaden z dwóch incydentów nie został zgłoszony do Prezesa Urzędu Ochrony Danych Osobowych. Dyrektor SPZOZ wyjaśnił, że obowiązek zgłaszania naruszeń wynika z art. 33 RODO, chyba, że jest mało prawdopodobne, by naruszenie to skutkowało ryzykiem naruszenia praw lub wolności. W przypadku pierwszego incydentu administrator stwierdził, że ma do czynienia z niskim ryzykiem naruszenia praw i wolności osób fizycznych i nie jest zobligowany do zgłoszenia naruszenia Prezesowi Urzędu Ochrony Danych Osobowych. Natomiast drugie zdarzenie miało charakter incydentalny. Został on udokumentowany i zgłoszony administratorowi wraz z zaleceniem przeprowadzenia kontroli zabezpieczenia pomieszczenia serwerowni. Szpital pozyskał środki na doposażenie serwerowni, w związku z tym

trwają prace modernizacyjne, także pod kątem zabezpieczenia przeciwpożarowego. W obydwu przypadkach zostały sporządzone raporty z naruszenia ochrony danych wraz z wnioskami.

(akta kontroli str. 551-561, 586-587)

**2.8.** Od 25 maja 2018 r. do 20 marca 2019 r. do Szpitala wpłynęło 591 wniosków o udostępnienie dokumentacji medycznej, w tym 431 wniosków w 2018 r. i 160 wniosków w 2019 r. Analiza prawidłowości udostępnienia dokumentacji medycznej towarzystwom ubezpieczeniowym (pięć wniosków) oraz osobom fizycznym innym niż sam pacjent (sześć wniosków) wykazała, że dokumentację udostępniono wyłącznie upoważnionym przez pacjenta podmiotom (osobom) lub przedstawicielowi ustawowemu, zgodnie z funkcjonującą w Szpitalu procedurą dotyczącą udostępniania danych medycznych oraz art. 26 ust. 1 ustawy z dnia 6 listopada 2008 r. o prawach pacjenta i Rzeczniku Praw Pacjenta[45]. W jednym przypadku Szpital odmówił udostępnienia dokumentacji medycznej osobie fizycznej, gdyż wnioskujący nie był osobą upoważnioną przez pacjenta.

(akta kontroli str. 562-581)

**2.9.** Regulacje dotyczące ochrony danych przed ich utratą w wyniku awarii, błędów lub nieuprawnionej modyfikacji zostały opisane w IZSI. Określono w niej m.in. zasady: [1] wydawania upoważnień i przyznawania dostępu do systemu informatycznego; [2] przydziału haseł i identyfikatorów dla użytkowników; [3] rozpoczęcia i zakończenia pracy w systemie; [4] tworzenia oraz przechowywania kopii awaryjnych, nośników informatycznych i wydruków komputerowych; [4] ochrony systemu informatycznego; [5] napraw, przeglądów i konserwacji systemu oraz zbioru danych osobowych; [6] postępowania w zakresie komunikacji w sieci komputerowej. Ponadto określono sposób postępowania w przypadku naruszenia ochrony danych osobowych oraz obowiązek zachowania poufności i ochrony danych osobowych.

Oględziny serwerowni Szpitala wykazały, że dostęp do pomieszczenia zabezpieczony był drzwiami zamykanymi na klucz. Docelowo, w ramach realizowanego w Szpitalu projektu e-zdrowie, zainstalowane mają zostać drzwi przeciwpożarowe i antywłamaniowe z zamkiem szyfrowym. Na ścianie obok drzwi serwerowni zostały zamontowane czytniki do kart oraz panel numeryczny do wpisywania kodów. Okna zabezpieczono specjalną folią zapobiegającą nadmiernemu nagrzewaniu się pomieszczenia. Serwerownia wyposażona została w system alarmowy oraz system monitoringu, dwa klimatyzatory oraz gaśnicę. Wszystkie urządzenia informatyczne znajdowały się w specjalnie do tego przystosowanych szafach usytuowanych na podłodze technicznej, tj. powyżej poziomu posadzki. Na wypadek czasowego zaniku zasilania zastosowano układy podtrzymujące napięcie UPS.

Kopie zapasowe baz danych Szpitala, w myśl przepisów § 20 ust. 2 pkt 12 lit. b rozporządzenia KRI oraz postanowień Instrukcji, były przechowywane w specjalnie do tego przystosowanym pomieszczeniu znajdującym się w chronionej części budynku. Oględziny tego pomieszczenia wykazały, że zastosowano w nim następujące rozwiązania zabezpieczające: [1] zabezpieczono dostęp do pomieszczenia, stosując drzwi zamykane na klucz. W ramach projektu e-zdrowie dotychczasowe drzwi mają być wkrótce zastąpione drzwiami przeciwpożarowymi i antywłamaniowymi. Pomieszczenie nie posiada okien; [2] zamontowano system alarmowy oraz system monitoringu; [3] w pomieszczeniu był jeden klimatyzator i nie stwierdzono, aby w pomieszczeniu znajdowała się gaśnica; [5] na wypadek

[45] Dz. U. z 2017 r. poz. 1318, ze zm.

czasowego zaniku zasilania zastosowano układy podtrzymujące napięcie UPS; [6] wszystkie urządzenia informatyczne zamontowano w specjalnie do tego przystosowanych szafach.

W trakcie oględzin serwerowni oraz pomieszczenia, w którym przechowywano kopie zapasowe baz danych Szpitala stwierdzono pozostawione w nich kartonowe pudła oraz urządzenia informatyczne, które nie były podłączone do infrastruktury, co szerzej opisano w dalszej części wystąpienia, w sekcji *Stwierdzone nieprawidłowości*.

(akta kontroli str. 78-109, 435-445)

Oględziny 30 komputerów stacjonarnych Szpitala, w tym 10 obsługiwanych na oddziałach Szpitala przez lekarzy, 10 przez pielęgniarki oraz 10 przez pracowników administracyjnych, wykazały m.in., że:

- na wszystkich zainstalowany był program antywirusowy, posiadający aktualną wersję bazy sygnatur wirusów,
- w jednym komputerze zostały zablokowane porty USB, w pozostałych komputerach porty USB nie zostały zablokowane,
- na 28 komputerach użytkownicy posiadali ograniczone uprawnienia w systemie operacyjnym, które nie pozwalały na wprowadzanie zmian w konfiguracji tych urządzeń oraz instalację oprogramowania. Na dwóch komputerach powiodła się próba instalacji programu z nośnika zewnętrznego (pendrive),
- wszystkie komputery poddane oględzinom funkcjonowały poza systemem domenowym,
- na 20 komputerach wykorzystywany był program do przetwarzania danych medycznych HIPOKRATES, a na 10 przetwarzano dane osobowe pracowników Szpitala,
- dostęp do systemu operacyjnego (Windows) na 25 komputerach wymagał podania loginu i hasła;
- w 1 komputerze użytkowanym przez lekarza, po wprowadzeniu hasła w BIOS-ie uruchamiał się system operacyjny Windows;
- w przypadku 4 komputerów dostęp do systemu operacyjnego nie wymagał podania loginu i hasła;
- użytkownicy 3 komputerów przy logowaniu do systemu operacyjnego wykorzystywali przypisane sobie, unikalne dane uwierzytelniające (login i hasło);
- logowanie do systemu operacyjnego na 14 komputerach wymagało wprowadzenia loginu i hasła, jednak login nie był unikalny w systemie operacyjnym i nie można było na jego podstawie jednoznacznie określić osoby korzystającej z tego systemu (najczęściej login był nazwą pomieszczenia, w którym znajdował się komputer), ale komputer był użytkowany tylko przez jednego użytkownika i wymagał do uruchomienia wprowadzenia hasła;
- w przypadku 9 komputerów login nie był unikalny w systemie operacyjnym oraz nie można było na jego podstawie jednoznacznie określić osoby korzystającej z tego systemu (najczęściej login był nazwą pomieszczenia, w którym znajdował się komputer), a z tych samych danych uwierzytelniających korzystało kilku użytkowników;
- hasła do systemu operacyjnego posiadały długość wymagana przepisami wewnętrznymi.
- na 14 komputerach zainstalowany był system operacyjny Windows XP, na 2 komputerach zainstalowany był system operacyjny Windows Vista. Uwzględniając, iż producent zakończył wsparcie techniczne systemu Windows XP i Windows Vista, taki stan może w przyszłości stwarzać ryzyko dla bezpieczeństwa infrastruktury informatycznej dostęp do programu HIPOKRATES

służącego do przetwarzania danych medycznych pacjentów wymagał podania loginu i hasła. Login był identyfikowalny do użytkownika i odpowiadał danym osoby, która go wykorzystywała.

(akta kontroli str. 370-389)

Kopie bezpieczeństwa baz danych Szpitalnego Systemu Informacyjnego wykonywane były w sposób zautomatyzowany jeden raz na dobę poza godzinami pracy. Kopia bezpieczeństwa swoim zakresem obejmowały wszystkie bazy danych wchodzące w skład Szpitalnego Systemu Informacyjnego. Sprawdzenie poprawności wykonania kopii baz danych polegało na codziennej analizie ostatniego logu – plik tekstowy zawierający zapis wszystkich procedur wykonywania kopii bezpieczeństwa oraz ich rezultatu. Plik ten przechowywany był razem z każdą dobową kopią bezpieczeństwa. Ostatnia kopia bezpieczeństwa była okresowo sprawdzana pod kątem jej przydatności do odtworzenia danych w przypadku awarii systemu. Kopie bezpieczeństwa przechowywane były na serwerze backupowym zlokalizowanym w odpowiednio zabezpieczonym pomieszczeniu w osobnym budynku. W posiadaniu szpitala było 9 laptopów. Nie były przeznaczone do przetwarzania danych osobowych i nie stosowało się na tych urządzeniach ochrony kryptograficznej nośników pamięci (dysków twardych).

(akta kontroli str. 392)

Stwierdzone nieprawidłowości

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

1. Opaski na nadgarstkach pacjentów dwóch oddziałów[46] poddanych oględzinom zawierały widoczne imię i nazwisko pacjenta. Było to niezgodne z art. 36 ust. 5 ustawy z dnia 15 kwietnia 2011 r. o działalności leczniczej[47] oraz § 1 ust. 1, § 3 pkt 1) rozporządzenia Ministra Zdrowia z 20 września 2012 r. *w sprawie warunków, sposobu i trybu zaopatrywania pacjentów szpitala w znaki identyfikacyjne oraz sposobu postępowania w razie stwierdzenia ich braku*[48], które stanowią, że opaska zawierać powinna informacje zapisane w sposób uniemożliwiający identyfikację pacjenta przez osoby nieuprawnione.

   Dyrektor Szpitala wyjaśnił, że *RODO, choć wyraźnie wprowadza zasadę minimalizacji danych, nie ma na celu wprowadzenia całkowitej anonimizacji życia społecznego. Jest to szczególnie istotne w przypadku podmiotów leczniczych, musimy bowiem zwrócić uwagę, że wartość, jaką jest życie i zdrowie pacjenta, ma szczególne znaczenie i nie powinna być zagrożona przez działania mające na celu ochronę prywatności. Identyfikacja pacjenta jest kluczowa dla jego bezpieczeństwa. Może się np. zdarzyć sytuacja, że hospitalizowany pacjent opuści swoją salę i zasłabnie, bez opaski będzie trudno określić jego personalia. Leczymy przede wszystkim pacjentów wiekowych, z upośledzoną świadomością, gdzie kontakt jest utrudniony. Nie zawsze są w stanie podać swoje imię i nazwisko, a lekarz musi mieć pewność, że ma do czynienia z konkretnym chorym. Zgodnie z motywem 4 RODO przetwarzanie danych osobowych należy zorganizować w taki sposób, aby służyło ludzkości. Prawo do ochrony danych osobowych nie jest prawem bezwzględnym, należy je postrzegać w kontekście jego funkcji społecznej i wyważyć względem innych praw podstawowych w myśl zasady proporcjonalności. Ponadto Art. 9 ust. 2 lit. c pozwala na przetwarzanie danych osobowych niezbędnych do ochrony żywotnych interesów osoby, której dane*

[46] Oddział Neurologiczny i Oddział Chorób Wewnętrznych.

[47] Dz. U. z 2018 r. poz. 2190, ze zm.

[48] Dz. U. poz. 1098.

*dotyczą. Zgodnie z art. 9 ust. 2 lit. h RODO przetwarzanie danych osobowych dotyczących stanu zdrowia możliwe jest, gdy jest niezbędne do celów profilaktyki zdrowotnej, diagnozy medycznej, zapewnienia opieki zdrowotnej, leczenia lub zarządzania systemami i usługami opieki zdrowotnej lub zabezpieczenia społecznego na podstawie prawa państwa członkowskiego. RODO jako akt prawny o najszerszym zasięgu podlega zasadzie pierwszeństwa, która została wykształcona w orzecznictwie Trybunału Sprawiedliwości UE. Jest ona jedną z najważniejszych zasad określających stosunek prawa unijnego do prawa wewnętrznego państw członkowskich. W teorii oznacza pierwszeństwo stosowania prawa UE przed prawem krajowym państw członkowskich.*

NIK zauważa, że przepisy ustawy o działalności leczniczej i ww. rozporządzenia Ministra Zdrowia, wprowadzające obowiązek stosowania u pacjentów opasek identyfikacyjnych oznaczonych w sposób uniemożliwiający identyfikację pacjenta przez osoby nieuprawnione, nie są sprzeczne z RODO i nie zostały uchylone w związku z wejściem w życie tego rozporządzenia.

(akta kontroli str. 448-449)

2. W przypadku pięciu pracowników dostęp do programu Hipokrates przyznany został na wniosek samego pracownika zaakceptowany przez administratora systemu informatycznego, co było niezgodne z obowiązującą w Szpitalu Polityką Bezpieczeństwa, zgodnie z którą Dyrektor Szpitala określa, kto z podległych mu pracowników ma mieć konto w systemie informatycznym, określa uprawnienia użytkownika i wnioskuje o zmianę tych uprawnień. Wnioski o przyznanie dostępu przypadku trzech osób uzasadniono *usprawnieniem pracy kancelarii i sekretariatu szpitala związanej z rozdzielaniem pism do dekretacji, co wiąże się z koniecznością nadania ww. uprawnień.* Obowiązek wydawania przez administratora danych upoważnień do przetwarzania danych osobowych wynika z art. 29 RODO, a przed wejściem w życie tego rozporządzenia wynikał z art. 37 ustawy o ochronie danych osobowych z dnia 29 sierpnia 1997 r.[49]

   Dyrektor Szpitala, nie wyjaśnił powodów wydania upoważnień tej grupie pracowników przez ASI zamiast ADO. Na pytanie o przyczyny wydania upoważnień tym pracownikom podał, że o*becnie w SN ZOZ obowiązuje „odręczny" system dekretowania pism przez dyrekcję, celem ich załatwienia przez pracowników. Po wdrożeniu (połowa 2019 r.) elektronicznego systemu obiegu dokumentacji, proces ten będzie odbywał się wyłącznie w nim. W związku z przeprowadzoną reorganizacją struktury organizacyjnej SN ZOZ, niektóre komórki otrzymały szerszy niż dotychczas zakres obowiązków i w związku z tym zaistniała konieczność nadania uprawnień.*

   (akta kontroli str. 603-606)

3. Analiza upoważnień do przetwarzania danych osobowych wykazała, że jedna pielęgniarka posiadająca dostęp do programu Hipokrates (z 30 poddanych analizie) nie posiadała potwierdzenia nadania jej przez ADO pisemnego upoważnienia do przetwarzania danych osobowych. Było to niezgodne z art. 29 i art. 32 ust. 4 RODO, które wskazują, że administrator danych podejmuje działania w celu zapewnienia, by każda osoba fizyczna mająca dostęp do danych osobowych przetwarzała je wyłącznie na podstawie upoważnienia ADO i na jego polecenie. Z informacji uzyskanych z Działu Kadr, wynika, że osoba ta była obecna w pracy w okresie 10.10.2017-15.11.2017 r., a następnie przebywała na zwolnieniu oraz urlopach macierzyńskim, rodzicielskim

[49] Dz. U. z 2016 r. poz. 922, ze zm.

i wypoczynkowym). Obowiązek wydawania przez administratora danych upoważnień do przetwarzania danych osobowych przed wejściem w życie RODO wynikał z art. 37 ustawy o ochronie danych osobowych z dnia 29 sierpnia 1997 r.

Dyrektor Szpitala wyjaśnił, *że* przed wejściem w życie przepisów RODO (maj 2018) i obecnie (kwiecień 2019), pracownik ten jest trwale nieobecny w pracy.

(akta kontroli str. 603-607)

4. Szpital nie odebrał uprawnień do programu Hipokrates pięciu byłym pracownikom Szpitala (pracownicy posiadali aktywne konto), mimo, że od rozwiązania z nimi stosunku pracy minęło od 55 do 243 dni (według stanu na dzień 27 marca 2019 r.).

   Zgodnie z art. 5 pkt 1 lit. c RODO, przetwarzane dane osobowe powinny być adekwatne, stosowne oraz ograniczone do tego, co niezbędne do celów, w których są przetwarzane (zasada minimalizacji danych). Ponadto w świetle treści § 20 ust. 2 pkt 4 i 5 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[50], należy podejmować działania polegające na bezzwłocznej zmianie uprawnień, w przypadku zmiany zadań osób zaangażowanych w proces przetwarzania informacji. W tym kontekście, przedmiotowe uprawnienia byłych pracowników SPZOZ powinny być im odebrane niezwłocznie po wygaśnięciu stosunku pracy.

   Dyrektor SPZOZ wyjaśnił, że pracownicy szpitala nie mieli wpisanej w systemie informatycznym Hipokrates daty zakończenia możliwości logowania do systemu, natomiast byli pozbawieni praw do aplikacji potrzebnych do wglądu i edycji danych. Data zakończenia możliwości logowania została już potwierdzona i użytkownicy są nieaktywni.

   (akta kontroli str. )

5. W dwóch z 18 analizowanych zgłoszeniach za pośrednictwem systemu help desk zamieszczono niezanonimizowane dane osobowe dwóch pacjentów: imię, nazwisko i pesel, a w jednym z tych przypadków także informację o rodzaju wykonywanego pacjentowi badania. Było to niezgodne z wyrażoną w art. 5 pkt 1 lit. c RODO zasadą adekwatności i minimalizacji danych.

   Kierownik Sekcji Informatyki Szpitala wyjaśnił, że SPZOZ jest aktualnie na etapie wdrożenia projektu e-zdrowie, w związku z czym jest dość duże zamieszanie i ogrom pracy. Umowa z firmą Asseco Poland S.A. została zawarta dnia 6 marca 2018 r., jeszcze przed wejściem RODO. Wyjaśniam, iż w tych dwóch przypadkach konieczne było podanie danych ze względu na szybką reakcję ze strony Wykonawcy i potrzebę zastosowania konkretnego, szybkiego rozwiązania (brak możliwości innej identyfikacji problemu). Przy kolejnych zgłoszeniach tego typu wszystkie dane będą zanonimizowane przed wysłaniem na help desk do wykonawcy.

   (akta kontroli str. 478-478)

6. W trakcie oględzin serwerowni oraz pomieszczenia, w którym przechowywano kopie zapasowe baz danych Szpitala znajdowały się kartonowe pudła oraz urządzenia informatyczne, które nie były podłączone do infrastruktury. Część

z tych przedmiotów była łatwopalne. Serwerownia, z uwagi na prawdopodobieństwo wystąpienia przegrzania macierzy dyskowych lub przepięcia elektrycznego nie powinna być miejscem do ich składowania.

Dyrektor Szpitala wyjaśnił, że *elementy wyposażenia były przechowywane w serwerowni tylko tymczasowo przez bardzo krótki okres. Elementy wyposażenia takie jak pudło kartonowe, sprzęt elektroniczny oraz kilka nowych komputerów zostały usunięte z serwerowni.*

(akta kontroli str. 598)

7. Podczas oględzin 30 komputerów stacjonarnych Szpitala (po 10 obsługiwanych przez lekarzy, pielęgniarki i pracowników administracyjnych), stwierdzono następujące naruszenia bezpieczeństwa danych przechowywanych w postaci elektronicznej:
   - dwóch użytkowników komputerów posiadało uprawnienia administratora (powiodła się próba instalacji programu z nośnika zewnętrznego), chociaż nie wykonywali czynności związanych z zapewnieniem prawidłowego działania sieci komputerowej. Posiadanie takich uprawnień było niezgodne z § 20 ust. 2 pkt 4 rozporządzenia KRI, według którego zarządzanie bezpieczeństwem informacji realizowane jest w szczególności przez podejmowania działań zapewniających, że osoby zaangażowane w proces przetwarzania informacji posiadają stosowne uprawnienia i uczestniczą w tym procesie w stopniu adekwatnym do realizowanych przez nie zadań oraz obowiązków, mających na celu zapewnienie bezpieczeństwa informacji;
   - w przypadku 4 komputerów, dostęp do systemu operacyjnego nie wymagał podania loginu i hasła, na 14 komputerach login nie był unikalny w systemie operacyjnym i nie można było na jego podstawie jednoznacznie określić osoby korzystającej z tego systemu, a na 9 login nie był unikalny w systemie operacyjnym i z tych samych danych uwierzytelniających (login i hasło) korzystało kilku użytkowników.

     Było to niezgodne z obowiązująca w Szpitalu IZSI, zgodnie z którą osoba upoważniona lub użytkownik systemu informatycznego upoważniony do dostępu do danych osobowych otrzymuje od ASI identyfikator (login) umożliwiający dostęp do systemu. Identyfikator jest unikalny w ramach systemu oraz jest jawny tzn. pozwala ASI i innym osobom upoważnionym jednoznacznie określić osobę korzystająca z systemu i podlega rejestracji w systemie informatycznym. Działanie to było również niezgodne z § 20 ust. 2 pkt 7 lit. a i § 21 ust. 2 pkt 3, w związku z § 20 ust. 1 rozporządzenia KRI, gdyż bez przyznania indywidualnych loginów użytkownikom, nie była możliwa prawidłowa rozliczalność systemów. Przy takich rozwiązaniach nie jest możliwe do ustalenia, która z osób fizycznych używających tego samego (jednego) loginu, przetwarzała w systemach (w tym przypadku w systemie operacyjnym) dane podlegające prawnej ochronie. Jednocześnie, zgodnie z motywem 39 preambuły RODO, dane osobowe powinny być przetwarzane w sposób zapewniający im odpowiednie bezpieczeństwo i odpowiednią poufność, w tym ochronę przed nieuprawnionym dostępem do nich i do sprzętu służącego ich przetwarzaniu oraz przed nieuprawnionym korzystaniem z tych danych i z tego sprzętu.

   (akta kontroli str. 78-113, 370-389)

Dyrektor Szpitala wyjaśnił, że Szpital aktualnie jest na etapie wdrożenia projektu e-zdrowie, czyli również na etapie wymiany przestarzałych komputerów bez

wsparcia technicznego producenta dla użytkowników, personelu Szpitala. Systematyczna i codzienna wymiana komputerów powoduje naprawę wymienionych nieścisłości takich jak logowanie użytkowników do systemu operacyjnego. Na czterech zidentyfikowanych komputerach system wymusza wprowadzenie hasła do systemu operacyjnego, na dwóch zidentyfikowanych nie ma możliwości zainstalowania przez użytkownika programu wprowadzonego na nośniku zewnętrznym.

(akta kontroli str. 586-598)

**OCENA CZĄSTKOWA**

Najwyższa Izba Kontroli negatywnie ocenia niezapewnienie przez Szpital prawidłowego przetwarzania i ochrony danych osobowych.

# IV. Wnioski

W związku ze stwierdzonymi nieprawidłowościami, Najwyższa Izba Kontroli, na podstawie art. 53 ust. 1 pkt 5 ustawy o NIK, wnosi o:

Wnioski

1. Dokonanie przeglądu i aktualizacji regulacji wewnętrznych dotyczących ochrony danych osobowych.
2. Przeprowadzenie szkoleń dotyczących ochrony danych osobowych oraz szkoleń uwzględniających zagadnienia z zakresu bezpieczeństwa informacji określone w § 20 ust. 2 pkt 6 rozporządzenia KRI dla wszystkich pracowników zaangażowanych w proces przetwarzania informacji.
3. Zaopatrywanie opasek identyfikacyjnych pacjentów w znaki nieujawniające imion i nazwisk pacjentów osobom postronnym.
4. Udzielanie upoważnień do przetwarzania danych osobowych zgodnie z RODO i uregulowaniami wewnętrznymi.
5. Bezzwłoczne odbieranie upoważnień w systemach informatycznych byłym pracownikom.
6. Dokonywanie zgłoszeń serwisowych w sposób zapewniający ochronę danych osobowych pacjentów.
7. Nadanie wszystkim użytkownikom komputerów indywidualnych danych do autoryzacji w systemach operacyjnych oraz wprowadzenie rozwiązań uniemożliwiających pracę kilku osób na jednym koncie użytkownika.

# 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 Lublinie. 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.

Obowiązek poinformowania NIK o sposobie wykorzystania uwag i wykonania wniosków

Zgodnie z art. 62 ustawy o NIK należy poinformować Najwyższą Izbę Kontroli, w terminie 21 dni od otrzymania wystąpienia pokontrolnego, o sposobie 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.

Lublin, 23 kwietnia 2019 r.

Kontrolerzy
Agnieszka Bury
doradca prawny

.....
*podpis*

Monika Cieniuch
starszy inspektor kontroli państwowej

.....
*podpis*

Dyrektor
Delegatury Najwyższej Izby Kontroli
w Lublinie
Edward Lis

.....
*Podpis*