NAJWYŻSZA IZBA KONTROLI

Delegatura w Poznaniu

LPO. 410.002.02.2019

Pan Marek Czaplicki
Dyrektor Wojewódzkiego Szpitala dla Nerwowo
i Psychicznie Chorych „Dziekanka” im. Aleksandra
Piotrowskiego w Gnieźnie
ul. Poznańska 15
62-200 Gniezno

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	Wojewódzki Szpital dla Nerwowo i Psychicznie Chorych „Dziekanka" im. Aleksandra Piotrowskiego w Gnieźnie, ul. Poznańska 15, 62-200 Gniezno (dalej: Szpital albo Dziekanka)
Kierownik jednostki kontrolowanej	Marek Czaplicki, Dyrektor Wojewódzkiego Szpitala dla Nerwowo i Psychicznie Chorych „Dziekanka" im. Aleksandra Piotrowskiego w Gnieźnie, od 30 czerwca 2017 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 8 marca 2019 r.[1]
Podstawa prawna podjęcia kontroli	Art. 2 ust. 2 ustawy z dnia 23 grudnia 1994 r. o Najwyższej Izbie Kontroli[2]
Jednostka przeprowadzająca kontrolę	Najwyższa Izba Kontroli Delegatura w Poznaniu
Kontroler	Mirosław Babkiewicz, specjalista kontroli państwowej, upoważnienie do kontroli nr LPO/6/2019 z 10 stycznia 2019 r. (akta kontroli str. 1-3)

[1] Badania kontrolne objęły także działania sprzed tego okresu, które miały związek z zagadnieniami będącymi przedmiotem kontroli.
[2] Dz. U. z 2019 r. poz. 489, dalej: ustawa o NIK.

II. Ocena ogólna[3] kontrolowanej działalności

OCENA OGÓLNA

Szpital terminowo opracował wymaganą dokumentację oraz procedury związane z ochroną przetwarzanych danych osobowych, jednak dane osobowe nie były w pełni prawidłowo chronione i przetwarzane.

W związku z rozpoczęciem stosowania przepisów rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r.[4] (dalej: RODO), w Szpitalu opracowano dokumentację tworzącą Politykę Bezpieczeństwa Ochrony Danych Osobowych (dalej: Polityka) i wdrożono procedury dotyczące ochrony danych osobowych, tworząc kompleksowy system zarządzania bezpieczeństwem informacji, zgodnie z wymogiem określonym w § 20 ust. 1 rozporządzenia Rady Ministrów z dnia 12 kwietnia 2012 r.[5] (dalej: rozporządzenie KRI). Realizowano obowiązki związane z analizą procesów przetwarzania danych, a wprowadzone rozwiązania zmierzające do zapewnienia ochrony danych osobowych pacjentów gwarantowały poszanowanie ich prywatności. Personelowi Dziekanki zapewniono dostęp do danych osobowych w zakresie adekwatnym do potrzeb oraz niezwłocznie odbierano go pracownikom, którzy przestali być zatrudniani. Szpitalne komputery były wykorzystywane zgodnie z przeznaczeniem wynikającym z zakresu dostępu personelu do systemów i były odpowiednio zabezpieczone. Prawidłowo udostępniano dokumentację medyczną pacjentów, a w umowach powierzenia przetwarzania danych osobowych zawierano wymagane przez RODO warunki. Pomieszczenie serwerowni było prawidłowo użytkowane, monitorowane i zabezpieczone.

Stwierdzono przypadki wskazujące na możliwość nieuprawnionego ujawnienia danych osobowych pacjentów przy ich rejestrowaniu, prowadzeniu ruchu chorych i przechowywaniu dokumentacji medycznej. Przeszkolenie jedynie niewielkiej części pracowników Dziekanki z zakresu przepisów RODO oraz brak przy jednym ze stanowisk rejestracyjnych klauzuli informacyjnej, o której mowa w art. 13 ust. 1-2 tego rozporządzenia, nie sprzyjały zapewnieniu optymalnego poziomu ochrony danych osobowych w Szpitalu. Ponadto stwierdzono nieprawidłowości dotyczące aktualizowania regulaminu organizacyjnego Dziekanki, zamieszczania na jej stronie internetowej niepełnej informacji o powołaniu IOD oraz nieprowadzenia rejestru podmiotów, którym w drodze umowy powierzono przetwarzanie danych osobowych. Nieprawidłowości te miały jednak charakter formalny i nie stwierdzono aby miały negatywny wpływ na bezpieczeństwo przetwarzania i ochronę danych osobowych w Szpitalu.

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

[4] 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 2016 r., str. 1, ze zm. Wejście w życie 24 maja 2016 r., rozpoczęcie stosowania 25 maja 2018 r., dalej: RODO.

[5] W sprawie Krajowych Ram Interoperacyjności minimalnych wymagań dla rejestrów publicznych i wymiany informacji w postaci elektronicznej oraz minimalnych wymagań dla systemów teleinformatycznych (Dz. U. z 2017 r. poz. 2247., dalej: rozporządzenie KRI).

III. Opis ustalonego stanu faktycznego oraz oceny cząstkowe[6] kontrolowanej działalności

OBSZAR

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

Opis stanu faktycznego

1.1. W Szpitalu od 1 maja 2018 r.[7] funkcjonował Inspektor Ochrony Danych (dalej: IOD), wyznaczony przez Dyrektora będącego Administratorem Danych Osobowych (dalej: ADO). Dyrektor w regulaminie organizacyjnym Dziekanki[8] nie określił stanowiska IOD ani jego zadań, w regulaminie tym nadal natomiast widniało samodzielne stanowisko Administratora Bezpieczeństwa Informacji (dalej: ABI), któremu nie wyznaczono żadnych zadań[9].

IOD nie był pracownikiem Szpitala i realizował usługi na jego rzecz[10] w ramach prowadzonej przez siebie działalności gospodarczej z zakresu ochrony danych osobowych. Posiadał on odpowiednie kwalifikacje zawodowe do pełnienia tej funkcji i kompetencje do świadczenia usług związanych z ochroną danych osobowych w systemach informatycznych[11]. W Dziekance umożliwiono IOD wykonywanie obowiązków w sposób niezależny, nieograniczający zakresu jego działań[12].

Zawiadomienie o wyznaczeniu IOD zostało przesłane przez ADO do Prezesa Urzędu Ochrony Danych Osobowych (dalej: Prezes UODO) 1 sierpnia 2018 r., tzn. jeden dzień po terminie określonym w art. 158 ust. 5 ustawy o ochronie danych osobowych. Szpital podejmował próby przesłania tego zawiadomienia w terminie, jednakże z uwagi na zakłócenia w funkcjonowaniu witryny okazały się one nieskuteczne[13].

Zawiadomienie zawierało dane określone w art. 10 ust. 1 i 3 ww. ustawy. Informacja o powołaniu IOD, wraz z jego adresem kontaktowym (e-mailowym) widniała na stronie internetowej Szpitala[14]. Nie zawierała ona imienia i nazwiska IOD[15].

Dziekanka nie była operatorem usługi kluczowej, o którym mowa w art. 5 ust. 1 w zw. z art. 2 pkt 16 ustawy z dnia 5 lipca 2018 r. o krajowym systemie

---

[6] 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.

[7] Data określona w umowie z dnia 30 marca na świadczenie usług IOD (pełnienie obowiązków IOD).

[8] Wprowadzony zarządzeniem Dyrektora nr 17/2018 z 11 maja 2018 r. w sprawie wprowadzenia Regulaminu Organizacyjnego, dalej: Regulamin Organizacyjny.

[9] O czym szerzej w sekcji „Stwierdzone nieprawidłowości".

[10] Przed wejściem w życie RODO IOD nie był zatrudniony w Szpitalu i nie wykonywał na jego rzecz takich usług.

[11] IOD m.in. miał ukończone studia podyplomowe w kierunkach: ochrona danych osobowych, zarządzanie projektami informatycznymi i zarządzanie w opiece zdrowotnej oraz ukończył szkolenia z zakresu: powołania IOD, opracowania Polityki Bezpieczeństwa Informacji, ochrony danych osobowych i dokumentacji medycznej w jednostce organizacyjnej i obowiązków pracodawcy w tym zakresie, a także z zakresu monitoringu w administracji zgodnego z RODO, administratora sieci informatycznej, ochrony informacji niejawnej. Był on także administratorem systemu akredytowanym przez Agencję Bezpieczeństwa Wewnętrznego.

[12] Według umowy z 30 marca 2018 r. na pełnienie obowiązków IOD, do zadań IOD należało: informowanie o stanie ochrony danych osobowych, monitorowanie przestrzegania RODO i innych przepisów o ochronie danych osobowych i polityki bezpieczeństwa danych osobowych, w tym podział obowiązków, działania zwiększające świadomość, szkolenia pracowników a także współpraca z Prezesem Urzędu Ochrony Danych Osobowych i pełnienie funkcji punktu kontaktowego dla organu nadzorczego w kwestiach związanych z przetwarzaniem danych osobowych, prowadzenie konsultacji w tym zakresie. Dodatkowo do zadań IOD należało przeprowadzanie audytów, wydawanie w imieniu ADO upoważnień do przetwarzania danych osobowych, kierowanie pracą administratora systemu informatycznego w zakresie zabezpieczenia stanowisk komputerowych z dostępem do danych osobowych, nadawanie uprawnień w systemie. IOD podlegał bezpośrednio Dyrektorowi.

[13] Komunikat: Nieudane nadanie na skrytkę. […] Kolejka skrytki jest przepełniona (1000/1000) (kod 0). Ponadto sygnalizowane prace serwisowe co najmniej od 18:30 do 24:00 dnia 31 lipca 2018 r.

[14] W zakładce: „Pacjent", pod adresem: https://dziekanka.net/ochrona-danych-osobowych/.

[15] O czym szerzej w sekcji „Stwierdzone nieprawidłowości".

cyberbezpieczeństwa[16], a IOD nie był członkiem wewnętrznych struktur odpowiedzialnych za cyberbezpieczeństwo, określonych w art. 14 tej ustawy.

(dowód: akta kontroli str. 4-52, 273-289, 355-362)

1.2. W Szpitalu w 2018 r., w związku z wejściem w życie i rozpoczęciem stosowania RODO, opracowano i wprowadzono do stosowania dokumentację z zakresu ochrony danych osobowych. Tworzyły ją dokumenty wchodzące w skład Polityki, zatwierdzonej przez Dyrektora w dniu 25 maja 2018 r.[17], w tym: [1] Raport Szacowania Ryzyka i Doboru Środków Bezpieczeństwa, [2] Zasady Ogólne, [3] Procedury Bezpieczeństwa. W Polityce, w ramach procedury kontroli dostępu do informacji, określono m.in. cel, zakres stosowania procedury, odpowiedzialność za jej przestrzeganie a także ustanowiono następujące elementy: [1] Instrukcja udzielania dostępu do zasobów informatycznych, w tym: utworzenie stanowiska, zmiany na koncie, [2] Instrukcja tworzenia haseł oraz postępowania z hasłami administratorów, [3] Stosowane metody i środki uwierzytelniania oraz procedury związane z ich zarządzaniem i użytkowaniem, [4] Zasady postępowania dotyczące dostępu pracowników Szpitala do systemów informatycznych udostępnianych do celów służbowych przez zewnętrzne instytucje, poprzez sieć Internet lub inną sieć rozległą, [5] Kontrola dostępu do sieci komputerowej, [6] Zasady postępowania dotyczące pracy na odległość oraz urządzeń przenośnych i nośników danych wynoszonych poza siedzibę Szpitala, [7] Kontrola dostępu do pomieszczeń serwerowni i pomieszczeń technicznych, [8] Procedura przeglądu uprawnień do systemów.

W ramach procedury profilaktyki antywirusowej zdefiniowano i określono: [1] Zasady ogólne ochrony przed szkodliwym oprogramowaniem, [2] Zalecenia dla użytkowników stacji roboczych, [3] Postępowanie w przypadku ujawnienia lub podejrzenia istnienia wirusa.

W ramach procedury tworzenia kopii zapasowych zdefiniowano i określono: [1] cel procedury, [2] zakres stosowania, [3] wykonywanie kopii systemów informatycznych, [4] testowanie kopii zapasowych, [5] odzyskiwanie danych i systemów informatycznych z kopii zapasowych.

W ramach Polityki funkcjonowały także: [1] Regulamin korzystania z komputerów przenośnych, na których są przetwarzane dane osobowe poza strefą przetwarzania danych osobowych, [2] Regulamin korzystania z komputerów służbowych, [3] Bezpieczeństwo nośników i sprzętu mobilnego poza siedzibą jednostki (telefony i tablety służbowe), [4] Procedura wykonywania przeglądów i konserwacji, [5] Procedura nadawania uprawnień do dostępu do danych osobowych [6] Procedura alarmowa, w tym: dziennik uchybień i zagrożeń – (załącznik nr 1), protokół zagrożenia/uchybienia (załącznik nr 2), procedura działań korygujących i zapobiegawczych, procedura bieżącego szacowania ryzyka i wdrażanie wypracowanych wniosków, [7] Charakterystyka możliwych „uchybień i zagrożeń", [8] Rejestr uchybień i zagrożeń oraz postępowanie osób funkcyjnych. Poza procedurami stanowiącymi załączniki do Polityki, nie przewidziano konieczności opracowania dodatkowych instrukcji uszczegóławiających zasady ochrony danych w Szpitalu.

Zasady zapoznania się Polityką zostały określone w jej treści[18], zgodnie z którą pracownicy Dziekanki przetwarzający dane osobowe zostali z nią zapoznani na

[16] Dz. U. poz. 1560

.

[17] Zarządzenie Dyrektora nr 18/2018 z 25 maja 2018 r. w sprawie organizacji systemu ochrony danych osobowych i powołania Inspektora Ochrony Danych Osobowych.

[18] Polityka Bezpieczeństwa Danych Osobowych, Część Ogólna, w rozdz. 1.3: „Sposób i zakres udostępniania dokumentu".

szkoleniu z zakresu przepisów RODO oraz pisemnie poinformowani o dostępności tego dokumentu w Sekretariacie Szpitala.

W okresie objętym kontrolą NIK nie dokonywano przeglądów ani aktualizacji dokumentacji dotyczącej regulacji wewnętrznych z zakresu ochrony danych osobowych, w tym zawartych w Polityce. Na dzień kontroli, tj. 20 lutego 2019 r. Polityka ta nie wymagała aktualizacji. Dyrektor wyjaśnił, że jej przegląd i aktualizacja zostały zaplanowane po upływie roku od jej wprowadzenia.

(dowód: akta kontroli str. 53-178, 355-362)

1.3. W Szpitalu był prowadzony w formie pisemnej i elektronicznej rejestr zawierający kompleksową ewidencję operacji realizowanych przez ADO na danych osobowych i zawierający wszystkie dane, o których mowa w art. 30 ust. 1 i 2 RODO. Według stanu na dzień 25 maja 2018 r. rejestr zawierał 19 pozycji, a na dzień 15 stycznia 2019 r. – 21 pozycji. Forma rejestru była zgodna ze wzorem określonym w Polityce.

(dowód: akta kontroli str. 53-178, 305-310)

1.4. W Szpitalu, w związku z rozpoczęciem stosowania RODO, dokonano analizy ryzyka, o której mowa w art. 32 RODO. Analiza ta stanowiła część Polityki[19] i obejmowała zasoby systemu teleinformatycznego i czynnik ludzki (łącznie: 14 rodzajów zasobów), a także zagrożenia ze strony sił natury oraz celowych i przypadkowych działań człowieka (łącznie 35 rodzajów zagrożeń), które mogłyby spowodować ujawnienie lub utratę danych osobowych z zasobu Szpitala.

W celu identyfikacji podatności na ryzyko opracowano listę potencjalnych słabych punktów systemu bezpieczeństwa informacji. Poziom podatności określono odrębnie dla ochrony: poufności, integralności i dostępności, w 5-stopniej skali z punktacją od 1 do 10[20]. Dla każdego z ryzyk określono prawdopodobieństwo zaistnienia i skutek, szacując ich wartość.

Z analizy wynikało, że najsłabszym ogniwem w systemie bezpieczeństwa przetwarzania danych osobowych był czynnik ludzki. Największą wartość ryzyka oszacowano dla ochrony dostępności, w tym kradzieży informacji zawierającej dane osobowe, kradzieży urządzeń i sprzętu mobilnego, nieuprawnionego kopiowania danych, użycia fałszywego oprogramowania, nielegalnego przetwarzanie danych, awarii, niewłaściwego działania urządzeń i utraty zasilania elektrycznego.

Ponadto IOD w obszarze danych osobowych przeprowadził audyt Szpitala[21] w zakresie stopnia zapewnienia bezpieczeństwa danych w stosunku do ryzyk zagrożenia dla bezpieczeństwa przetwarzania danych osobowych[22], według stanu na dzień 24 maja 2018 r. IOD stwierdził brak: klauzuli informacyjnej skierowanej do pracowników i pacjentów Dziekanki (została ona opracowana w trakcie audytu); analizy upoważnień ze względu na czynności realizowane przez osoby upoważnione do przetwarzania danych osobowych w celu uzyskania pełnej rozliczalności; rejestru czynności przetwarzania danych (został opracowany w trakcie audytu); rejestru umów na powierzenie przetwarzania danych osobowych przez inne podmioty; „zapisów" dotyczących nadzoru nad przestrzeganiem przepisów z zakresu ochrony danych osobowych; przejrzystej rozliczalności

[19] „Raport Szacowania Ryzyka i Doboru Środków Bezpieczeństwa".
[20] Brak (0), niski poziom (1-4), średni poziom (5-7), wysoki poziom (8-9), ekstremalny poziom (10).
[21] Data sporządzenia 29 czerwca 2018 r.
[22] Możliwość: zainstalowania złośliwego oprogramowania, wykorzystania luk w systemach urządzeń mobilnych, ataku zewnętrznego ograniczającego dostęp do danych, przejęcia informacji wysyłanych pocztą elektroniczną, ataku w celu przejęcia danych - phising, wystąpienia braku zasilania energetycznego, przekierowania - pharming, nieuprawnionego dostępu do nośników danych, braku zasilania energetycznego, zalania wodą lub innymi substancjami z instalacji wewnętrznych, pożaru, powodzi, przegrzania, a także awaria sprzętu i jego zły stan techniczny, niewydolność urządzeń, używanie niewydolnych urządzeń oprogramowania niemającego wsparcia producenta, kradzież sprzętu mobilnego.

przebywania osób w strefach przetwarzania danych (zarządzanie kluczami do pomieszczeń). W trakcie realizacji były działania z zakresu szyfrowania danych osobowych (w tym baz danych), komputerów stacjonarnych i mobilnych a także uzyskiwanie zdolności do ciągłego zapewnienia poufności, integralności i odporności systemów i usług przetwarzania bezpośredniego. IOD wskazał na konieczność podjęcia szeregu działań[23], zauważył ponadto prawidłowe działania w kierunku: uszczelnienia dostępu do Internetu i stosowania urządzeń brzegowych wysokiej jakości i ich aktualizacji oraz ograniczania dostępu osobom postronnym do systemu i jego ochrony przed podsłuchem pracowników Dziekanki. W części dotyczącej fizycznych środków zabezpieczających dane osobowe, IOD zauważył właściwe przygotowanie pomieszczenia serwerowni pod względem jej zabezpieczenia fizycznego jak i właściwej eksploatacji.

Analiza stopnia zaawansowania wykonania przez Szpital wskazań zawartych w ww. audycie wykazała ich zasadniczą realizację, za wyjątkiem m.in.: wdrożenia alarmowania w przypadku niepożądanych i potencjalnie niebezpiecznych działań użytkownika; monitorowania wszystkich operacji i zaimplementowania szyfrowania pamięci przenośnych. Brak było także dyspozytora kluczy, który mógłby wykazać pełną rozliczalność. W trakcie realizacji były zalecenia: przeszkolenia wszystkich osób z zakresu ochrony danych osobowych i organizacji ochrony danych osobowych w Szpitalu, zapewnienia poufności, integralności i dostępności danych oraz zalecenie wdrożenia kryptografii.

Dyrektor wyjaśnił m.in., że do dnia 5 marca 2019 r. zakończono wdrożenie alarmowania w przypadku niepożądanych i potencjalnie niebezpiecznych działań użytkownika, a w zakresie monitorowania wszystkich operacji zmodyfikowano jego zakres (zapisywanie są najważniejsze operacje). Dodał, że zalecenie zaimplementowania szyfrowania pamięci przenośnych jest nieaktualne (z uwagi na wyłączenie możliwości używania przenośnych nośników danych), podobnie jak kwestia dyspozytora kluczy, który mógłby wykazać pełną rozliczalność (z uwagi na to, że dostęp do serwera mają pracownicy Działu Informatyki i Dyrektor oraz prowadzony jest rejestr osób z zewnątrz, przebywających w serwerowni). Ponadto Dyrektor wyjaśnił, że Dziekanka jest w trakcie pozyskiwania środków na wdrożenie EDO[24], na zakup macierzy (w celu zwiększenia możliwości przechowywania danych) i na zakup UPS[25] o większej mocy.

(dowód: akta kontroli str. 192-203, 366-370, 422-426, 428-429)

1.5. W Szpitalu nie dokonywano oceny skutków dla ochrony danych osobowych, o której mowa w art. 35 RODO. Dyrektor wyjaśnił, że zgodnie z Komunikatem Prezesa UODO z dnia 17 sierpnia 2018 r.[26] Szpital nie był zobligowany do dokonywania ww. oceny[27].

(dowód: akta kontroli str. 355-362)

1.6. Na dzień 31 stycznia 2019 r. łączna liczba pracowników Dziekanki wynosiła 795 osób, w tym obowiązki 721 (90,7%) były związane z przetwarzaniem danych osobowych. W związku z rozpoczęciem stosowania RODO, 25 sierpnia 2018 r.

[23] Takich jak: instalowanie najnowszych aktualizacji oprogramowania, wdrożenie kryptografii, zastosowanie alarmowania w przypadku niepożądanych lub potencjalnie niebezpiecznych działań użytkownika, monitorowanie wszystkich operacji na plikach danych, audytowanie czynności tworzenia, usuwania i kopiowania plików.
[24] W zakresie elektronicznego uwierzytelniania dokumentacji.
[25] Ang. *uninterruptible power supply* (niezakłócone zasilanie energią) - urządzenie lub system, którego funkcją jest utrzymanie zasilania innych urządzeń elektrycznych lub elektronicznych w przypadku zaniku lub nieprawidłowych parametrów zasilania sieciowego.
[26] W sprawie wykazu rodzajów operacji przetwarzania danych osobowych wymagających oceny skutków przetwarzania dla ich ochrony (M.P. poz. 827).
[27] W ww. komunikacie Prezes UODO nie wskazał danych medycznych przetwarzanych w szpitalach, jako wymagających przeprowadzenia takiej oceny.

IOD przeprowadził szkolenie, którym objęto 65 pracowników związanych z przetwarzaniem ww. danych (9,0%), zatrudnionych w 36 komórkach organizacyjnych Szpitala (72,0% wszystkich komórek). Po tym dniu, co najmniej do 22 lutego 2019 r. nie przeprowadzano już szkoleń w tym zakresie[28]. Dyrektor umożliwił pracownikom dostęp do materiałów informacyjnych i szkoleniowych w tym przedmiocie, poprzez ich umieszczenie na pulpitach roboczych wszystkich stanowisk komputerowych Szpitala[29].

(dowód: akta kontroli str. 214-272, 355-362)

1.7. W Dziekance nie stosowano kodeksu dobrych praktyk ani medycznego kodeksu branżowego. Dyrektor wyjaśnił, że treść kodeksu branżowego będzie w Ministerstwie Zdrowia ujednolicana dla całej branży. Ponadto wskazał, że kodeks branżowy ochrony zdrowia został przekazany 13 listopada 2018 r. do zatwierdzenia przez Prezesa UODO, w związku z czym Szpital do dnia kontroli NIK[30] działał w tym zakresie na podstawie wytycznych przekazanych do publicznej wiadomości.

(dowód: akta kontroli str. 355-362)

Stwierdzone nieprawidłowości

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

1. Zamieszczona na stronie internetowej Szpitala[31] informacja o powołaniu IOD, wbrew wymogom określonym w art. 11 w zw. z art. 10 ust. 1 ustawy o ochronie danych osobowych, nie zawierała jego imienia i nazwiska.

Dyrektor wyjaśnił, że to niedopatrzenie zostało poprawione w trakcie kontroli NIK.

(dowód: akta kontroli str. 273-289, 355-362)

2. W strukturze organizacyjnej Szpitala określonej w Regulaminie Organizacyjnym nie wydzielono nowego samodzielnego stanowiska pracy dla funkcjonującego IOD, a pozostawiono nieaktualne stanowisko ABI (§ 9 ust. 6 pkt B lit. a). Zgodnie z art. 24 ust. 1 pkt 3 ustawy z dnia 15 kwietnia 2011 r. o działalności leczniczej[32], w regulaminie organizacyjnym powinna zostać w szczególności określona struktura organizacyjna zakładu leczniczego. Ponadto, w myśl art. 24 ust. 1 RODO oraz punktu II.A.3 załącznika do komunikatu Nr 23 Ministra Finansów z 16 grudnia 2009 r.[33], 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 wyjaśnił, że powyższa nieprawidłowość wynikała z nieskorygowania nieaktualnej regulacji, z uwagi na procedurę zatwierdzania treści ww. regulaminu przez Radę Społeczną Szpitala. Zapewnił, że stosowna korekta zostanie przeprowadzona na najbliższym posiedzeniu tego organu.

(dowód: akta kontroli str. 4-52, 273-289, 355-362)

3. Do dnia kontroli NIK (22 lutego 2019 r.) szkoleniem z zakresu przepisów RODO objęto tylko 9% pracowników Dziekanki, przy czym nie przeszedł go żaden z pracowników 14 z 50 komórek organizacyjnych Szpitala[34]. W myśl § 20 ust. 2

[28] O czym szerzej w sekcji „Stwierdzone nieprawidłowości".
[29] Były to pliki: „Podstawowe pojęcia RODO" i „Przewodnik po RODO w Służbie Zdrowia".
[30] Tj. 20 lutego 2019 r.
[31] W zakładce: „Pacjent", pod adresem: https://dziekanka.net/ochrona-danych-osobowych/.
[32] Dz.U. 2018 r. poz. 2190, dalej: ustawa o działalności leczniczej.
[33] W sprawie standardów kontroli zarządczej dla sektora finansów publicznych (Dz. Urz. MF nr 15 poz. 84).
[34] W tym: Dział Socjalny, Dział Techniczny, Pracownia EKG i EEG, Gabinet Stomatologiczny, Dział Żywienia, Laboratorium Diagnostyczne, Oddz. 15 Psychiatryczny Ogólny (męski), Oddz. 2 Psychogeriatryczny, Oddz. 25 Detoksykacyjny Dla Uzależnionych Od Alkoholu (żeński), Oddz. 4 Psychiatryczny Dla Przewlekle Chorych (męski), Oddz. 6 p. Psychiatryczny Dla Przewlekle Chorych, Oddz. 9 Psychiatryczny Ogólny (męski), Poradnia Zdrowia Psychicznego i Pracownia USG.

pkt 6 rozporządzenia KRI, zarządzanie bezpieczeństwem informacji realizowane jest w szczególności poprzez zapewnienie przez kierownictwo podmiotu publicznego szkolenia osób zaangażowanych w proces przetwarzania informacji.

Dyrektor wyjaśnił, że plan szkoleń na 2018 r. obejmował 41 innych szkoleń specjalistycznych związanych z informatyzacją dla wszystkich grup zawodowych, nie było więc możliwości przeszkolenia większej liczby pracowników Szpitala z zakresu przepisów RODO, bez zaburzenia normalnego toku funkcjonowania Szpitala.

NIK wskazuje, że nieobjęcie ww. szkoleniem pozostałych 91% pracowników Szpitala, pomimo upływu ponad 10 miesięcy od rozpoczęcia stosowania RODO, mogło mieć negatywny wpływ na stan ich wiedzy oraz na skuteczność ochrony danych osobowych w Dziekance. Przemawia za tym m.in. incydent związany z opuszczeniem niezabezpieczonego stanowiska komputerowego przez pracownika, opisany w sekcji „stwierdzone nieprawidłowości" w obszarze drugim niniejszego wystąpienia pokontrolnego.

(dowód: akta kontroli str. 214-272, 355-362)

OCENA CZĄSTKOWA

W Szpitalu wyznaczono IOD oraz prawidłowo opracowano dokumentację i procedury związane z ochroną przetwarzanych danych osobowych, które zostały zatwierdzone przez Dyrektora. Jednakże tylko niewielka część pracowników Dziekanki została przeszkolona z zakresu przepisów RODO, co nie sprzyjało zapewnieniu optymalnego poziomu ochrony danych osobowych w Szpitalu. Ponadto w niezaktualizowanym Regulaminie Organizacyjnym Szpitala brakowało stanowiska IOD, a na stronie internetowej Dziekanki nie podano jego imienia i nazwiska. Nieprawidłowości te miały jednak charakter głównie formalny - nie stwierdzono aby wpłynęły one negatywnie na skontrolowaną działalność.

OBSZAR

2. Zapewnienie prawidłowego przetwarzania i ochrony danych osobowych

Opis stanu faktycznego

2.1. Oględziny losowo wybranych oddziałów szpitalnych, w tym: nr 1: Detoksykacyjnego dla Uzależnionych od Alkoholu – Męskiego (dalej: Oddział nr 1), nr 6 Psychiatrycznego dla Przewlekle Chorych: I piętro - męski i II piętro – koedukacyjny (dalej: Oddział nr 6) i nr 13 Psychiatrii Sądowej (dalej: Oddział nr 13) wykazały, że wejście na teren zbadanych oddziałów było możliwe tylko za wiedzą i zgodą personelu (drzwi wejściowe były otwierane przez personel oddziału) a dla osób upoważnionych – tylko za pomocą karty kodów. Na łóżkach szpitalnych pacjentów nie było danych o pacjentach. Nie posiadali oni również żadnych innych oznaczeń (np. opasek na nadgarstkach)[35].

W dyżurkach pielęgniarskich ww. oddziałów dane osobowe pacjentów zawarte w dokumentacji medycznej były przechowywane w szufladach lub szafach, które za wyjątkiem Oddziału nr 6 koedukacyjnego[36] posiadały możliwość zamknięcia na klucz. Prowadzone w dyżurkach listy z nazwiskami pacjentów i wskazaniem sal, na których przebywali (tzw. ruch chorych), zawierały dane osobowe pacjentów, i za wyjątkiem dyżurki Oddziału nr 1[37], były poza zasięgiem wzroku osób postronnych przebywających w tych pomieszczeniach. Nie stwierdzono przypadków opuszczenia przez pielęgniarki dyżurek bez zamykania tych pomieszczeń na klucz. Logowanie do komputera wymagało dwustopniowego podania loginu i hasła,

[35] Tj. zgodnie z art. 36 ust. 3 i 4 ustawy o działalności leczniczej.
[36] O czym szerzej w sekcji „Stwierdzone nieprawidłowości".
[37] Jak wyżej.

a automatyczne blokowanie dostępu następowało po 10 minutach stanu bezczynności. Nie stwierdzono przypadków pozostawienia w dyżurce niezablokowanego komputera.

Dokumentacja medyczna w gabinetach lekarskich Oddziału nr 1 i Oddziału nr 6 (żeńskiego) była przechowywana w szafach zamykanych na klucz. Szafy na Oddziale nr 6 (koedukacyjnym) i na Oddziale nr 13 nie miały natomiast zamknięcia[38]. W trakcie oględzin Oddziału nr 1 osoby z personelu opuściły gabinet, zamykając go i zabierając klucz, w pozostałych przypadkach osoby te nie opuszczały gabinetów.

Oględziny stanowiska rejestracji pacjentów Laboratorium Diagnostycznego i stanowiska (wspólnego) rejestracji do obydwu poradni przyszpitalnych (Geriatrycznej oraz Zdrowia Psychicznego) wykazały, że: dane osobowe (dokumentacja medyczna) pacjentów nie były widoczne dla osób postronnych (byli oni oddzieleni od rejestratorek wysokimi pulpitami) a lokalizacja monitorów komputerów uniemożliwiała innym osobom wgląd do wyświetlanych danych. Rejestracja pacjentów odbywała się na podstawie okazywanych dowodów osobistych, pracownicy stanowisk rejestracji w kontaktach z pacjentami nie wypowiadali na głos informacji zawierających dane osobowe. Kolejność wizyt pacjentów była ustalana zgodnie z kolejnością zgłoszeń i była realizowana przez samych pacjentów, z zachowaniem ich anonimowości.

Rejestracja w Laboratorium odbywała się w odrębnym pomieszczeniu, gdzie w widocznym miejscu znajdowała się tablica informująca pacjentów o konieczności wchodzenia pojedynczo i klauzula informacyjna zawierająca: dane AD, IOD, ich funkcje, cele i podstawy przetwarzania danych i ich kategorie, okres przechowywania danych. Oględziny wykazały nieobecność rejestratorki w Laboratorium, drzwi do tego pomieszczenia były otwarte, a monitor komputera był włączony (komputer nie był zablokowany)[39]. System HIS[40] nie był uruchomiony.

Oględziny obydwu poradni przyszpitalnych: Geriatrycznej i Zdrowia Psychicznego, pod kątem sposobu przetwarzania danych osobowych, wykazały, że sposób wzywania pacjenta do gabinetu zapewniał mu anonimowość. Kolejność wizyt pacjentów odpowiadała kolejności zgłoszenia na wspólnym dla tych poradni stanowisku rejestracji i nie byli oni imiennie wzywani przez lekarza. W widocznym dla pacjentów miejscu tej rejestracji nie zamieszczono natomiast klauzuli informacyjnej, o której mowa w art. 13 ust. 1-2 RODO[41].

W gabinecie lekarskim karta pacjenta nie była widoczna dla kolejnego pacjenta. Nie stwierdzono również przypadków pozostawienia przez lekarza gabinetu lekarskiego lub komputera bez nadzoru.

Polityka zawierała[42] regulamin funkcjonowania monitoringu wizyjnego. Do realizacji zadań z tego zakresu[43] został wyznaczony ASI Szpitala i były one przez niego wykonywane.

(dowód: akta kontroli str. 290-304, 337-354, 422-426, 428-429)

2.2. Dokumentacja medyczna była w Dziekance prowadzona w wersji papierowej, bez jej wytwarzania z zastosowaniem modułu EDO, wchodzącego w skład HIS. Personel niemedyczny Szpitala, za wyjątkiem działów: Informatyki oraz Statystyki i Sprawozdawczości Medycznej, pracował w odrębnym budynku Administracji Szpitala i liczył 52 osoby. Żaden z pracowników w tym budynku nie przetwarzał

[38] Jak wyżej.
[39] Jak wyżej.
[40] Hospital Information System – oprogramowanie do obsługi pacjentów wewnątrz podmiotu leczniczego.
[41] O czym szerzej w sekcji „Stwierdzone nieprawidłowości".
[42] W części: „Procedury Bezpieczeństwa", Procedura P_23 „Regulamin funkcjonowania monitoringu wizyjnego".
[43] W tym: utrwalanie materiału z monitoringu wizyjnego i przechowywanie przez 30 dni.

danych medycznych pacjentów ani nie miał do nich dostępu, ponieważ system HIS nie był w tym budynku zainstalowany. Spośród pozostałych stanowisk niemedycznych zlokalizowanych w innych budynkach Szpitala, pełny dostęp do danych medycznych mieli jedynie pracownicy ww. dwóch działów, co wynikało z zakresów ich obowiązków.

(dowód: akta kontroli str. 179-188, 371-388a, 390-391)

2.3. ADO wydawał upoważnienia do przetwarzania danych osobowych odpowiednich (tzn. w zakresie odpowiadającym realizowanym zadaniom) grupom zawodowym m.in. takim jak: lekarze, pielęgniarki, instruktorzy terapii zajęciowej, opiekunowie, technicy EEG i RTG, pracownicy komórek: BHP, biblioteki, laboratorium, poradni, działów: organizacyjnego, finansowego, informatyki, jakości usług, spraw pracowniczych, statystyki i sprawozdawczości medycznej, technicznego, zamówień publicznych, epidemiologii, izby przyjęć, księgowości, działu żywienia. Nie wydawał natomiast takich upoważnień, salowym ani personelowi sprzątającemu.

Personel medyczny Szpitala (lekarze i pielęgniarki) miał uprawnienia użytkownika systemu nadane mu przez ADO i uczestniczył w procesie przetwarzania danych osobowych w stopniu adekwatnym do realizowanych obowiązków. Wszystkim 30 losowo wybranym i skontrolowanym pielęgniarkom przypisano uprawnienia dostępu do danych osób leczonych wyłącznie na oddziałach, na których pracowały.

(dowód: akta kontroli str. 244-272, 310-311)

2.4. Wszystkim 32 pracownikom, którzy zakończyli pracę w okresie od 25 maja 2018 r. do dnia kontroli NIK (6 lutego 2019 r.), najpóźniej w dniu zakończenia stosunku pracy zdeaktywowano dostęp do systemów informatycznych zawierających dane osobowe pacjentów.

(dowód: akta kontroli str. 244-272, 312-315)

2.5. Dziekanka korzystała z mechanizmu zdalnego zgłaszania usterek dostawcom oprogramowania związanego z udzielaniem świadczeń zdrowotnych. Szpital miał zawartą jedną umowę[44] dotyczącą świadczenia usług serwisu oprogramowania i pomocy technicznej tzw. help desk. W okresie objętym kontrolą NIK odnotowano 92 przypadki korespondencji z usługodawcą poprzez help desk. W zbadanej przez NIK próbie losowo wybranych 50 zapisów tej korespondencji nie wystąpiły przypadki ujawnienia danych osobowych.

(dowód: akta kontroli str. 329-331, 335-362)

2.6. Szpital w okresie objętym kontrolą NIK był stroną 10 zawartych umów, na podstawie których powierzył przetwarzanie danych osobowych, oraz jednej umowy, na podstawie której przetwarzanie tych danych powierzono jemu. Umowy te dotyczyły 10 podmiotów medycznych i jednego informatycznego (dostawca usług informatycznych z zakresu oprogramowania, wraz z usługą help desk). Analiza treści pięciu wybranych umów wykazała, że po 25 maja 2018 r. zostały zawarte do tych umów odpowiednie aneksy, w których ujęto wymogi z zakresu ochrony danych osobowych pacjentów i pracowników Szpitala, określone art. 28 ust. 3 RODO.

W odniesieniu do przesłanek zawierania ww. umów Dyrektor wyjaśnił, że wynikały one z konieczności realizacji zadań z zakresu świadczeń medycznych, których Szpital nie może samodzielnie zapewnić, a także z potrzeby sprawnego i skutecznego rozwiązywania problemów informatycznych.

[44] Nr 1/2017 z 23 lutego 2017 r. na sprawowanie pełnego nadzoru autorskiego oraz świadczenia opieki serwisowej nad szpitalnym zintegrowanym systemem informatycznym.

Rejestr umów powierzenia przetwarzania danych osobowych został założony dopiero w trakcie kontroli NIK[45], w dniu 22 lutego 2019 r.

(dowód: akta kontroli str. 316-329, 355-362, 389, 392-426, 428-429)

2.7. W prowadzonym przez IOD Dzienniku Uchybień i Zagrożeń, do dnia rozpoczęcia kontroli NIK, nie odnotowano przypadków naruszenia zasad ochrony danych osobowych pacjentów. Do Szpitala nie wpływały także skargi lub wnioski dotyczące ochrony tych danych. Zgodnie z wymogami Polityki[46], stwierdzony w toku kontroli NIK przypadek naruszenia zasad ochrony danych osobowych pacjentów[47] został niezwłocznie zgłoszony[48] przez ASI do IOD i odnotowany w ww. Dzienniku. IOD zaakceptował podjęte przez Szpital działania korygujące, polegające na: pouczeniu personelu Laboratorium o konieczności każdorazowego wylogowania się z systemu operacyjnego, poddaniu analizie czynności logowania i wylogowania oraz sprawdzeniu komputera pod względem poprawności działania mechanizmów zabezpieczających.

(dowód: akta kontroli str. 354a-362)

2.8. W Regulaminie Organizacyjnym i w Polityce określono zasady udostępniania dokumentacji medycznej. Wskazano m.in., że Szpital[49] udostępnia dokumentację medyczną pacjentów na podstawie złożonych przez nich wniosków, z zachowaniem i przestrzeganiem tajemnicy zawartej w dokumentacji. W Rejestrze Udostępnionej Dokumentacji Medycznej (był on prowadzony w wersji papierowej) odnotowano w okresie objętym kontrolą NIK 284 przypadki udostępnienia dokumentacji medycznej pacjentów Szpitala, w tym w 112 wydano ją pacjentom, a w 172 podmiotom lub osobom innym niż pacjent (w 137 - instytucjom, w tym w pięciu – zakładom ubezpieczeń[50] a w 35 - osobom fizycznym). Badanie prawidłowości udostępniania ww. dokumentacji osobom fizycznym innym niż pacjent[51] i zakładom ubezpieczeń[52] wykazało, że została ona wydana upoważnionym osobom. Zapytania od zakładów ubezpieczeń na podstawie art. 38 i 40 ustawy o działalności ubezpieczeniowej, każdorazowo zawierały uwierzytelnioną kopię upoważnienia od pacjenta i kopię polisy zawierającej zgodę pacjenta na wystąpienie w jego imieniu i uzyskanie jego danych medycznych.

Szpital nie prowadził ewidencji odrzuconych wniosków o wydanie dokumentacji medycznej. Kierownik Działu Statystyki i Sprawozdawczości Medycznej wyjaśniła, że z uwagi na to, że Dziekanka nie prowadzi elektronicznego rejestru wniosków, nie jest w stanie podać liczby odmów udostępnienia dokumentacji medycznej bez przejrzenia dokumentacji medycznej wszystkich pacjentów. Liczba pacjentów na dzień kontroli to około 800 osób, a dokumentacja medyczna jest przechowywana w sześciu archiwach. Szpital na obszarze ok. 30 ha mieści się w 24 budynkach pełniących funkcje medyczne. Dodała, że każdy wniosek o udostępnianie dokumentacji medycznej podlega weryfikacji a w przypadku odmowy jej wydania wnioskujący jest informowany o prawie do złożenia skargi.

(dowód: akta kontroli str. 332a-335)

2.9. Oględziny serwerowni Szpitala wykazały, że była ona odpowiednio zabezpieczona. Dostęp do niej był możliwy wyłącznie przez drzwi zabezpieczone

[45] O czym szerzej w sekcji „Stwierdzone nieprawidłowości".
[46] P_9_ Procedura Alarmowa.
[47] O którym szerzej w punkcie 1. sekcji „Stwierdzone nieprawidłowości".
[48] W tym samym dniu, w formie Protokołu Zagrożenia/Uchybienia.
[49] Dział Statystyki i Sprawozdawczości Medycznej.
[50] W rozumieniu ustawy z dnia 11 września 2015 r. o działalności ubezpieczeniowej i reasekuracyjnej (Dz. U. z 2019 r. poz. 381), dalej: ustawa o działalności ubezpieczeniowej.
[51] Badaniem objęto 30 szt. losowo wybranych przypadków.
[52] Badaniem objęto wszystkie przypadki.

antywłamaniowo i przeciwpożarowo, wyposażone w dwa zamki. Serwerownię wyposażono w systemy: klimatyzacji, wykrywania pożaru, sygnalizacji włamania, monitoringu wizyjnego (nad wejściem była umieszczona kamera monitoringu wizyjnego, nadzorowanego przez ASI), zainstalowano czujnik wykrywania zalania i umieszczono gaśnicę przeciwpożarową, posiadającą aktualny atest ważności. Okno serwerowni było trwale zabezpieczone przed dostępem z zewnątrz (okratowane). Serwery znajdujące się w pomieszczeniu były umieszczone w specjalnie do tego przeznaczonych szafach, zainstalowane były urządzenia do podtrzymania napięcia na wypadek zaniku zasilania (UPS-y), nie było zbędnych lub łatwopalnych materiałów. Według oświadczenia ASI, kopie zapasowe baz danych systemu HIS były wykonywane dwa razy dziennie, kopie inkrementalne (przyrostowe[53]) – cztery razy dziennie. Kopie baz danych pozostałych systemów[54] były wykonywane raz dziennie. Wszystkie kopie zapasowe baz danych były bezpiecznie przechowywane w szafie oddzielnego, zamykanego i okratowanego pomieszczenia poza serwerownią, z wyłącznym dostępem dla pracowników Działu Informatyki. Fakt dokonania przez NIK oględzin serwerowni został odnotowany w dzienniku zdarzeń, prowadzonym przez Dział Informatyki.
W Dziekance łączna liczba stanowisk komputerowych, w tym: terminali, komputerów stacjonarnych i komputerów mobilnych, wynosiła 362. Nie były one przypisane do konkretnych użytkowników. Każdy użytkownik mógł zalogować się na każdym komputerze, stosownie do swoich uprawnień wynikających z wyznaczonego mu stanowiska pracy i miejsca jej wykonywania. Wszystkie stanowiska komputerowe posiadały aktualny system operacyjny[55]. Profile użytkowników były przechowywane na serwerze Szpitala, w związku z tym, żaden jego pracownik po zalogowaniu się na komputerze, na którym przed chwilą ktoś inny pracował, nie miał dostępu do danych poprzednika - w momencie logowania z serwera każdorazowo były pobierane tylko pliki aktualnego użytkownika. Do uwierzytelnienia w systemie operacyjnym wykorzystywane było logowanie domenowe - każdy użytkownik posiadał unikatowy login, nadawany mu przez ASI. Standardowy login składał się z kilku pierwszych liter imienia i nazwiska. W przypadku, gdy taka kombinacja była zajęta, ADO nadawał użytkownikowi niestandardowy login. Dodatkowo, w przypadku terminali, w celu odblokowania urządzenia do zalogowania, konieczne było zastosowanie indywidualnej karty chipowej.

Oględziny 30 losowo wybranych komputerów służących do przetwarzania danych osobowych (w tym po 10 szt. użytkowanych przez: lekarzy, pielęgniarki oraz pracowników administracji Szpitala) wykazały, że dane te były przetwarzane z zachowaniem zasad określonych w regulaminach wchodzących w skład Polityki. Uwierzytelnianie użytkownika w systemie operacyjnym komputera następowało wyłącznie z użyciem loginu i hasła dostępu, które miało odpowiednią liczbę znaków. Użytkownicy mieli uprawnienia zgodne z konfiguracją domeny, bez możliwości zainstalowania dowolnego oprogramowania. Komputery były wykorzystywane zgodnie z przeznaczeniem wynikającym z zakresu dostępu do systemu, były zabezpieczone przed podłączeniem do nich zewnętrznych nośników pamięci i posiadały aktualny program antywirusowy. Nie wystąpiły przypadki zalogowania się do systemu z wykorzystaniem loginu lub hasła przez osobę, która nie była właścicielem tego loginu.

---

[53] Kopia przyrostowa bazuje na schemacie tworzenia kopii zapasowej danych, które zostały zmienione lub dodane, od czasu utworzenia ostatniej, dowolnej kopii zapasowej. Kopia przyrostowa nie kumuluje plików nowych i zmodyfikowanych, dlatego każdorazowo odnosi się do ostatniej wykonanej kopii zapasowej, pomijając poprzednie.

[54] W tym: Simple i Płatnik.

[55] W przypadku terminali był to Windows Server 2008 R2, a w przypadku komputerów i laptopów był to MS Windows, wersja 7, 8.1 lub 10.

(dowód: akta kontroli str. 53-188, 299-304, 363-365, 371-389, 427)

Stwierdzone nieprawidłowości

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

1. Stwierdzono ryzyko nieuprawnionego zapoznania się z danymi zastrzeżonymi wyłącznie dla personelu Szpitala w sytuacji, gdy rejestratorka Laboratorium opuściła pomieszczenie, w którym wykonywała swoje zadania, pozostawiając niezamknięte drzwi i włączony komputer, niezabezpieczony przed dostępem do systemu[56] osób nieupoważnionych.

W Polityce[57] wskazano m.in. niezamykanie pomieszczeń oraz niestosowanie zasady czystego ekranu jako typowe incydenty w obszarze bezpieczeństwa danych, wymagające przeprowadzenia postępowania wyjaśniającego. W przypadku pozostawienia bez nadzoru pomieszczenia, w którym przechowywane są dane osobowe oraz komputera niezabezpieczonego hasłem, należało zabezpieczyć te dane oraz powiadomić IOD, który sporządzał protokół uchybienia[58].

Rejestratorka wyjaśniła, że opuszczenie przez nią miejsca pracy wynikało z konieczności przekazania materiału biochemicznego (co wynikało z jej zakresu czynności), do pracowni mieszczącej się o dwa pokoje dalej. Podała, że trwało to - jej zdaniem - nie dłużej niż 2 minuty i nie była w tym czasie zalogowana do systemu HIS. Dodała, że w czasie jej nieobecności nie nastąpiło ujawnienie danych osobowych na zewnątrz, a komputer zostałby automatycznie zablokowany po upływie 10 minut bezczynności.

NIK wskazuje, że wprawdzie ww. rejestratorka została w dniu 24 maja 2018 r. przeszkolona na stanowisku pracy w związku z rozpoczęciem stosowania RODO, jednak szkolenie to nie obejmowało przypomnienia o konieczności każdorazowego blokowania komputera przed opuszczeniem stanowiska pracy. Szkolenie uzupełniające zostało przeprowadzone w trakcie kontroli NIK, 12 lutego 2019 r. Dyrektor wyjaśnił, że pouczono personel Laboratorium o konieczności każdorazowego blokowania stacji roboczych (wylogowania się z systemu operacyjnego). Ponadto wskazał, że w celu wyeliminowania analogicznych sytuacji Szpital poszerzy zakres szkolenia o elementarne zasady pracy z danymi osobowymi na stanowiskach komputerowych.

(dowód: akta kontroli str. 141, 145, 337-354b, 422-426)

2. Prowadzona w dyżurce pielęgniarskiej Oddziału nr 1 lista zawierająca imiona i nazwiska pacjentów wraz ze wskazaniem sali, na której przebywają (tzw. ruch chorych), była widoczna dla wszystkich osób przebywających w tym pomieszczeniu, także nieuprawnionych. Ponadto, w dyżurce pielęgniarskiej Oddziału nr 6 koedukacyjnego oraz w gabinetach lekarskich Oddziału nr 6 koedukacyjnego i Oddziału nr 13 dokumentacja medyczna pacjentów była przechowywana w szafach, które nie były zamykane na klucz.
Stan ten stwarzał ryzyko ujawnienia tych danych osobom nieuprawnionym i był niezgodny z motywem 39 preambuły oraz art. 5 ust. 1 lit. f. RODO, w myśl których 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. Także w Polityce wskazano m.in. niewłaściwe zabezpieczenie fizyczne pomieszczeń i dokumentów oraz niezamykanie szaf jako incydent w obszarze

[56] Z wyłączeniem systemu HIS, do którego nie była zalogowana.
[57] Procedura P_09 Procedura alarmowa, ust. 3 lit. c i ust. 5.
[58] Rejestr Uchybień i Zagrożeń oraz postępowanie osób funkcyjnych (kod 1 i 2).

bezpieczeństwa danych, wymagający przeprowadzenia postępowania wyjaśniającego[59].

Dyrektor wyjaśnił, że ruch chorych w ww. dyżurce został w trakcie kontroli NIK skutecznie zabezpieczony przed ujawnieniem danych osobowych pacjentów, oraz zadeklarował, iż pozostałe nieprawidłowości zostaną na bieżąco usunięte. Podał też, że Szpital dokona oględzin pozostałych oddziałów i do końca czerwca 2019 r. uzupełni ewentualne braki w ww. zakresie.

(dowód: akta kontroli str. 141, 145, 337-344, 422-426, 428-429)

3. W Szpitalu do dnia 22 lutego 2019 r. nie prowadzono odrębnego rejestru podmiotów, którym w drodze umowy powierzono przetwarzanie danych osobowych. Dyrektor wyjaśnił, że w Szpitalu zamiast odrębnego rejestru ww. umów, był prowadzony rejestr wszystkich umów. Podniósł ponadto, że żaden z przepisów RODO ani ustawy nie przewiduje obowiązku prowadzenia takiego rejestru.

NIK wskazuje, że obowiązek prowadzenia przedmiotowego rejestru wynikał z obowiązującej w Szpitalu Polityki[60]. Rejestr ten został założony w trakcie kontroli NIK.

(dowód: akta kontroli str. 153, 389, 422-426)

4. Na wspólnym stanowisku rejestracji dla Poradni Geriatrycznej oraz Poradni Zdrowia Psychicznego w widocznym dla pacjentów miejscu brakowało klauzuli informacyjnej zawierającej m.in. dane AD i IOD, cele i podstawy przetwarzania danych i ich kategorie oraz okres przechowywania danych, tj. informacje, o których mowa w art. 13 ust. 1-2 RODO. Zgodnie z tymi przepisami, jeżeli dane osobowe osoby, której dane dotyczą, są od niej zbierane, to administrator podczas pozyskiwania tych danych podaje jej wszystkie ww. informacje.

Dyrektor wskazał, że klauzula ta znajdowała się w pomieszczeniu ww. poradni, jednocześnie przyznając, iż była niewidoczna dla pacjentów.

W toku oględzin NIK, ww. klauzula została umieszczona na tablicy ogłoszeń.

(dowód: akta kontroli str. 338, 422-426)

OCENA CZĄSTKOWA

W Szpitalu dane osobowe nie były w pełni prawidłowo chronione i przetwarzane. Zakres dostępu personelu Dziekanki do danych osobowych był adekwatny do potrzeb na zajmowanym przez poszczególne osoby stanowisku. Właściwie udostępniano dokumentację medyczną pacjentów i zawierano wymagane umowy powierzenia przetwarzania danych osobowych, które spełniały wymogi określone w art. 28 RODO. Szpitalne komputery były wykorzystywane zgodnie z przeznaczeniem wynikającym z zakresu dostępu personelu do systemów i odpowiednio zabezpieczone. Podejmowano też odpowiednie działania w celu minimalizacji ryzyka utraty tych danych. Wystąpiły jednak pojedyncze przypadki wskazujące na możliwość nieuprawnionego ujawnienia danych osobowych pacjentów przy ich rejestrowaniu, prowadzeniu ruchu chorych i przechowywaniu dokumentacji medycznej w dyżurkach pielęgniarskich i gabinetach lekarskich. Na stanowisku jednej z rejestracji brakowało też klauzuli informacyjnej, o której mowa w art. 13 ust. 1-2 RODO. Nieprawidłowość polegająca na nieprowadzeniu odrębnego rejestru podmiotów, którym w drodze umowy powierzono przetwarzanie danych osobowych, miała charakter formalny.

[59] Procedura P_09 Procedura alarmowa, ust. 3 lit. c i ust. 5, a także Rejestr Uchybień i Zagrożeń oraz postępowanie osób funkcyjnych (kod 3 i 7).
[60] Procedura P_14 Dostępu Podmiotów Zewnętrznych, ust. 1

IV. Wnioski

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

1) zaktualizowania regulaminu organizacyjnego Szpitala w zakresie stanowiska i zadań IOD,
2) objęcia wszystkich pracowników Szpitala zaangażowanych w proces przetwarzania danych osobowych szkoleniami z zakresu przepisów RODO,
3) zapewnienia organizacji pracy w zakresie: zabezpieczania opuszczanych pomieszczeń, rozpoczynania i zawieszania pracy z systemami informatycznymi, prowadzenia ruchu chorych oraz przechowywania dokumentacji medycznej, zapewniającej pełną ochronę danych osobowych.

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

Poznań, dnia 17 kwietnia 2019 r.

Najwyższa Izba Kontroli
Delegatura w Poznaniu

Kontroler	Dyrektor
Mirosław Babkiewicz	z up. Tomasz Nowiński
Specjalista kontroli państwowej	p.o. Wicedyrektor
.....	.....
podpis	*podpis*