NAJWYŻSZA IZBA KONTROLI
Delegatura w Poznaniu

LPO.410.002.04.2019

Cezary Chmielecki
Dyrektor Samodzielnego Publicznego Zakładu
Opieki Zdrowotnej w Kole
ul. Księcia Józefa Poniatowskiego 25, 62-600 Koło

WYSTĄPIENIE POKONTROLNE

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

NAJWYŻSZA IZBA KONTROLI
Delegatura w Poznaniu
ul. Dożynkowa 9H, 61-662 Poznań
T +48 61 655 62 00, F +48 61 655 62 01
lpo@nik.gov.pl

I. Dane identyfikacyjne

Jednostka kontrolowana	Samodzielny Publiczny Zakład Opieki Zdrowotnej w Kole, ul. Księcia Józefa Poniatowskiego 25, 62-600 Koło (dalej: Szpital albo SPZOZ)
Kierownik jednostki kontrolowanej	Cezary Chmielewski, Dyrektor SPZOZ w Kole, od 21 października 2015 r. (dalej: Dyrektor)
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 27 lutego 2019 r.
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 Poznaniu
Kontroler	Tomasz Otworowski, specjalista kontroli państwowej, upoważnienie do kontroli nr LPO/11/2019 z 14 stycznia 2019 r. (akta kontroli str. 1-2)

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

II. Ocena ogólna[2] kontrolowanej działalności

OCENA OGÓLNA

Dane osobowe przetwarzane przez Szpital w okresie od 25 maja 2018 r. do 27 lutego 2019 r.[3] były co do zasady prawidłowo chronione. W okresie objętym kontrolą, SPZOZ posiadał opracowaną i wdrożoną Politykę Bezpieczeństwa Informacji[4] (dalej: Polityka), służącą zapewnieniu realizacji celów i zadań z zakresu ochrony danych osobowych. Realizacja tych zadań następowała w sposób zgodny z prawem i efektywny, przy zapewnieniu odpowiedniego stopnia ochrony praw i wolności osób fizycznych w związku z przetwarzaniem ich danych osobowych.

Szpital prawidłowo wyznaczył IOD oraz zapewnił przeszkolenie personelu w zakresie przepisów o ochronie danych osobowych. W SPZOZ prowadzono rejestr czynności przetwarzania tych danych oraz dokonano analizy procesów ich przetwarzania. Pomimo wdrożenia i funkcjonowania Polityki i regulaminu organizacyjnego Szpitala, nie przeprowadzono jednak ich przeglądu i aktualizacji. Od 2018 r. nie sporządzano także planu sprawdzeń oraz sprawozdania rocznego stanu funkcjonowania systemu ochrony danych osobowych SPZOZ.

Obowiązujące w Szpitalu rozwiązania techniczne i organizacyjne co do zasady zapewniały prawidłowe przetwarzanie i ochronę danych osobowych. Personel SPZOZ posiadał, adekwatne do wykonywanych obowiązków, prawo dostępu do zbioru danych osobowych w zintegrowanym systemie informatycznym. Szpital nie zaktualizował natomiast zakresu pisemnego upoważnienia do przetwarzania danych osobowych jednego zatrudnionego pracownika i nie usunął z tego systemu pięciu kont byłych pracowników. Właściwie udostępniano dokumentację medyczną pacjentów i zawierano wymagane umowy powierzenia przetwarzania danych osobowych. Podejmowano też odpowiednie działania w celu minimalizacji ryzyka utraty tych danych, jednak nie zapewniono odrębnego pomieszczenia dla serwera kopii zapasowej. Stwierdzono też przypadki przechowywania na komputerach służbowych dokumentacji medycznej pacjentów bez uzasadnionego powodu, co w sytuacji braku wdrożenia zindywidualizowanego sposobu logowania do systemów operacyjnych komputerów, wymaganego Polityką, mogło stwarzać zagrożenie dla bezpieczeństwa takich danych i wiązało się z ryzykiem ich ujawnienia osobom nieuprawnionym. Nie wyeliminowano również takiego ryzyka w zakresie danych pacjentów zamieszczonych na tablicach z ruchem chorych.

[2] Najwyższa Izba Kontroli formułuje ocenę ogólną jako ocenę pozytywną, ocenę negatywną albo ocenę w formie opisowej.
[3] Dalej: okres objęty kontrolą.
[4] Zarządzenie Nr 25/2017 Dyrektora SPZOZ z 6 lipca 2017 r.

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. W dniu 18 sierpnia 2018 r. Dyrektor, zgodnie z obowiązkiem wynikającym z art. 8 ustawy z dnia 10 maja 2018 r. o ochronie danych osobowych[6] i art. 37 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] (dalej: RODO) wyznaczył Inspektora Ochrony Danych (dalej: IOD). Do jego obowiązków należało wykonywanie zadań IOD wynikających z RODO oraz ustawy o ochronie danych osobowych.

Dyrektor, jako Administrator Danych Osobowych[8] (dalej: ADO), realizując obowiązek określony w art. 10 ust. 1 ustawy o ochronie danych osobowych terminowo powiadomił[9] Prezesa Urzędu Ochrony Danych Osobowych o wyznaczeniu IOD, tj. w ciągu 14 dni od jego wyznaczenia. W zawiadomieniu ujęto wszystkie dane, o których mowa w art. 10 ust. 1 i 3 ustawy o ochronie danych osobowych.

Dane obejmujące imię i nazwisko oraz adres poczty elektronicznej IOD zamieszczone zostały na stronie internetowej Szpitala, zgodnie z art. 11 ustawy o ochronie danych osobowych.

IOD posiadał odpowiednie kwalifikacje do pełnienia tej funkcji m.in. z uwagi na ukończenie szkolenia doskonalącego dla inspektorów danych osobowych w maju 2018 r. oraz szkolenia w zakresie stosowania przepisów ochrony danych osobowych w sektorze medycznym we wrześniu 2018 r.

Poprzednio, do dnia 17 sierpnia 2018 r., w SPZOZ obsadzone było stanowisko Administratora Bezpieczeństwa Informacji[10] (dalej: ABI), przez inną osobę. Osoba pełniąca tę funkcję legitymowała się ukończonymi w 2017 r. studiami podyplomowymi w zakresie ochrony danych osobowych i informacji niejawnych.

Strukturę organizacyjną Szpitala, określono w Regulaminie Organizacyjnym SPZOZ w Kole[11], którego jednak nie zaktualizowano w zakresie powołania IOD (co szerzej opisano w sekcji „stwierdzone nieprawidłowości").

(akta kontroli str. 343-357, 449-452)

SPZOZ 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[12]. Z wyjaśnień Dyrektora wynikało, że SPZOZ nie uzyskał takiej decyzji w związku z brakiem w swojej strukturze organizacyjnej szpitalnego oddziału ratunkowego.

(akta kontroli str. 339-342)

[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 (dalej: ustawa o ochronie danych osobowych). Weszła w życie 25 maja 2018 r.
[7] Dz. Urz. UE L 119 z 4 maja 2016 r., str. 1 ze zm.
[8] W rozumieniu art. 4 pkt 7 RODO. Wejście w życie 24 maja 2016 r. Rozpoczęcie stosowania 25 maja 2018 r.
[9] 30 sierpnia 2018 r.
[10] O którym mowa w art. 36a ustawy z dnia 29 sierpnia 1997 r. o ochronie danych osobowych (Dz. U. z 2016 r. poz. 922 ze zm., uchylona z dniem 6 lutego 2019 r.), dalej: ustawa o ochronie danych osobowych z 1997 r.
[11] Załącznik do Uchwały Nr 1/VI/2017 Rady Społecznej przy SPZOZ w Kole z 21 grudnia 2017 r., dalej: Regulamin Organizacyjny.
[12] Dz. U. z 2018 r. poz. 1560.

1.2. W okresie objętym kontrolą w Szpitalu obowiązywała, wprowadzona w lipcu 2017 r., Polityka wraz z Instrukcją Zarządzania Systemem Informatycznym Ochrony Danych Osobowych, stanowiącą jej integralną część (dalej: Instrukcja). Polityka określała zasady postępowania w zakresie bezpieczeństwa ochrony danych osobowych. Celem tej Polityki było zapewnienie właściwego przetwarzania danych, zbieranie ich dla oznaczonych, zgodnych z prawem celów, niepoddawanie danych osobowych dalszemu przetwarzaniu niezgodnemu z celami ich gromadzenia, przetwarzanie danych oraz przechowywanie ich w postaci umożliwiającej identyfikację osób, których dotyczą nie dłużej niż było to niezbędne do osiągniecia celu przetwarzania. Polityka odnosiła się do danych osobowych przetwarzanych w zbiorach tradycyjnych (forma papierowa) oraz w systemach informatycznych.

Polityka określała również zadania i obowiązki ABI, zastąpionego od 18 sierpnia 2018 r. przez IOD, do których należało m.in.: sprawdzanie zgodności przetwarzania danych osobowych z obowiązującymi przepisami, aktualizacje dokumentacji bezpieczeństwa danych osobowych, zapoznanie osób upoważnionych do przetwarzania danych osobowych z obowiązującymi w Szpitalu zasadami oraz dokonywanie analizy stanu ochrony danych.

Instrukcja określała zasady bezpieczeństwa danych osobowych przetwarzanych w systemach informatycznych.

W Szpitalu nie sporządzono planu sprawdzeń na 2018 r. oraz sprawozdania stanu systemu ochrony danych osobowych za 2018 r., których obowiązek przygotowania wynikał z obowiązującej Polityki. Ponadto, po rozpoczęciu od 25 maja 2018 r. stosowania RODO, IOD nie przeprowadził przeglądu i aktualizacji obowiązującej Polityki. Kwestie te szerzej opisano w dalszej części wystąpienia, w sekcji *„stwierdzone nieprawidłowości”.*

Zasady ochrony danych osobowych w SPZOZ określały również dodatkowe instrukcje i procedury dotyczące: monitoringu wizyjnego[13], udostępniania dokumentacji medycznej[14], zaopatrywania pacjentów w znaki identyfikacyjne[15]. Ponadto, na stronie internetowej Szpitala zamieszczono informacje dla pacjentów o wprowadzonych zasadach przetwarzania danych osobowych, gdzie jako podstawę prawną podano RODO, wskazano właściwe dane kontaktowe i obowiązki wyznaczonego IOD oraz podano klauzulę informacyjną dla osób, od których dane osobowe miały być pozyskiwane. Treść tej klauzuli spełniała wymogi określone w art. 13 RODO. Sposób wprowadzenia Polityki wśród pracowników został opisany w pkt 1.6 wystąpienia.

(akta kontroli str. 10-149, 158-201, 343-347)

1.3. Zgodnie z obowiązkiem wynikającym z art. 30 ust. 3 RODO, w Szpitalu prowadzono rejestr czynności przetwarzania w formie pisemnej, w tym elektronicznej (arkusz Excel). Rejestr czynności zawierał wszystkie elementy określone w art. 30 ust. 1 RODO tj. nazwy czynności przetwarzania (41 pozycji), cel i kategorię osób i danych, które były przetwarzane, planowane terminy usunięcia poszczególnych kategorii danych, kategorie odbiorców, których dane osobowe zostały ujawnione oraz ogólny opis technicznych i organizacyjnych środków bezpieczeństwa stosowanych zgodnie z wymaganiami art. 32 ust. 1 RODO. Rejestr zawierał również nazwę ADO oraz IOD wraz z danymi kontaktowymi.

(akta kontroli str. 150-157)

[13] „Instrukcja Zarządzania Systemem Monitoringu Wizyjnego w Samodzielnym Publicznym Zakładzie Opieki Zdrowotnej w Kole” – SPZOZ.ABI.I.1.1.2017 z 31 sierpnia 2017 r.

[14] „Instrukcja Udostępniania Dokumentacji Medycznej na Zewnątrz Samodzielnego Publicznego Zakładu Opieki Zdrowotnej w Kole” – SPZOZ/DSM/I/1/1/13 z 1 lutego 2013 r.

[15] „Procedura zaopatrywania pacjentów dorosłych, dzieci i noworodki w znaki identyfikacyjne” – SPZOZ.PP.SPO.11.1.2017 z 1 sierpnia 2018 r.

1.4. W Szpitalu dokonano analizy ryzyka, o której mowa w art. 32 RODO, stanowiącej Załącznik nr 2 do Polityki w obszarze bezpieczeństwa sprzętowego i czynnika ludzkiego. W wyniku analizy wyodrębniono 31 możliwych do wystąpienia ryzyk m.in.: włamania, kradzieży, pożaru, zalania, awarii, uzyskania dostępu przez osobę nieupoważnioną, błędu i złośliwego działania użytkowników, używania prostych haseł, utraty danych z lokalnych dysków oraz braku kopii danych. Dla każdego z ryzyk określono prawdopodobieństwo i skutek oraz oszacowano jego wartość. Największą wartość oszacowanego ryzyka przypisano możliwości wystąpienia ataków wirusów komputerowych, awarii UPS, stacji roboczej i serwerów oraz uszkodzeń spowodowanych przez wyładowania atmosferyczne. W przypadku 24 ryzyk, których oszacowana wartość była na poziomie 10 punktów i wyższym[16] wskazano działania zapobiegawcze i korygujące. Rekomendowane działania, które zostały podjęte bezpośrednio przed wdrożeniem Polityki, dotyczyły m.in.: zapewnienia aktualnej wersji systemu antywirusowego, okresowego sprawdzania poprawności działania UPS, zapewnienia ochrony przepięciowej oraz innych systemów alarmowych, wykonywania kopii danych serwera, zapewnienia odpowiedniego poziomu złożoności haseł i okresowej ich wymiany oraz podnoszenia świadomości pracowników.

(akta kontroli str. 41-42, 443-447)

1.5. W Szpitalu nie została wykonana ocena skutków dla ochrony danych, o której mowa w art. 35 RODO. Obowiązek wykonania tej oceny dotyczył 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. Prezes UODO w komunikacie wydanym na podstawie art. 35 ust. 4 RODO[17] 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 stanowiła czynność fakultatywną, przy czym Grupa Robocza ds. Ochrony Osób Fizycznych w Zakresie Przetwarzania Danych Osobowych[18] zdecydowanie zalecała dokonanie takiej oceny dla operacji przetwarzania już trwających przed 25 maja 2018 r.[19] oraz w przypadkach, gdy nie jest jasne, czy wymagana jest ocena, ponieważ jest ona „przydatnym narzędziem, które może pomóc administratorom danych w zapewnieniu zgodności z prawem ochrony danych". Dyrektor oraz IOD wyjaśnili, że w trakcie opracowania nowej polityki bezpieczeństwa, której wprowadzenie przewidziano na początek II kwartału 2019 r. zostanie uaktualniony również rejestr czynności przetwarzania danych oraz przeprowadzona zostanie nowa ocena ryzyka zagrożeń związanych z przetwarzaniem danych osobowych. W związku z tym zostanie przeprowadzona również analiza procesów przetwarzania danych osobowych oraz dokonana ocena skutków dla ochrony danych.

(akta kontroli str. 343-347)

[16] Powyżej poziomu ryzyka akceptowalnego tj. dziewięć punktów.

[17] 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).

[18] Grupa Robocza została powołana na podstawie art. 29 dyrektywy 95/46/WE Parlamentu Europejskiego i Rady z dnia 24 października 1995 r. w sprawie ochrony osób fizycznych w zakresie przetwarzania danych osobowych i swobodnego przepływu tych danych (Dz. Urz. UE L 281 z 24 października 1995 r., str. 31). Jest 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 Parlamentu Europejskiego i Rady z dnia 12 lipca 2002 r. dotyczącej przetwarzania danych osobowych i ochrony prywatności w sektorze łączności elektronicznej (Dz. Urz. UE L 201 z 12 lipca 2002 r., str. 37).

[19] 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 dostęp z dnia 21 lutego 2019 r.

1.6. Szpital zorganizował szkolenie w sprawie przetwarzania danych osobowych w lipcu 2017 r. tj. bezpośrednio przed wprowadzeniem Polityki. Zakres szkolenia obejmował wprowadzenie planowanych zmian prawnych na rynku usług medycznych wynikających z RODO. Szkolenie zostało przeprowadzone przez podmiot zewnętrzny i objęto nim wszystkich 338 zatrudnionych pracowników SPZOZ.

W późniejszym okresie, do sierpnia 2018 r. Szpital zorganizował kolejne szkolenia, którym objęto łącznie 189 nowo zatrudnionych pracowników. Szkolenie to przeprowadził ABI, działający później jako IOD. Ponadto IOD udostępnił pracownikom Szpitala na serwerze wewnętrznym prezentację multimedialną dotyczącą ochrony danych osobowych. Kolejne szkolenie (przypominające) z zakresu ochrony danych Szpital planował przeprowadzić w II kwartale 2019 r.

Nie stwierdzono udokumentowania przeszkolenia z ochrony danych osobowych ośmiu pracowników zatrudnionych na umowę o pracę od 1 września 2018 r. do 20 lutego 2019 r. Z wyjaśnień Dyrektora oraz IOD wynikało, że osoby te zostały zapoznane z zasadami ochrony danych osobowych ustnie, a z uwagi na opracowywanie nowej polityki bezpieczeństwa informacji, w tym nowych druków oświadczeń odstąpiono od odrębnego dokumentowania przeprowadzenia szkolenia poza ujęciem tych pracowników w ewidencji osób upoważnionych do przetwarzania danych osobowych.

(akta kontroli str. 227, 339-342, 373-378)

1.7. W Szpitalu nie stosowano kodeksu dobrych praktyk ani medycznego kodeksu branżowego. Z wyjaśnień Dyrektora Szpitala wynikało, że Szpital oczekuje na zatwierdzenie „Kodeksu postępowania dla sektora ochrony zdrowia wydanego zgodnie z art. 40 RODO dot. podmiotów wykonujących działalność leczniczą i podmiotów przetwarzających”[20] przez Prezesa UODO, po czym Kodeks zostanie wprowadzony do stosowania. Natomiast sposoby postępowania określone w „Przewodniku po RODO w służbie zdrowia” opracowanym przez Grupę Roboczą ds. Ochrony Danych Osobowych działającą w Ministerstwie Cyfryzacji, opublikowanym we wrześniu 2018 r. zostały już częściowo wdrożone w Szpitalu, a pozostałe wytyczne zostaną ujęte w aktualizowanej Polityce

(akta kontroli str. 339-342, 443-447)

Stwierdzone nieprawidłowości

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

1. Pomimo rozpoczęcia stosowania w dniu 25 maja 2018 r. RODO nie dokonano przeglądu i aktualizacji obowiązującej w SPZOZ Polityki i Regulaminu Organizacyjnego.

1.1. We wprowadzonej w lipcu 2017 r. Polityce na dzień 29 stycznia 2019 r. nadal odnoszono się do nieobowiązującego stanu prawnego oraz ustanowionego ABI, pomimo że podstawa prawna jego wyznaczenia, tj. art. 36a ustawy o ochronie danych osobowych z 1997 r. utraciła moc, a w miejsce ABI 18 sierpnia 2018 r. powołano IOD (w oparciu o art. 8 ustawy o ochronie danych osobowych w zw. z art. 37 RODO). Nieprzeprowadzenie ww. aktualizacji było niezgodne z art. 24 ust. 1 RODO, w myśl którego obowiązkiem ADO było m.in. wdrożenie odpowiednich środków organizacyjnych, poddawanych w razie potrzeby przeglądom i uaktualnianiu, aby przetwarzanie odbywało się zgodnie z ww. rozporządzeniem i aby móc to wykazać.

Z wyjaśnień Dyrektora oraz IOD wynikało, że prowadzono działania w zakresie opracowania nowej polityki bezpieczeństwa, których zakończenie, z uwagi

[20] Wersja 22 z 13 listopada 2018 r.

na zmiany kadrowe oraz obszerność i zawiłość tematyki przewidziano na początek II kwartału 2019 r.

(akta kontroli str. 10-81, 343-347)

1.2. W strukturze organizacyjnej Szpitala określonej w Regulaminie Organizacyjnym nie wydzielono nowego samodzielnego stanowiska pracy IOD a pozostawiono nieaktualne stanowisko ABI (§ 3 ust. 9 lit. e, tiret 10). Zgodnie z art. 24 ust. 1 pkt 3 ustawy z dnia 15 kwietnia 2011 r. o działalności leczniczej[21] w regulaminie organizacyjnym powinna zostać w szczególności określona struktura organizacyjna zakładu leczniczego. Ponadto, w myśl ww. art. 24 ust. 1 RODO oraz punktu II.A.3 załącznika do komunikatu Nr 23 Ministra Finansów z 16 grudnia 2009 r.[22], administrator wdraża m.in. odpowiednie środki organizacyjne, aby przetwarzanie danych odbywało się zgodnie z tym rozporządzeniem, a struktura organizacyjna jednostki powinna być dostosowana do aktualnych celów i zadań.

Dyrektor Szpitala wyjaśnił, że zaistniała sytuacja wynikała ze zmian kadrowych i braku czasu oraz zadeklarował, że regulamin ten zostanie zaktualizowany w najbliższym możliwym czasie.

(akta kontroli str. 343-347, 443-453)

2. IOD[23], w okresie od stycznia 2018 r. do co najmniej 13 lutego 2019 r., nie przygotowywał planu sprawdzeń, o którym mowa w punkcie 5 i 6 rozdziału XII Polityki i w konsekwencji nie przedstawiał go ADO[24]. Zgodnie z treścią ww. punktów Polityki plan sprawdzeń powinien być przygotowywany na okres nie krótszy niż kwartał i nie dłuższy niż rok. Ponadto IOD nie sporządził za 2018 r. sprawozdania rocznego stanu funkcjonowania systemu ochrony danych osobowych dla ADO, według zasad i wzoru określonych w rozdziale X i XIII Polityki.

Dyrektor oraz IOD przyznali, że ww. dokumentów nie sporządzono. Wskazali, że spowodowane to było m.in. zmianami kadrowymi na stanowisku ABI i IOD, skoncentrowaniem się w pierwszej kolejności na uaktualnieniu dokumentacji do wymogów RODO oraz przygotowywaniem nowej polityki ochrony danych, której wprowadzenie przewidziano na początek II kwartału 2019 r. Dodali, że kompleksowy audyt zostanie przeprowadzony po opracowaniu tej polityki.

(akta kontroli str. 10-82, 369-377)

OCENA CZĄSTKOWA

Szpital prawidłowo wyznaczył IOD oraz zapewnił przeszkolenie personelu w zakresie przepisów o ochronie danych osobowych. W SPZOZ prowadzono rejestr czynności przetwarzania tych danych oraz dokonano analizy procesów ich przetwarzania. Pomimo wdrożenia i funkcjonowania Polityki i Regulaminu Organizacyjnego nie przeprowadzono jednak ich przeglądu i aktualizacji w związku z rozpoczęciem stosowania RODO. Od 2018 r. nie sporządzano także planu sprawdzeń oraz sprawozdania rocznego stanu funkcjonowania systemu ochrony danych osobowych Szpitala.

OBSZAR

2. Zapewnienie prawidłowego przetwarzania i ochrony danych osobowych.

Opis stanu faktycznego

2.1. W Szpitalu wprowadzono i stosowano rozwiązania techniczne i organizacyjne, które nie doprowadziły do ujawnienia danych medycznych pacjentów i nie stwarzały

[21] Dz.U. 2018 r. poz. 2190.
[22] W sprawie standardów kontroli zarządczej dla sektora finansów publicznych (Dz. Urz. MF nr 15 poz. 84).
[23] Według obowiązującej w Szpitalu Polityki był to ABI.
[24] Ostatni plan sprawdzeń zatwierdzony przez ADO dotyczył okresu lipiec-grudzień 2017 r.

istotnego ryzyka wystąpienia takiej sytuacji. Przyjęto rozwiązania polegające na tym, że[25]:

- hospitalizowanych pacjentów zaopatrywano w opaski nadgarstkowe, gdzie dane osobowe umieszczano ręcznie po stronie wewnętrznej opasek, natomiast po stronie widocznej naniesiono dane identyfikacyjne – nr księgi rejestracyjnej. Na łóżkach szpitalnych nie stwierdzono obecności kart pacjentów zawierających informacje o ich stanie zdrowia,

- dane osobowe i medyczne pacjentów były przechowywane w dyżurkach pielęgniarskich oraz w gabinetach lekarskich w zamkniętych szafach, przy czym tablice z ruchem chorych[26] umieszczono na ścianach pomieszczeń dyżurek, co opisano w dalszej części wystąpienia w sekcji „stwierdzone nieprawidłowości",

- nie stwierdzono sytuacji pozostawienia dyżurki i gabinetu lekarskiego bez właściwego nadzoru, w tym pozostawienia niezabezpieczonych komputerów z dostępem do dokumentacji medycznej pacjentów,

- w poradni specjalistycznej wyodrębniono jedno okienko rejestracyjne na ogólnodostępnym, stosunkowo wąskim korytarzu. Przy okienku rejestracyjnym umieszczono informację o wymogu przebywania przy okienku wyłącznie jednej osoby, a ponadto w trakcie oględzin personel rejestracji informował pacjentów o konieczności zachowania odpowiedniego odstępu. W okienku znajdowała się informacja o konieczności przedstawienia dowodu osobistego. Nie stwierdzono sytuacji, w której personel rejestracji posługiwał się nazwiskami pacjentów, a ich identyfikacja odbywała się wyłącznie na podstawie okazanych dowodów osobistych. W obrębie wzroku pacjentów nie były widoczne dane z ekranów komputerów[27] lub dokumenty pacjentów,

- nie stwierdzono wzywania pacjenta do gabinetu poprzez podawanie nazwisk. Kolejność wejścia do gabinetu lekarskiego ustalali sami pacjenci,

- w gabinetach poradni specjalistycznych, w obrębie wzroku, znajdowała się wyłącznie dokumentacja oczekującego na badanie pacjenta,

- na tablicy ogłoszeń umieszczono klauzulę informacyjną ochrony danych osobowych, zawierającą m.in. nieprawidłowy adres e-mail IOD (o czym szerzej w sekcji „stwierdzone nieprawidłowości"),

- nie stwierdzono sytuacji pozostawienia bez nadzoru gabinetów poradni specjalistycznej oraz pomieszczenia rejestracji.

W SPZOZ wprowadzono system monitoringu wizyjnego, obejmujący kamery usytuowane na elewacjach zewnętrznych budynku oraz na korytarzach: Izby przyjęć, przychodni POZ[28] i oddziału dziecięcego. Nagrania przechowywane były na dysku rejestratora cyfrowego przez okres 30 dni. Dostęp do zapisanych danych posiadał wyłącznie administrator systemu informatycznego (dalej: ASI). Na drzwiach wejściowych Szpitala umieszczono tablicę informacyjną o monitoringu a dane ADO, kontakt IDO oraz podstawę prawną przetwarzania danych osobowych zamieszczono na tablicy ogłoszeń.

(akta kontroli str. 274-294, 453-454)

2.2. Zarządzanie siecią w Szpitalu odbywało się bez wykorzystania usługi katalogowej Active Directory[29] i pseudonimizacji danych osobowych.

[25] Ustalenia oparto na podstawie przeprowadzenia oględzin trzech oddziałów szpitalnych: dziecięcego, chirurgii oraz wewnętrznego I oraz okienka rejestracji do poradni specjalistycznych i oględzin trzech gabinetów specjalistycznych: poradni chirurgicznej, poradni ginekologicznej oraz poradni urologicznej.
[26] Lista z nazwiskami pacjentów i wskazaniem sali, na której przebywali.
[27] Ekrany komputerów były odwrócone o 180 stopni w stosunku do pola widzenia osoby postronnej.
[28] Podstawowej Opieki Zdrowotnej.
[29] Tj. bez zarządzania centralnego przez ASI.

SPZOZ korzystał ze zintegrowanego systemu informatycznego dedykowanego dla podmiotów leczniczych (dalej: zintegrowany system informatyczny) składającego się m.in. z modułów zapewniających wszystkie niezbędne funkcjonalności dla tworzenia, przechowywania i udostępniania dokumentacji pacjenta. Dostęp do tego systemu dla każdego pracownika posiadającego upoważnienie IOD, nadawany był w sposób indywidualny (z wykorzystaniem nazwiska pracownika). Hasła o odpowiedniej złożoności były generowane samodzielnie przez użytkownika. System wymagał odświeżania hasła co 30 dni i obowiązywał zakaz powtórzeń pięciu ostatnich kombinacji haseł. Do sieci Szpitala podłączonych było 101 komputerów[30]. Nie stwierdzono dostępu do zintegrowanego systemu informatycznego przez nieuprawniony personel administracyjny SPZOZ[31]. Z administracji Szpitala dostęp do systemu posiadali wyłącznie pracownicy Działu Świadczeń Medycznych[32]. Jak wyjaśnili Dyrektor oraz ASI, Szpital był na etapie pozyskiwania z Urzędu Marszałkowskiego Województwa Wielkopolskiego nowych serwerów, po których instalacji[33] zaplanowano wdrożenie zhierarchizowanej usługi katalogowej.

(akta kontroli str. 257-263, 293-294, 343-344, 359-360)

2.3. Pielęgniarski personel medyczny posiadał dostęp do zintegrowanego systemu informatycznego, nadany przez ASI na podstawie decyzji ADO. Dostępu tego nie posiadali natomiast sanitariusze i opiekunowie medyczni. W przypadku wszystkich 30 analizowanych osób jego zakres był adekwatny do stanowiska i wykonywanych zadań. W 29 przypadkach rzeczywisty zakres dostępu do zbioru danych odpowiadał zakresowi wynikającemu z upoważnienia, natomiast w jednym przypadku był szerszy niż określony w upoważnieniu (o czym szerzej w sekcji „stwierdzone nieprawidłowości").

(akta kontroli str. 230-256)

2.4. W okresie od 25 maja 2018 r. do 23 stycznia 2019 r. w związku z wygaśnięciem stosunku pracy 14 pracowników Szpitala, z tego 10, którym założono konta w zintegrowanym systemie informatycznym, dwóm z nich niezwłocznie odebrano dostęp do zintegrowanego systemu informatycznego. Kolejne trzy osoby dalej świadczyły swoje usługi na podstawie umowy zlecenia wykonywania zadań pielęgniarki odcinkowej. Natomiast pięć pozostałych osób posiadało nadal aktywne konta w zintegrowanym systemie informatycznym (co szerzej opisano w sekcji „stwierdzone nieprawidłowości).

(akta kontroli str. 257-263)

2.5. Szpital korzystał z mechanizmu zdalnego zgłaszania usterek dostawcy oprogramowania zintegrowanego systemu informatycznego, określonego w umowie. Rejestr za okres od 25 maja 2018 r. do 25 stycznia 2019 r. obejmował 32 zgłoszenia. Zgłoszenia były kierowane wyłącznie za pośrednictwem platformy wsparcia technicznego HELP DESK przygotowanej przez dostawcę i nie zawierały załączonych plików z danymi osobowymi pacjentów. Łącznie 22 z nich dotyczyły problemów, których rozwiązanie wymagało dostępu dostawcy do bazy danych osobowych gromadzonych przez SPZOZ. Zgłaszającym usterki był wyłącznie ABI. Dostęp do plików Szpitala dostawca otrzymywał po zgłoszeniu takiej konieczności i uzyskaniu autoryzacji użytkownika za pomocą loginu i hasła nadanego przez ABI. O fakcie usunięcia przyczyn zgłoszenia dostawca informował ABI, który dokonywał weryfikacji usługi i potwierdzał usunięcie problemu.

[30] 65 nowych komputerów z systemem Windows 10 Professional, 18 starych komputerów (17 z systemem Windows XP i jeden z systemem Windows 7 Home Premium) oraz 16 terminali i dwa laptopy.
[31] Badanie przeprowadzono na próbie 30 pracowników.
[32] Sześć osób.
[33] Dostawa przewidziana w III kwartale 2019 r.

(akta kontroli str. 268-273)

2.6. W okresie objętym kontrolą obowiązywały cztery umowy, w których Szpital był podmiotem przetwarzającym dane osobowe oraz 87, w których występował jako podmiot powierzający przetwarzanie danych. Wszystkie pięć losowo wybranych, szczegółowo badanych umów powierzenia przetwarzania danych osobowych zawierało elementy określone w art. 28 ust. 3 RODO tj. przedmiot i czas trwania przetwarzania, charakter i cel przetwarzania, rodzaj danych osobowych oraz kategorie osób, których dane dotyczą, a także prawa administratora.

Począwszy od września 2018 r. Szpital nie zawierał nowych umów powierzenia danych, w związku z przedłużeniem okresu obowiązywania 80 umów na świadczenie usług medycznych przez personel biały (lekarze, pielęgniarki).

(akta kontroli str. 228-256, 373-377)

2.7. W Dzienniku uchybień i zagrożeń[34] nie odnotowano w okresie od 25 maja 2018 r. do 21 lutego 2019 r. żadnych zdarzeń, na których okoliczność należałoby sporządzić protokół uchybień lub protokół zagrożenia.

W lipcu 2017 r. Generalny Inspektor Ochrony Danych Osobowych przeprowadził w Szpitalu kontrolę na okoliczność udostępnienia w czerwcu 2017 r. danych osobowych osobom nieuprawnionym. W wydanej decyzji GIODO nakazał usunięcie uchybień w procesie przetwarzania danych osobowych, poprzez uzupełnienie Polityki w zakresie sporządzenia wykazu budynków, pomieszczeń lub ich części tworzących obszar, w którym przetwarzane były dane osobowe, wykazu zbioru danych osobowych wraz ze wskazaniem programów zastosowanych do przetwarzania tych danych, opisu struktury zbiorów danych wskazującego zawartość poszczególnych pól informacyjnych i powiązania między nimi oraz sposobu przepływu danych pomiędzy poszczególnymi systemami. Ponadto nakazał uzupełnienie Instrukcji poprzez dodanie części opisowej w zakresie procedury tworzenia kopii zapasowych zbiorów danych oraz programów i narzędzi programowych służących do ich przetwarzania, sposobu, miejsca i okresu przechowywania elektronicznych nośników informacji zawierających dane osobowe oraz kopii zapasowych. Decyzja GIODO została wykonana przez Szpital. W sprawie udostępnienia danych osobowych osobom nieuprawnionym prowadzone było postępowanie karne w kierunku popełnienia przestępstwa z art. 51 ust. 2 ustawy o ochronie danych osobowych z 1997 r., zakończone wydaniem wyroku skazującego w marcu 2018 r.

(akta kontroli str. 148-149, 373-377, 379-442)

2.8. W okresie od 25 maja 2018 r. do 14 lutego 2019 r. Szpital 1 473 razy udostępnił dokumentację medyczną pacjentów, z czego w 23 przypadkach zakładom ubezpieczeń[35], w 224 uprawnionym organom lub podmiotom[36] oraz w 1.226 przypadkach przedstawicielowi ustawowemu albo osobie upoważnionej przez pacjenta. W przypadku zakładów ubezpieczeń Szpital udostępniał dokumentację medyczną zawsze za zgodą pacjentów. W 18 przypadkach dokumentacja została udostępniona na podstawie pisemnego wniosku upoważnionego przedstawiciela ubezpieczyciela oraz udzielonego pełnomocnictwa. W pięciu przypadkach dokumentację udostępniono na podstawie kopii upoważnienia dla przedstawiciela ubezpieczyciela bez jej uwierzytelnienia, co - jak wyjaśnili Dyrektor Szpitala oraz IOD - nastąpiło w związku z załączeniem odpowiednio potwierdzonych

[34] O którym mowa w rozdziale X Polityki, prowadzonym przez ABI/IOD, w którym należało dokumentować przypadki stwierdzenia naruszenia ochrony danych osobowych.
[35] W rozumieniu ustawy z dnia 11 września 2015 r. o działalności ubezpieczeniowej i reasekuracyjnej (Dz. U. z 2019 r. poz. 381).
[36] W tym Zakładowi Ubezpieczeń Społecznych, o którym mowa w ustawie z dnia 13 października 1998 r. o systemie ubezpieczeń społecznych (Dz. U. z 2019 r. poz. 300, ze zm.).

pełnomocnictw przy innych wnioskach. Składający wyjaśnienia zapowiedzieli niezwłoczne wystąpienie do zakładów ubezpieczeń o dostarczenie odpowiednich dokumentów.

Analiza 30 wniosków o wydanie dokumentacji medycznej osobie upoważnionej przez pacjenta wykazała, że we wszystkich przypadkach osoba odbierająca dokumentację posiadała pisemne upoważnienie pacjenta do jej odbioru.

Szpital w sześciu przypadkach odmówił udostępnienia dokumentacji, z czego w trzech z uwagi na brak pacjenta w bazie danych, a w innych z uwagi na upłynięcie 20-letniego okresu składowania dokumentacji oraz w związku z tym, że wnioskujący nie był osobą upoważnioną przez pacjenta.

(akta kontroli str. 202-226, 373-377)

2.9. W celu ochrony danych osobowych przed ich utratą w wyniku awarii, błędów lub nieuprawnionej modyfikacji wprowadzono:

- system zabezpieczeń serwerowni przeznaczonej do przetwarzania danych medycznych, archiwizacji oraz do zapewnienia połączenia z internetem, w której usytuowano w specjalnych szafach serwery, w tym serwer dedykowany do zintegrowanego systemu informatycznego. Dostęp do pomieszczenia serwerowni był zabezpieczony przed dostępem osób nieuprawnionych. Pomieszczenie to wyposażono w systemy m.in. kontroli dostępu oraz wykrywania pożaru, włamania lub zalania. Ponadto, serwerownię wyposażono m.in. w urządzenia podtrzymywania napięcia, gaśnice przeciwpożarowe, urządzenia i systemy regulacji temperatury.

- konieczność tworzenia kopii zapasowej baz danych (serwer kopii zapasowych). Kopię przechowywano w pomieszczeniu serwerowni na serwerze innym niż bazy danych. Tworzenie kopii bezpieczeństwa odbywało się w sposób automatyczny, częstotliwość tworzenia kopii (pełen backup – całość) - trzy razy dziennie, ponadto raz w miesiącu dokonywano sprawdzenia poprawności wykonywania tych kopii. ASI utworzył dwie odrębne procedury dla kopii bezpieczeństwa danych medycznych zintegrowanego systemu informatycznego oraz danych pracowników i kontrahentów. Jedynym nośnikiem przechowywania kopii zapasowych był serwer kopii zapasowych. Po otrzymaniu z Urzędu Marszałkowskiego Województwa Wielkopolskiego w III kwartale 2019 r. dodatkowego serwera będzie on pełnił funkcję serwera kopii zapasowej serwera kopii zapasowej tzw. back-up back-up'u. Procedury te zostały opracowane i wdrożone zgodnie z Decyzją GIODO z 19 października 2017 r.

Szpital posiadał dwa komputery przenośne niewyposażone w systemy ochrony kryptograficznej dysku twardego, jednakże na komputerach tych nie przechowywano danych osobowych.

W wyniku oględzin 30 komputerów, z czego 20 użytkowanych przez personel medyczny (po 10 przez lekarzy i personel pielęgniarski) stwierdzono, że:

a) na 23 komputerach zainstalowano system Windows 10 Professional, a na pozostałych Windows XP Home Edition lub Windows 7 Home Premium.

Jak wyjaśnił Dyrektor Szpitala oraz ASI, SPZOZ był na etapie wymiany komputerów na nowe, posiadające m.in. nadal wspierane przez producenta systemy operacyjne.

NIK wskazuje, że użytkowanie systemów operacyjnych nieposiadających już aktualnego wsparcia producenta oprogramowania może zwiększać ryzyko utraty danych oraz obniżać skuteczność ochrony antywirusowej.

b) wszystkie komputery posiadały dostęp do sieci Szpitala poprzez konto lokalne na podstawie hasła o odpowiedniej złożoności, nadanego indywidualnie dla każdego komputera. Login komputerów użytkowanych przez personel medyczny był identyczny dla wszystkich urządzeń, a znajomość haseł dostępu do poszczególnych

komputerów pracownicy[37] przekazywali sobie drogą ustną (co szerzej opisano w sekcji „stwierdzone nieprawidłowości"). Natomiast login komputerów użytkowanych przez personel administracyjny był indywidualny dla każdego komputera. Poza ujawnionymi przypadkami, opisanymi w dalszej części wystąpienia w sekcji *„stwierdzone nieprawidłowości"*, na komputerach nie stwierdzono przechowywania danych osobowych pacjentów w formie plików oraz dostępu do dysków lub udostępnionych folderów sieciowych zawierających takie dane. Dla uzyskania dostępu do danych osobowych pacjentów, które co do zasady powinny znajdować się wyłącznie w zintegrowanym systemie informatycznym, należało wprowadzić loginy oraz hasła, przypisane indywidualnie dla każdego pracownika i spersonalizowane. Sam dostęp do komputerów SPZOZ generalnie nie dawał zatem możliwości zapoznawania się z danymi osobowymi pacjentów.

c) na komputerach zainstalowano program antywirusowy z aktualną bazą danych wirusów.

d) komputery były zabezpieczone przed próbą instalacji dowolnego oprogramowania przez użytkownika.

e) na dyskach twardych czterech komputerów użytkowanych przez lekarzy oraz czterech użytkowanych przez personel pielęgniarski znajdowała się dokumentacja medyczna pacjentów. Jak wyjaśnił Dyrektor oraz IOD, na jednym z komputerów na oddziale ginekologiczno-położniczym[38] znajdowały się wyłącznie wypisy pacjentów przygotowane do wydruku a na drugim w rejestracji poradni POZ[39] znajdował się rejestr chorób zakaźnych wprowadzony na polecenie Państwowej Inspekcji Sanitarnej (kwestię pozostałych sześciu komputerów szerzej opisano w sekcji „stwierdzone nieprawidłowości").

f) porty USB nie były zabezpieczone przed możliwością podłączenia do nich nośników pamięci.

Z wyjaśnień Dyrektora oraz ASI wynikało, że SPZOZ posiadał 65 komputerów nowego typu, na których została wprowadzona ochrona zapisu na nośnikach USB/CD/DVD, natomiast na pozostałych nie było takiej możliwości technicznej. Szpital był w trakcie wymiany wszystkich komputerów, której ukończenie zaplanowano na koniec marca 2019 r.

(akta kontroli str. 78-81, 264-267, 293-338, 369-372, 443-448)

Stwierdzone nieprawidłowości

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

1. Tablice z ruchem chorych umieszczone na ścianach pomieszczeń w dyżurkach pielęgniarskich oddziałów dziecięcego, chirurgicznego oraz wewnętrznego I zawierały dane osobowe, w tym nazwiska pacjentów. Stwarzało to ryzyko ujawnienia tych danych osobom nieuprawnionym. W myśl motywu 39 preambuły oraz art. 5 ust. 1 lit. f. RODO, dane osobowe powinny być przetwarzane w sposób zapewniający im odpowiednie bezpieczeństwo i odpowiednią poufność, w tym ochronę przed nieuprawnionym dostępem do nich, niedozwolonym lub niezgodnym z prawem przetwarzaniem.

Dyrektor oraz IOD wyjaśnili ww. stan m.in. przyjętą w Szpitalu praktyką, ułatwiającą prawidłową lokalizację pacjentów, dodając jednocześnie, że tablice były zawieszone poza zasięgiem wzroku osób trzecich.

NIK wskazuje, że jakkolwiek danych ujętych na tych tablicach nie można było odczytać ze strefy wejściowej do trzech dyżurek albo z miejsca przy ladzie czwartej

[37] Do 28 osób.
[38] PG-LEKARZE
[39] POZ-REJESTRACJA

z nich, to jednak istniało ryzyko ich ujawnienia osobom nieuprawnionym, m.in. w przypadku wejścia w głąb tych pomieszczeń.

Dyrektor oraz IOD zadeklarowali zmianę sposobu postępowania w tym zakresie, poprzez ujmowanie na tablicach wyłącznie imion pacjentów, a przypadku ich zbieżności – dodawanie pierwszej lub kolejnej litery nazwiska.

(akta kontroli str. 274-294, 443-447)

2. Jeden pracownik Szpitala oraz pięciu byłych pracowników posiadało nieuprawniony dostęp do części zbiorów danych osobowych pacjentów.

2.1. Jedna z pielęgniarek Oddziału Chirurgii oprócz dostępu do zbioru danych tego oddziału wynikającego z udzielonego jej pisemnego upoważnienia do przetwarzania danych osobowych, miała również dostęp do zbioru danych „Gabinetu Pielęgniarki POZ" oraz „Gabinetu Lekarza POZ1 nocna i świąteczna", niewynikający z ww. ani też jakiegokolwiek innego upoważnienia.

Dyrektor oraz IOD wyjaśnili m.in., że wynikało to z bieżącej potrzeby wykonywania obowiązków służbowych (przesunięcia pomiędzy oddziałami szpitalnymi a poradnią lekarza POZ).

(akta kontroli str. 230-256, 361-365)

2.2. Pięciu byłych pracowników Szpitala, według stanu na 23 stycznia 2019 r., posiadało aktywne konto w zintegrowanym systemie informatycznym, pomimo wygaśnięcia ich stosunków pracy w okresie od 26 lipca do 31 grudnia 2018 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[40], 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.

NIK dostrzega jednocześnie, że dostęp do tego systemu był możliwy wyłącznie za pośrednictwem sieci lokalnej Szpitala, tj. nie był możliwy bez fizycznego dostępu do stanowisk komputerowych zlokalizowanych na jego terenie, a po rozwiązaniu ww. umów o pracę nie stwierdzono prób logowania przez byłych pracowników.

Z wyjaśnień Dyrektora i IOD wynikało, że obowiązująca Polityka nie zakładała formy cofania uprawnień dostępu i z tego powodu prawdopodobnie ASI nie został powiadomiony i nie cofnął uprawnień w systemie. Jednocześnie zapowiedzieli przeprowadzenie audytu osób upoważnionych do przetwarzania danych w systemach informacyjnych.

(akta kontroli str. 257-263, 293-294, 361-367)

3. W SPZOZ nie wdrożono zindywidualizowanej usługi logowania się personelu medycznego do systemów operacyjnych komputerów Szpitala. Login komputerów był identyczny dla wszystkich urządzeń, a znajomość haseł dostępu do poszczególnych komputerów pracownicy przekazywali sobie drogą ustną[41]. Praktyka taka była niezgodna z treścią rozdziału II (Definicje), III (Zabezpieczenia infrastruktury informatycznej i telekomunikacyjnej) i VIII (Metody i środki

[40] Dz.U. z 2017 r. poz. 2247, dalej: rozporządzenie KRI.

[41] Szczegółowym badaniem objęto 20 komputerów wykorzystywanych przez biały personel. Do jednego komputera hasło znało nawet do 28 osób.

uwierzytelnienia) Instrukcji, w myśl której dostęp do systemu operacyjnego komputera, w którym przetwarzane były dane osobowe dopuszczony był wyłącznie za pomocą procesu uwierzytelniania z wykorzystaniem identyfikatora użytkownika oraz hasła. Zgodnie z Instrukcją identyfikator użytkownika był to ciąg znaków literowych, cyfrowych lub innych jednoznacznie identyfikujący osobę upoważnioną do przetwarzania danych w systemie informatycznym, natomiast hasło należało zachować w poufności, a jego przekazywanie innym osobom było zabronione. Wreszcie, zabezpieczenia infrastruktury informatycznej odnosiły się m.in. do sprzętowych i programowych środków ochrony przed nieuprawnionym dostępem do danych osobowych, w tym środków zapewniających rozliczalność wykonywanych operacji, tj. pozwalających jednoznacznie przypisać określone działanie w systemie konkretnemu podmiotowi oraz umiejscowić je w czasie.

Jak wyjaśnił Dyrektor oraz ASI dostęp do danych medycznych pacjentów umożliwiał wyłącznie zintegrowany system informatyczny. Jednocześnie zadeklarował wdrożenie usługi Active-Directory po otrzymaniu dodatkowych serwerów w III kwartale 2019 r., która umożliwi pełne katalogowanie użytkowników komputerów.

(akta kontroli str. 293-338, 359-360, 372)

NIK wskazuje, że w świetle ww. regulacji niezbędne było wprowadzenie usługi umożliwiającej pełne monitorowanie wszystkich zdarzeń logowania, szczególnie w sytuacji, w której Instrukcja dopuszczała przechowywanie na twardych dyskach komputerów danych chronionych w trakcie uzasadnionej konieczności ich przetwarzania - co miało miejsce. Ponadto, także zgodnie z § 21 ust. 2 pkt 3 w zw. z § 20 ust. 1 rozporządzenia KRI, Szpital był zobowiązany do monitorowania dostępu użytkowników do systemu, w którym przetwarzano dane wrażliwe pacjentów w sposób zapewniający m.in. jego rozliczalność.

4. Serwer kopii zapasowych znajdował się w tym samym pomieszczeniu co serwer podstawowy, co w przypadku ewentualnego pożaru w tym pomieszczeniu albo jego zalania stwarzało ryzyko jednoczesnego uszkodzenia obu serwerów i w konsekwencji utraty znajdujących się na nich danych. Zgodnie z art. 5 ust. 1 lit. f RODO dane osobowe muszą być przetwarzane w sposób zapewniający odpowiednie ich bezpieczeństwo, w tym ochronę przed przypadkową utratą, zniszczeniem lub uszkodzeniem. Ponadto Szpital, w myśl § 20 ust. 2 pkt 12 lit. b rozporządzenia KRI, był zobowiązany do zapewnienia odpowiedniego poziomu bezpieczeństwa w systemach teleinformatycznych, polegającego w szczególności na minimalizowaniu ryzyka utraty informacji w wyniku awarii.

Z wyjaśnień Dyrektora oraz ASI wynikało, że nie było możliwości wydzielenia odrębnego drugiego pomieszczenia, odpowiednio zabezpieczonego i spełniającego wymogi dla serwerowni. Zadeklarowali, że po ukończeniu prowadzonej rozbudowy Szpitala serwer kopii serwera kopii zapasowej zostanie przeniesiony do zmodernizowanego skrzydła.

(akta kontroli str. 264-267, 293-294, 443-448)

4. Na dyskach twardych trzech komputerów użytkowanych przez lekarzy oraz trzech użytkowanych przez personel pielęgniarski, według stanu na dzień 4 lutego 2019 r., ujawniono dokumentację medyczną pacjentów. Zgodnie z art. 5 ust. 1 lit. e RODO dane osobowe co do zasady mogą być przechowywane w formie umożliwiającej identyfikację osoby, której dane dotyczą, przez okres nie dłuższy niż jest to niezbędne do celów, w których dane te są przetwarzane. Ponadto, w myśl punktu 4 rozdziału XI Instrukcji użytkownicy byli zobowiązani do niezwłocznego i trwałego usuwania/kasowania danych osobowych z nośników informacji (w tym dysków

twardych), po ustaniu powodu ich przechowywania chyba, że z powodu odrębnych przepisów należy je zachować na dłużej.

W złożonych wyjaśnieniach Dyrektor Szpitala oraz IOD nie wskazali powodów uzasadniających przechowywanie danych osobowych pacjentów na tych sześciu komputerach. Podali jednocześnie, że personel został pouczony o obowiązujących zasadach wynikających z Instrukcji (Polityki), zgodnie, z którymi dane medyczne pacjentów powinny być przechowywane w prowadzonych systemach zamkniętych. Sprawdzenie komputerów przeprowadzone przez IOD 13 lutego 2019 r. potwierdziło usunięcie z ich twardych dysków ww. danych.

(akta kontroli str. 293-307, 369-372)

5. Klauzula informacyjna w sprawie przetwarzania danych osobowych znajdująca się na tablicy ogłoszeń poradni specjalistycznych Szpitala zawierała nieprawidłowy adres e-mail IOD[42], o którym mowa w art. 13 ust. 1 lit. b RODO, co mogło utrudniać m.in. pacjentom nawiązanie z nim kontaktu.

Dyrektor Szpitala i IOS wyjaśnili, że ww. klauzula nie została zmieniona z uwagi na przeoczenie.

(akta kontroli str. 287-289, 361-366)

W toku prowadzonej przez NIK kontroli, klauzula ta została zaktualizowana.

(akta kontroli str. 368)

OCENA CZĄSTKOWA

Obowiązujące w Szpitalu rozwiązania techniczne i organizacyjne co do zasady zapewniały prawidłowe przetwarzanie i ochronę danych osobowych. Personel SPZOZ posiadał adekwatne do wykonywanych obowiązków prawo dostępu do zbioru danych osobowych w zintegrowanym systemie informatycznym. Szpital nie zaktualizował natomiast zakresu pisemnego upoważnienia do przetwarzania danych osobowych jednego pracownika i nie usunął z tego systemu pięciu kont byłych pracowników. Właściwie udostępniano dokumentację medyczną pacjentów i zawierano wymagane umowy powierzenia przetwarzania danych osobowych. Podejmowano też odpowiednie działania w celu minimalizacji ryzyka utraty tych danych, jednak nie zapewniono odrębnego pomieszczenia dla serwera kopii zapasowej. Stwierdzono też przypadki przechowywania na komputerach służbowych dokumentacji medycznej pacjentów bez uzasadnionego powodu. Nie wdrożono również środowiska logowania do systemu operacyjnego komputerów Szpitala w sposób zapewniający jego rozliczalność i nie wyeliminowano ryzyka dostępu osób nieuprawnionych do danych pacjentów zamieszczonych na tablicach z ruchem chorych.

IV. Wnioski

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

1) dokonanie przeglądu i aktualizacji Polityki Bezpieczeństwa Informacji oraz regulaminu organizacyjnego SPZOZ,
2) opracowywanie planów sprawdzeń oraz sprawozdań rocznych stanu funkcjonowania systemu ochrony danych osobowych Szpitala,
3) prowadzenie tablic ruchu chorych w sposób zapewniający odpowiednią ochronę danych osobowych pacjentów,
4) wdrożenie środowiska logowania do systemu operacyjnego komputerów Szpitala w sposób zapewniający jego rozliczalność,

[42] iod@comp-net.pl zamiast iod@spzozkolo.pl

5) skorelowanie poziomu dostępu pracowników do zintegrowanego systemu informatycznego z zakresem udzielonych im pisemnych upoważnień oraz niezwłoczne odbieranie takiego dostępu byłym pracownikom SPZOZ,
6) zorganizowanie, w miarę posiadanych możliwości, odrębnych pomieszczeń dla serwerów z danymi oraz serwerów z kopiami tych danych.

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

Poznań, 22 marca 2019 r.

Najwyższa Izba Kontroli
Delegatura w Poznaniu

Kontroler	Dyrektor
Tomasz Otworowski	z up. Tomasz Nowiński
specjalista kontroli państwowej	p.o. Wicedyrektor
.....	.....
podpis	*podpis*