NAJWYŻSZA IZBA KONTROLI
Delegatura w Białymstoku

LBI.410.002.04.2019

00069419

Pani Krystyna Marianna Dobrołowicz
Szpital Ogólny w Kolnie
ul. Wojska Polskiego 69, 18-500 Kolno

WYSTĄPIENIE POKONTROLNE

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

NAJWYŻSZA IZBA KONTROLI
Delegatura w Białymstoku
ul. Akademicka 4, 15-267 Białystok
T +48 85 874 81 00, F +48 85 874 81 33
lbi@nik.gov.pl

I. Dane identyfikacyjne

Jednostka kontrolowana	Szpital Ogólny w Kolnie[1], ul. Wojska Polskiego 69, 18-500 Kolno
Kierownik jednostki kontrolowanej	Krystyna Marianna Dobrołowicz – Dyrektor Szpitala od 27 maja 2004 r.
Zakres przedmiotowy kontroli	1. Opracowanie wymaganej dokumentacji oraz procedur związanych z ochroną przetwarzanych danych osobowych. 2. Zapewnienie prawidłowego przetwarzania i ochrony danych osobowych.
Okres objęty kontrolą	Od 25 maja 2018 r. do dnia zakończenia czynności kontrolnych NIK, tj. do 25 marca 2019 r. Badania kontrolne dotyczyły również działań sprzed tego okresu, jeśli miały związek z zagadnieniami będącymi przedmiotem kontroli.
Podstawa prawna podjęcia kontroli	Art. 2 ust. 2 ustawy z dnia 23 grudnia 1994 r. o Najwyższej Izbie Kontroli[2]
Jednostka przeprowadzająca kontrolę	Najwyższa Izba Kontroli Delegatura w Białymstoku
Kontrolerzy	1. Marcin Kiersnowski, specjalista kontroli państwowej, upoważnienie do kontroli nr LBI/27/2019 z 6 lutego 2019 r. 2. Piotr Jurkin, specjalista kontroli państwowej, upoważnienie do kontroli nr LBI/36/2019 z 7 marca 2019 r. (akta kontroli str. 1-5)

[1] Dalej: *Szpital*.
[2] Dz. U. z 2019 r. poz. 489. Ustawa zwana dalej: *ustawą o NIK*.

II. Ocena ogólna[3] kontrolowanej działalności

OCENA OGÓLNA

W Szpitalu dane osobowe nie były w pełni prawidłowo chronione i przetwarzane.

Uzasadnienie oceny ogólnej

Szpital wywiązał się z obowiązku powołania Inspektora Ochrony Danych i zgłoszenia tego faktu Prezesowi Urzędu Ochrony Danych Osobowych. Przeprowadzono wymaganą analizę ryzyka procesów przetwarzania danych osobowych oraz opracowano rejestr czynności przetwarzania tych danych. Pracowników Szpitala zapoznawano zaś z regulacjami dotyczącymi ochrony danych osobowych.

W Szpitalu prawidłowo chroniono i przetwarzano dane osobowe w skontrolowanych trzech oddziałach szpitalnych, dwóch (z trzech) poradniach specjalistycznych oraz w rejestracji ogólnej do poradni specjalistycznych. Personel administracyjny Szpitala oraz 26 pielęgniarek i położnych (z 30 analizowanych) przetwarzało dane osobowe w systemie HIS[4] adekwatnie do realizowanych zadań i obowiązków, a wszystkim byłym pracownikom Szpitala zablokowano dostęp do tego systemu. W pięciu analizowanych umowach powierzenia przetwarzania danych osobowych zamieszczono postanowienia wymagane art. 28 RODO[5]. Dokumentację medyczną pacjentów we wszystkich 33 skontrolowanych sprawach udostępniono zaś wyłącznie uprawnionym podmiotom.

Zastosowano fizyczne zabezpieczenia serwerowni Szpitala, w której przechowywano dane osobowe przetwarzane w formie elektronicznej oraz zminimalizowano ryzyko ich utraty lub nieuprawnionej modyfikacji za pośrednictwem wszystkich 30 objętych kontrolą komputerów.

Stwierdzono jednak nieprawidłowości, które polegały na:

- dostosowaniu regulacji wewnętrznych Szpitala do RODO dopiero po upływie ponad ośmiu miesięcy od wejścia w życie tego rozporządzenia,
- nieprowadzeniu, wbrew regulacjom wewnętrznym Szpitala, ewidencji osób upoważnionych do przetwarzania danych osobowych,
- nieprzestrzeganiu przez personel jednej poradni specjalistycznej (z trzech skontrolowanych) regulacji wewnętrznych dotyczących sposobu zabezpieczania papierowej dokumentacji medycznej,
- nadaniu czterem (z 30 analizowanych) pracownikom uprawnień w systemach informatycznych Szpitala w zakresie nieadekwatnym do realizowanych przez nich zadań i obowiązków,
- przechowywaniu kopii zapasowych elektronicznych baz danych Szpitala w tym samym pomieszczeniu, w którym przechowywano dane produkcyjne.

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. Wykonywanie na rzecz Szpitala czynności Inspektora Ochrony Danych (dalej: *IOD*) od 27 kwietnia 2018 r. zlecono osobie fizycznej.

Zgodnie z wymogami art. 37 ust. 5 RODO, IOD miał należyte przygotowanie i kwalifikacje zawodowe do pełnienia swojej funkcji. Ukończył m.in. studia podyplomowe w zakresie

---

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

[4] Hospital Information System – rodzaj oprogramowania przeznaczony do prowadzenia w wersji elektronicznej dokumentacji medycznej zbiorczej i indywidualnej oraz zarządzania ruchem chorych na oddziałach i w poradniach podmiotu leczniczego.

[5] Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (ogólne rozporządzenie o ochronie danych). Dz. Urz. UE L 119 z 2016 r., str. 1, ze zm. Dalej: *RODO*.

[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.

Menedżer bezpieczeństwa informacji z archiwistyką i w zakresie *Inspektor Ochrony Danych Osobowych oraz Administrator Danych.*

Dane kontaktowe IOD (e-mail, nr telefonu) opublikowano 11 maja 2018 r. na stronie internetowej Szpitala, co było zgodne z art. 37 ust. 7 RODO.

Szpital zawiadomił Prezesa Urzędu Ochrony Danych Osobowych o wyznaczeniu IOD w terminie określonym art. 158 ust. 4 ustawy z dnia 10 maja 2018 r. o ochronie danych osobowych[7]. Przekazane 31 lipca 2018 r. zawiadomienie zawierało wszystkie elementy określone art. 10 ust. 3 ustawy o ochronie danych osobowych. W związku z problemami technicznymi nieleżącymi po stronie Szpitala, zawiadomienie przesłano pierwotnie faksem, listem oraz e-mailem, a następnie (11 grudnia 2018 r.) w formie wymaganej art. 10 ust. 6 ustawy o ochronie danych osobowych.

IOD umożliwiono realizowanie obowiązków w sposób niezależny, stosownie do art. 38 ust. 3 i ust. 4 RODO. Wykonywał on bowiem w Szpitalu jedynie zadania IOD. Jednak dopiero w obowiązującej w Szpitalu od 4 lutego 2019 r. Polityce Ochrony Danych Osobowych zawarto zapisy gwarantujące jego niezależność. Określono m.in. bezpośrednią podległość IOD najwyższemu kierownictwu Szpitala, zakaz karania lub odwoływania IOD za wykonywanie czynności związanych z ochroną danych osobowych oraz zakaz wydawania poleceń dotyczących sposobu realizacji zadań IOD.

(akta kontroli str. 7-25, 101-103)

Do 11 lutego 2019 r. Szpital nie został uznany za operatora usługi kluczowej o której mowa w ustawie z dnia 5 lipca 2018 r. o krajowym systemie cyberbezpieczeństwa[8]. Do tego dnia nie otrzymał również zawiadomienia o wszczęciu wobec niego postępowania administracyjnego w sprawie uznania go za operatora takiej usługi. (akta kontroli str. 13)

1.2. Od 4 listopada 2016 r. do 4 lutego 2019 r. w Szpitalu obowiązywały; [1] *Polityka Bezpieczeństwa Danych Osobowych w Systemach Informatycznych w Szpitalu Ogólnym w Kolnie*; [2] *Instrukcja zarządzania systemem informatycznym przetwarzającym dane osobowe w Szpitalu Ogólnym w Kolnie*; [3] *Instrukcja postępowania w sytuacji naruszenia ochrony danych osobowych w Szpitalu Ogólnym w Kolnie.* Zostały one wprowadzone do stosowania zarządzeniami Dyrektora Szpitala nr 22/2016 oraz 23/2016 z 4 listopada 2016 r. i do 4 lutego 2019 r. nie były aktualizowane. Jako podstawę prawną opracowania tych instrukcji i polityki podano przepisy dotyczące ochrony danych osobowych w brzmieniu obowiązującym przed 25 maja 2018 r.[9]

W wymienionych dokumentach określono m.in.: [1] zasady postępowania w przypadku naruszenia danych osobowych; [2] zasady udostępniania danych osobowych przetwarzanych na poziomie regionalnym Podlaskiego Systemu Informacyjnego e-Zdrowie; [3] mechanizmy zabezpieczenia danych osobowych, w tym reguły dotyczące udzielania dostępu do danych osobowych; [4] zasady tworzenia i przechowywania kopii zapasowych systemów służących do przetwarzania danych osobowych; [5] procedury nadawania i odbierania uprawnień do przetwarzania danych i rejestrowania tych zdarzeń w systemie informatycznym; [6] reguły pracy na stanowisku komputerowym; [7] sposób i czas przechowywania nośników informacji. W opisywanej dokumentacji nie uregulowano natomiast części wymogów przewidzianych w RODO oraz w przepisach krajowych obowiązujących po 25 maja 2018 r., co szerzej opisano w dalszej części wystąpienia, w pkt 1 sekcji *Stwierdzone nieprawidłowości.* (akta kontroli str. 13, 26-57)

Zarządzeniem Dyrektora Szpitala nr 7/2019 z 4 lutego 2019 r. wprowadzono w Szpitalu nową *Politykę Bezpieczeństwa Ochrony Danych Osobowych w Szpitalu Ogólnym w Kolnie* (dalej: *PBODO*). W celu zapoznania pracowników z jej treścią, została ona przekazana kierownikom wszystkich jednostek organizacyjnych Szpitala z poleceniem jej przestrzegania. Analiza dokumentacji 30 (z 311) osób wykonujących pracę w Szpitalu

---

[7] Dz. U. poz. 1000, ze zm. Ustawa zwana dalej: *ustawą o ochronie danych osobowych.*

[8] Dz. U. poz. 1560.

[9] Ustawa z dnia 29 sierpnia 1997 r. o ochronie danych osobowych (Dz. U. z 2016 r. poz. 922, ze zm.) oraz rozporządzenie Ministra Spraw Wewnętrznych i Administracji z dnia 29 kwietnia 2004 r. w sprawie dokumentacji przetwarzania danych osobowych oraz warunków technicznych i organizacyjnych, jakim powinny odpowiadać urządzenia i systemy informatyczne służące do przetwarzania danych osobowych (Dz. U. Nr 100, poz. 1024.)

wg stanu na 11 lutego 2019 r. wykazała, że wszyscy złożyli oświadczenie o zapoznaniu się z treścią PBODO.

Zgodnie z motywem 78 RODO, w PBODO określono m.in.: [1] obszar przetwarzania danych osobowych, [2] kategorie osób, których dane są przetwarzane, [3] instrukcje wypełniania praw właścicieli danych (prawo dostępu do danych, prawo do poprawiania i uzupełniania danych, prawo do usunięcia danych, prawo do ograniczenia przetwarzania, prawo do przenoszenia danych, obowiązek powiadomienia o sprostowaniu, usunięciu lub ograniczeniu przetwarzania), [4] zasady ochrony danych w fazie projektowania, [5] zasady domyślnej ochrony danych, [6] środki organizacyjne służące bezpieczeństwu danych osobowych (system upoważnień do przetwarzania danych, system oświadczeń o zachowaniu poufności, szkolenia z zakresu ochrony danych, obowiązki osób upoważnionych, zasady powierzania przetwarzania danych osobowych), [7] środki techniczne służące bezpieczeństwu danych osobowych (zasady niszczenia dokumentacji, sposób zabezpieczenia budynku i pomieszczeń, zasady postępowania z kluczami, zasady korzystania z portali internetowych i poczty elektronicznej, zarządzanie oprogramowaniem, metody i środki uwierzytelniania w systemach informatycznych oraz procedury związane z ich zarządzaniem i użytkowaniem), [8] zasady postępowania w przypadku stwierdzenia incydentu naruszenia bezpieczeństwa danych osobowych, [9] zadania osób odpowiedzialnych za funkcjonowanie systemu ochrony danych osobowych w Szpitalu, w tym administratora danych osobowych, IOD, administratora systemów informatycznych, kierowników komórek organizacyjnych.

Integralną częścią PBODO były załączniki, w tym m.in.: [1] wykaz budynków i pomieszczeń, w których przetwarza się dane osobowe, [2] procedura udostępniania dokumentacji medycznej, [3] wykaz zbiorów danych i systemów informatycznych wykorzystywanych do ich przetwarzania, [4] wykaz wejść do budynków Szpitala, [5] regulamin funkcjonowania monitoringu wizyjnego w Szpitalu, [6] procedura tworzenia kopii zapasowych systemów informatycznych (procedura przechowywana w dziale informatyki Szpitala).

W PBODO założono też prowadzenie m.in. 13 rejestrów i ewidencji wg. określonych wzorów. Do 21 marca 2019 r. założono i prowadzono 12 z nich, w tym. m.in.: rejestr czynności przetwarzania danych osobowych, rejestr kategorii przetwarzania, ewidencję udostępniania danych osobowych, karty sprzętu komputerowego i oprogramowania, rejestr wykonywanych przeglądów i konserwacji sprzętu, ewidencję naruszeń bezpieczeństwa ochrony danych osobowych Szpitala, rejestr czynności prowadzonych przez IOD. Do tego dnia w Szpitalu nie założono i nie prowadzono ewidencji osób upoważnionych do przetwarzania danych osobowych, co szerzej opisano w dalszej części wystąpienia, w pkt 2 sekcji *Stwierdzone nieprawidłowości.*

Poza procedurami stanowiącymi załączniki do PBODO, nie przewidziano konieczności opracowania dodatkowych instrukcji uszczegóławiających zasady ochrony danych w Szpitalu. (akta kontroli str. 13, 58-171)

1.3. Zgodnie z art. 30 ust. 1 RODO, w Szpitalu prowadzono rejestr czynności przetwarzania danych osobowych. Dyrektor Szpitala wyjaśniła, że: *rejestr czynności przetwarzania danych osobowych (...) opracowany został na dzień 25 maja 2018 r.* W rejestrze ujęto 153 czynności przetwarzania dotyczących zbiorów danych osobowych przetwarzanych w Szpitalu. Zgodnie z wymogami art. 30 ust. 1 oraz ust. 3 RODO, rejestr prowadzony był w formie pisemnej i elektronicznej oraz zawierał wszystkie wymagane elementy.
(akta kontroli str. 13, 172-196, 379-385)

1.4. Do 11 lutego 2019 r. w Szpitalu przeprowadzono jedną analizę ryzyka przetwarzania danych osobowych, określoną w art. 32 RODO. W ramach tej analizy zidentyfikowano 22 zagrożeń (ryzyk) związanych z ochroną danych osobowych. Dla każdego z nich oszacowano poziom ryzyka (w skali od jednego do dziewięciu punktów), określony jako iloczyn prawdopodobieństwa wystąpienia ryzyka i jego istotności. W 18 przypadkach poziom ryzyka oszacowano na poziomie akceptowalnym (do trzech punktów). W trzech przypadkach poziom ryzyka oszacowano na poziomie średnim (od czterech do sześciu punktów), a w jednym – na poziomie dużym (od siedmiu do dziewięciu punktów).

Dla wszystkich czterech zagrożeń, dla których wartość ryzyka była na poziomie średnim albo dużym, określono działania w celu redukcji poziomu ryzyka oraz termin ich realizacji.

Do 31 marca 2019 r. (w celu zmniejszenia poziomu ryzyka awarii sprzętu, zasilania oraz systemów informatycznych) przewidziano m.in.: [1] przeprowadzanie regularnych przeglądów sprzętu teleinformatycznego i instalacji, [2] opracowanie planu ciągłości działania i przywrócenia działania systemów po awarii, [3] opracowanie procedury zachowania ciągłości działania bez udziału systemu informatycznego, [4] opracowanie procedury szybkiego przywracania dostępności w systemach informatycznych. Natomiast do 28 lutego 2019 r. (w celu redukcji ryzyka awarii sprzętu i nośników służących przechowywaniu kopii zapasowych baz danych) zaplanowano opracowanie procedury odtwarzania kopii zapasowych oraz regularne testowanie i monitorowanie urządzeń służących do tworzenia i przechowywania kopii bezpieczeństwa.

Do zakończenia kontroli NIK w Szpitalu opracowano wszystkie wymienione cztery pisemne procedury. Dyrektor Szpitala wyjaśniła też, że: *w Szpitalu urządzenia służące do tworzenia i przechowywania kopii zapasowych są stale monitorowane. W konsoli oprogramowania do tworzenia kopii zapasowych (...) systematycznie sprawdzane są statusy prawidłowości tworzenia kopii. Kopie zapasowe umieszczone są na macierzy danych wyposażonej w redundantne zasilacze oraz interfejsy sieciowe, odporne na awarię dwóch dysków twardych jednocześnie. Ponadto Szpital jest w trakcie projektowania rozwiązania umożliwiającego przesyłanie kopii zapasowych na oddzielną dedykowaną pamięć sieciową, która będzie znajdowała się poza serwerownią główną Szpitala. W Szpitalu do chwili obecnej nie zaistniała konieczność odtwarzania systemów informatycznych z kopii zapasowych. W Szpitalu nie odtwarzano testowo kopii zapasowych ze względu na brak środowiska testowego. Z uwagi na ogromne koszty infrastrukturalne planowane jest uruchomienie środowiska testowego w ograniczonym zakresie na jednej z maszyn wirtualnych.* (akta kontroli str. 161-171, 197-204, 379-385)

1.5. W Szpitalu nie została wykonana ocena skutków dla ochrony danych, o której mowa w art. 35 RODO, ponieważ nie rozpoczęto przetwarzania nowych kategorii danych osobowych, w szczególności z użyciem nowych narzędzi, a placówka nie wprowadziła nowych rodzajów usług medycznych, które nie byłyby wykonywane wcześniej. Pojedyncza (bieżąca) ocena operacji wiążących się z wysokim ryzykiem jest fakultatywna, przy czym Grupa Robocza ds. Ochrony Danych[10] zalecała dokonanie oceny skutków dla ochrony danych dla operacji przetwarzania już trwających przed 25 maja 2018 r.[11] oraz w przypadkach, gdy nie jest jasne, czy taka ocena jest wymagana, ponieważ jest ona *przydatnym narzędziem, które może pomóc administratorom danych w zapewnieniu zgodności z prawem ochrony danych.* Dyrektor Szpitala wyjaśniła, że: *ocenę skutków planowanych operacji przetwarzania danych osobowych należy wykonać przed rozpoczęciem przetwarzania. W Szpitalu od 25 maja 2018 r. do chwili obecnej nie wdrażano nowych systemów, aplikacji, ani też przetwarzania nowych kategorii danych osobowych, co wiązałoby się z koniecznością przeprowadzenia takiej oceny. W związku z powyższym IOD stwierdził, że nie jest ona konieczna w obecnej sytuacji. Przeprowadzono natomiast analizę ryzyka przetwarzania danych osobowych w Szpitalu, która zawiera w sobie elementy oceny skutków dla ochrony danych, a przeprowadzana jest dla realizowanych w Szpitalu procesów przetwarzania.* (akta kontroli str. 13, 379-385)

1.6. Jednym z zadań IOD, w myśl art. 39 ust. 1 lit. b RODO, było prowadzenie szkoleń personelu uczestniczącego w operacjach przetwarzania danych. Kwestie przeprowadzania szkoleń zostały również określone w PBODO, gdzie wskazano, że wszyscy pracownicy, bez względu na formę zatrudnienia i charakter pracy, przed rozpoczęciem pełnienia obowiązków służbowych, zobligowani są do odbycia szkolenia z zakresu bezpieczeństwa danych osobowych przetwarzanych w Szpitalu. IOD, realizując wyżej wymieniony obowiązek, 22 i 29 maja oraz 12 czerwca 2018 r. przeprowadził grupowe szkolenia dla pracowników Szpitala z zakresu ochrony danych osobowych, w tym bezpieczeństwa informacji. Zakres szkoleń obejmował m.in. cele i zakres stosowania RODO, obowiązek

---

[10] Grupa Robocza była niezależnym organem doradczym w zakresie ochrony danych i prywatności. Została ona powołana na mocy 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 1995 r., str. 31, ze zm.) i działała do 25 maja 2018 r.

[11] Wytyczne dotyczące oceny skutków dla ochrony danych (https://www.giodo.gov.pl/1520281/id_art/9957/j/pl – dostęp z 18 marca 2019 r.).

informacyjny, pozycje IOD, podstawowe pojęcia związane z ochroną danych osobowych, zasady przetwarzania danych i zagrożenia z tym związane. W szkoleniach wzięło udział 161 z 311 (52%) osób świadczących pracę w Szpitalu na 11 lutego 2019 r. Szpital nie posiadał dokumentacji, potwierdzającej objęcie szkoleniami dotyczącymi ochrony danych osobowych pozostałej części personelu. Dyrektor Szpitala wyjaśniła, że: *w szkoleniach z zakresu ochrony danych osobowych nie uczestniczyli wszyscy pracownicy i współpracownicy Szpitala z rożnych powodów ich absencji, tj. zwolnień lekarskich, urlopów, dyżurów w innych podmiotach. Niemniej jednak materiały ze szkolenia IOD udostępnił wszystkim pracownikom komórek organizacyjnych Szpitala w celu zapoznania się z ich treścią oraz stosowania. Ponadto IOD podnosi cyklicznie świadomość pracowników Szpitala, dotyczącą zasad przetwarzania danych oraz zmian w tym zakresie, poprzez przekazywanie materiałów dotyczących ochrony danych (...). Wszyscy pracownicy Szpitala podpisali oświadczenia o zachowaniu poufności przetwarzanych przez nich danych osobowych.* Analiza akt osobowych 30 wybranych losowo pracowników Szpitala nieobjętych szkoleniami z 22 i 29 maja oraz 12 czerwca 2018 r. wykazała, że wszyscy złożyli oświadczenie o zapoznaniu się z przepisami RODO, ustawy o ochronie danych osobowych oraz PBODO i zobowiązali się do zachowania w tajemnicy przetwarzanych danych osobowych. Ponadto IOD, realizując obowiązek określony w art. 39 ust. 1 lit. b RODO, 2 października 2018 r. przekazał pracownikom Szpitala *Przewodnik po RODO w służbie zdrowia,* opracowany 24 września 2018 r. przez Ministerstwo Zdrowia oraz Ministerstwo Cyfryzacji[12]. (akta kontroli str. 81, 205-269, 379-385)

1.7. Szpital nie zobowiązał się formalnie (np. poprzez deklarację stosowania) do przestrzegania regulacji zawartych w *Kodeksie postępowania dla sektora ochrony zdrowia*[13], opracowanym przez Polską Federację Szpitali. Wniosek o jego przyjęcie, na podstawie art. 40 RODO, został 13 listopada 2018 r. przedłożony przez autorów Prezesowi Urzędu Ochrony Danych Osobowych. Dyrektor Szpitala wyjaśniła, że: *Szpital deklaruje stosowanie regulacji zawartych Kodeksie postępowania dla sektora ochrony zdrowia, gdy tylko zostanie oficjalnie zatwierdzony przez Prezesa Urzędu Ochrony Danych Osobowych.* (akta kontroli str. 13, 379-385)

Stwierdzone nieprawidłowości

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

1. Aktualizację regulacji wewnętrznych dotyczących ochrony danych osobowych, w celu dostosowania ich do przepisów RODO, zakończono w Szpitalu dopiero 4 lutego 2019 r., tj. po upływie ponad ośmiu miesięcy od wejścia w życie tego rozporządzenia. Do tego dnia obowiązywały regulacje wprowadzone zarządzeniami Dyrektora Szpitala nr 22/2016 oraz 23/2016 z 4 listopada 2016 r., które nie uwzględniały części wymogów przewidzianych w RODO oraz w przepisach krajowych obowiązujących po 25 maja 2018 r., w tym m.in. obowiązku zgłaszania naruszenia ochrony danych osobowych organowi nadzorczemu (art. 33 RODO), prawa do sprostowania danych (art. 16 RODO), prawa do usunięcia danych (art. 17 RODO), prawa do ograniczenia przetwarzania (art. 18 RODO), obowiązku powiadomienia o sprostowaniu lub usunięciu danych osobowych lub o ograniczeniu przetwarzania (art. 19 RODO), obowiązku informowania pracowników o wprowadzeniu monitoringu terenu Szpitala oraz monitoringu poczty elektronicznej (art. 22^2 oraz art. 22^3 ustawy z dnia 26 czerwca 1974 r. Kodeks pracy[14]), statusu IOD w strukturach Szpitala (art. 38 RODO).

   Przeprowadzenie aktualizacji regulacji wewnętrznych Szpitala po ponad ośmiu miesiącach, stanowiło naruszenie przepisu art. 24 ust. 1 i 2 RODO, zgodnie z którym do obowiązków administratora danych osobowych, należy m.in. poddawanie w razie potrzeby przeglądom i aktualizacja przyjętych polityk ochrony danych i regulacji wewnętrznych w tym zakresie. Dyrektor Szpitala wyjaśniła, że: *dokumentacja dotycząca ochrony danych osobowych na podstawie obowiązujących od 25 maja 2018 r. przepisów RODO, tworzona była przez IOD oraz personel Szpitala od początku maja 2018 roku.*

---

[12] https://www.gov.pl/web/cyfryzacja/rodo-w-sluzbie-zdrowia-po-pierwsze-pacjent – dostęp z 18 marca 2019 r.

[13] http://www.rodowzdrowiu.pl/wp-content/uploads/2018/11/2018-11-13-KODEKS-BRAN%C5%BBOWY-Wniosek-o-zatwierdzenie-kodeksu-postepowania.pdf – dostęp z 18 marca 2019 r.

[14] Dz. U. z 2018 r. poz. 917, ze zm.

Sukcesywnie opracowywano politykę oraz kolejne jej załączniki. Niektóre dokumenty takie, jak umowy powierzenia, rejestry czynności oraz kategorii przetwarzania, realizacja obowiązku informacyjnego i inne czynności zostały wykonane lub opracowane na dzień 25 maja 2018 r. Pozostałe załączniki do dokumentacji powstawały sukcesywnie. Zespoły pracowników opracowywały wraz z IOD poszczególne regulaminy i procedury, które niejednokrotnie były poprawiane i zmieniane. Ponieważ praca nad dokumentacją stanowiła dodatkowe zadania dla pracowników, a priorytetem dla nich było wykonanie swoich bieżących obowiązków pracowniczych, których w podmiocie takim, jak Szpital jest bardzo dużo, prace nad dokumentacją przeciągały się. Także z rożnych powodów absencji (okres urlopowy, zwolnienia lekarskie pracowników i osób decyzyjnych), wydłużał się czas prac nad dokumentacją, która jest stosunkowo obszerna i zawiera ponad czterdzieści załączników w postaci procedur, regulaminów, oraz wzorów dokumentów. Priorytetem Administratora było, aby wdrożyć dokumentację kompletną i opracowaną na wysokim poziomie (...). (akta kontroli str. 13, 26-58, 379-385)

2. Do 21 marca 2019 r. w Szpitalu nie założono i nie prowadzono ewidencji osób upoważnionych do przetwarzania danych osobowych, wymaganej PBODO (pkt 5.3.18). Dyrektor Szpitala wyjaśniła, że: *PBODO wraz z załącznikami wdrożono w Szpitalu 4 lutego 2019 r. Wraz z nią wprowadzono nowe upoważnienia do przetwarzania danych osobowych oraz oświadczenia o zachowaniu poufności. By sprawniej przeprowadzić proces upoważniania bardzo dużej liczby pracowników oraz odbiór oświadczeń, zaangażowano do ich zbierania kierowników komórek organizacyjnych Szpitala. Z rożnych uzasadnionych powodów nie wszystkie upoważnienia spłynęły na czas do Sekcji Służb Pracowniczych, w związku z czym uzupełnienie ewidencji na dzień kontroli nie było możliwe, a przekazana w niekompletnej formie nie wykazałaby wszystkich pracowników upoważnionych do przetwarzania danych. Ewidencja jest w trakcie uzupełniania przez IOD i dopracowana zostanie do końca marca br.*
(akta kontroli str. 78-81, 147, 171, 379-385)

OCENA CZĄSTKOWA

Szpital wywiązał się z obowiązku opracowania dokumentacji oraz procedur uwzględniających przepisy RODO. Jednak ich dostosowanie do nowych regulacji nastąpiło dopiero po ponad ośmiu miesiącach od wejścia w życie RODO, a do 25 marca 2019 r. w Szpitalu nie założono i nie prowadzono ewidencji osób upoważnionych do przetwarzania danych osobowych, wymaganej PBODO. Wywiązano się z obowiązku powołania IOD i zgłoszenia tego faktu Prezesowi Urzędu Ochrony Danych Osobowych. Przeprowadzono wymaganą analizę ryzyka procesów przetwarzania danych osobowych oraz opracowano rejestr czynności przetwarzania tych danych, zawierający wszystkie wymagane elementy. Pracowników Szpitala zapoznawano z regulacjami dotyczącymi ochrony danych osobowych i zagadnieniami dotyczącymi bezpieczeństwa danych.

2. Zapewnienie prawidłowego przetwarzania i ochrony danych osobowych

Opis stanu faktycznego

2.1. Oględziny funkcjonującej w Szpitalu rejestracji ogólnej wykazały, że właściwie i zgodnie z PBODO chroniono dane osobowe rejestrujących się pacjentów. Wszystkie trzy okna rejestracji zorganizowano w sposób uniemożliwiający wgląd w dokumenty osoby z sąsiedniego okienka. W obrębie wzroku rejestrujących się pacjentów nie stwierdzono dokumentów zawierających dane osobowe innych osób, a monitory komputerów znajdujące się w rejestracji były ustawione w sposób umożliwiający wgląd jedynie personelowi Szpitala. W pomieszczeniu rejestracji dokumentacja medyczna była przechowywana w zamykanych metalowych szafkach.

Pomiędzy oknami rejestracji nie zamontowano przesłon utrudniających podsłuchanie rozmowy prowadzonej na sąsiadującym stanowisku. Jednak osoby rejestrujące, zgodnie z PBODO, dbały o prowadzenie rozmów z pacjentami w sposób uniemożliwiający usłyszenie ich treści przez osoby nieuprawnione, w tym nie wypowiadały na głos informacji zawierających dane osobowe i identyfikowały pacjentów na podstawie dowodów tożsamości.

Pacjenci po dokonanej rejestracji otrzymywali numery określające kolejność wizyty w wybranej poradni wraz z planowaną godziną i datą wizyty.

Zapewniono odstęp pomiędzy osobami przy okienku a kolejnymi pacjentami w kolejce, poprzez wyznaczenie linii na podłodze. W trakcie oględzin kolejne osoby czekały na podejście do okienka za wyznaczoną linią. Przy każdym okienku znajdowała się również informacja, że może przebywać przy nim tylko jedna osoba.

W widocznym miejscu znajdowała się klauzula informacyjna, zgodna z załącznikiem do PBODO i spełniająca wymagania określone w art. 13 ust. 1 i 2 RODO.

(akta kontroli str. 81-83, 117-118, 270-272)

Również oględziny trzech (z ośmiu) oddziałów szpitalnych[15] wykazały, że prawidłowo chroniono tam dane osobowe pacjentów. Ustalono m.in., że:

- na łóżkach pacjentów dwóch oddziałów nie umieszczano kart pacjentów z danymi osobowymi, a na jednym oddziale karty pacjentów były zasłonięte,
- zgodnie z art. 36 ust. 3 i 5 ustawy z dnia 15 kwietnia 2011 r. o działalności leczniczej[16], na dwóch oddziałach pacjentów zaopatrzono w wydrukowane opaski identyfikacyjne zawierające kod kreskowy, inicjały pacjenta oraz numer z księgi głównej szpitala, a na trzecim oddziale (psychiatrycznym) pacjentów nie zaopatrzono w znaki identyfikacyjne, zgodnie z ust. 4 powołanego przepisu,
- we wszystkich trzech oddziałowych dyżurkach pielęgniarskich oraz w dwóch (z trzech) oddziałowych gabinetach lekarskich zamykanych na klucz, dokumentację medyczną przechowywano w szafkach z zamkami, a w jednym gabinecie lekarskim (również zamykanym na klucz i wyposażonym w szafki z zamkami) dokumentacja medyczna w trakcie oględzin znajdowała się w oddzielnych teczkach, ustawionych pionowo na półkach, co uniemożliwiało odczytanie ich treści,
- w trakcie oględzin w oddziałowych dyżurkach pielęgniarskich oraz w gabinetach lekarskich znajdował się personel medyczny, a w przypadku jego braku pomieszczenia te zostały zamknięte na klucz, którego nie pozostawiano w zamku,
- wszystkie nieużywane w trakcie oględzin komputery były wyłączone albo uruchomiony był na nich wygaszacz ekranu. (akta kontroli str. 270-272)

Oględziny trzech (z 16) gabinetów poradni specjalistycznych[17] funkcjonujących w Szpitalu wykazały natomiast, że:

- wywoływanie pacjentów wszystkich trzech poradni odbywało się w sposób gwarantujący anonimowość, tj. poprzez słowa *następny proszę,*
- pomieszczeń poradni nie pozostawiano bez nadzoru,
- w dwóch (z trzech) poradniach dokumentację medyczną przechowywano w sposób uniemożliwiający zapoznanie się z jej treścią przez osoby nieuprawnione, a w jednej poradni leżała ona na biurku przyjmującego lekarza, co szerzej opisano w dalszej części wystąpienia, w pkt 1 sekcji *Stwierdzone nieprawidłowości.* (akta kontroli str. 270-272)

Ponadto w ramach oględzin stwierdzono, że w skontrolowanych oddziałach szpitalnych, rejestracji ogólnej oraz w poradniach specjalistycznych nie funkcjonował monitoring wizyjny. Kamery monitoringu zamontowano natomiast wewnątrz budynku Szpitala, w ośmiu innych miejscach. Za ich pomocą monitorowano trzy wejścia do Szpitala, trzy korytarze, poczekalnię przy ogólnej izbie przyjęć Szpitala oraz wnętrze kabiny windy osobowej. Obraz z kamer wyświetlany był w sekretariacie Szpitala. W trakcie oględzin najstarszy utrwalony i przechowywany zapis pochodził sprzed dziewięciu dni. Zasady udostępniania danych z monitoringu opisano w regulaminie funkcjonowania monitoringu wizyjnego w Szpitalu, stanowiącym załącznik do PBODO.

Informacja o funkcjonującym w Szpitalu monitoringu (zawierająca m.in. dane administratora dane osobowe, kontakt do IOD oraz cele przetwarzania danych) znajdowała się na tablicy ogłoszeń oraz przy rejestracji ogólnej. W pobliżu każdej z ośmiu kamer znajdował się też piktogram informujący o monitorowaniu terenu. (akta kontroli str. 117-118, 270-272)

---

[15] Oddziały: Psychiatryczny, Pediatryczny oraz Wewnętrzny.

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

[17] Poradnie: Chirurgii ogólnej, Rehabilitacji leczniczej, Kardiologiczna.

2.2. Według stanu na 11 lutego 2019 r. personel komórek administracyjnych Szpitala liczył 61 osób, z których 13 miało dostęp do systemu informatycznego typu HIS. Osoby te posiadały upoważnienia do przetwarzania danych osobowych. Analiza uprawnień nadanych tym 13 osobom w systemie HIS wykazała, że odpowiadały one zakresom zadań i obowiązków realizowanych przez tych pracowników. Dostęp do systemu HIS możliwy był jedynie po autoryzacji pracownika z wykorzystaniem indywidualnego loginu i hasła.
(akta kontroli str. 273-274, 282-287, 293-294)

2.3. Analiza przeprowadzona na próbie 30 (ze 118) pielęgniarek i położnych zatrudnionych w Szpitalu na 11 lutego 2019 r. wykazała, że posiadały one upoważnienia do przetwarzania danych osobowych. W systemie HIS 26 (87%) osób posiadało dostęp do danych osobowych pacjentów jedynie z oddziałów szpitalnych, na których świadczyły pracę. Natomiast cztery (13%) osoby miały dostęp do danych pacjentów także z innych komórek organizacyjnych Szpitala, co szerzej opisano w dalszej części wystąpienia, w pkt 2 sekcji *Stwierdzone nieprawidłowości.* (akta kontroli str. 275-280, 295-310)

Natomiast analiza akt osobowych wszystkich pracowników zatrudnionych na stanowiskach opiekun medyczny (jedna osoba), kierowca (sześć osób), elektryk (jedna osoba) oraz pracownik gospodarczy (25 osób) wykazała, że osobom tym nie wydano upoważnień do przetwarzania danych osobowych, zgodnie z realizowanymi przez nich obowiązkami.
(akta kontroli str. 273-274, 311)

2.4. Od 25 maja 2018 r. do 11 lutego 2019 r. 34 osoby zaprzestały świadczyć pracę w Szpitalu, z których 18 miało przyznany w okresie zatrudnienia dostęp do systemów informatycznych Szpitala, w tym 17 do aplikacji HIS. Analiza uprawnień tych 18 osób wykazała, że na 26 lutego 2019 r. mieli oni zablokowaną możliwość pracy w programach informatycznych, a odnotowana w nich data ostatniego logowania nie była późniejsza, niż data zaprzestania świadczenia pracy w Szpitalu. (akta kontroli str. 281-292, 312-313)

2.5. Szpital, zgodnie z umową asysty technicznej, usterki i błędy w działaniu aplikacji HIS zgłaszał dostawcy oprogramowania poprzez stronę internetową. Od 25 maja 2018 r. do 12 marca 2019 r. dokonano 47 zgłoszeń. Analiza ich treści wykazała, że dostawcy oprogramowania wraz ze zgłoszeniem nie przekazywano danych osobowych pacjentów Szpitala, co było zgodne z zasadą minimalizacji danych, wyrażoną w art. 5 ust. 1 lit. c RODO. Tylko w jednym przypadku podano imiona i pierwszą literę nazwiska czterech pacjentów, co nie pozwalało jednak na jednoznaczną identyfikację tych osób.
(akta kontroli str. 314-329)

2.6. W okresie objętym kontrolą obowiązywały 42 umowy powierzenia danych osobowych. W 21 z nich Szpital był podmiotem przetwarzającym, a w pozostałych 21 administratorem danych (powierzającym przetwarzanie). Szpital umowami powierzył przetwarzanie danych osobowych wykonawcom realizującym na rzecz Szpitala m.in. obsługę prawną, usługi IOD, usługi inspektora ds. obrony cywilnej i zarządzania kryzysowego, serwisu oprogramowania oraz usługi informatyczne. Analiza treści pięciu (z 21) umów powierzenia przez Szpital przetwarzania danych osobowych innym podmiotom wykazała, że zawierały one wszystkie postanowienia wymagane art. 28 ust. 3 RODO. (akta kontroli str. 330-352)

2.7. Od 25 maja 2018 r. do 11 lutego 2019 r. w rejestrze naruszeń bezpieczeństwa ochrony danych osobowych Szpitala odnotowano dwa incydenty. Pierwszy związany był z pozostawieniem bez nadzoru otwartego pomieszczenia z niezabezpieczoną dokumentacją medyczną, a drugi dotyczył sfotografowania telefonem dokumentacji medycznej pacjentów pracowni fizjoterapii przez jej pracownika. Po przeprowadzeniu postępowań wyjaśniających, IOD ustalił okoliczności towarzyszące naruszeniom oraz podjął działania w celu minimalizacji skutków incydentów, w tym zabezpieczył otwarte pomieszczenie oraz pobrał wyjaśnienia od pracownika pracowni fizjoterapii, który wskazał, że: *natychmiast usunął zdjęcie z zasobów telefonu i nie udostępniał go osobom nieupoważnionym.*

Żaden z dwóch incydentów nie został zgłoszony do Prezesa Urzędu Ochrony Danych Osobowych. W rejestrze naruszeń bezpieczeństwa ochrony danych osobowych Szpitala IOD wskazał, że w żadnej sprawie nie doszło do naruszenia poufności danych przetwarzanych w Szpitalu. Dyrektor Szpitala wyjaśniła, że: *naruszenie z 25 września*

2018 r., polegające na pozostawieniu bez nadzoru otwartego pomieszczenia (...), nie doprowadziło do naruszenia poufności, dostępności, czy też integralności danych osobowych, które znajdowały się w tym obszarze. W poczekalni nie znajdowały się w czasie wystąpienia incydentu osoby postronne. Interwencja IOD była bardzo szybka, zabezpieczono dokumentację i pomieszczenie, pouczono pracowników. W związku z tym, że nie doszło do naruszenia bezpieczeństwa danych przetwarzanych wówczas w pomieszczeniu (...) podjęto decyzję o niezgłaszaniu incydentu do Prezesa Urzędu Ochrony Danych Osobowych. Naruszenie z 30 stycznia 2019 r., dotyczące utrwalenia na zdjęciu dokumentacji zawierającej dane osobowe (...) nie zostało zgłoszone do Prezesa Urzędu Ochrony Danych Osobowych, ponieważ na podstawie przeprowadzonego postępowania ustalono, iż dane zarejestrowane w telefonie komórkowym natychmiast zostały z niego usunięte i nie zostały upublicznione, przesłane lub udostępnione osobom trzecim. Pracownik złożył w tym temacie wyjaśnienie oraz oświadczenie, które dołączono do dokumentacji. Po konsultacji z IOD, podjęto decyzję, iż możliwość naruszenia bezpieczeństwa danych była na tyle mało prawdopodobna, że incydent nie kwalifikuje się do zgłoszenia do Prezesa Urzędu Ochrony Danych Osobowych.

(akta kontroli str. 353-354, 379-385)

2.8. Od 25 maja 2018 r. do 6 marca 2019 r. w Szpitalu rozpatrzono 881 wniosków o udostępnienie dokumentacji medycznej. W 879 przypadkach Szpital wydał dokumentację medyczną, w tym w 752 sprawach pacjentowi, w 124 przypadkach – podmiotom lub osobom innym niż pacjent, a w trzech sprawach – firmom ubezpieczeniowym. W dwóch przypadkach odmówiono wydania informacji z dokumentacji medycznej, przy czym w jednej sprawie nie podano danych osoby upoważnionej do dokumentacji medycznej pacjenta, a w drugim przypadku nie zezwolono uczelni wyższej na wgląd do księgi bloku operacyjnego z lat 2000–2018 z powodu braku możliwości jej zanonimizowania.

Analiza prawidłowości udostępnienia dokumentacji medycznej firmom ubezpieczeniowym (trzy sprawy) oraz osobom fizycznym innym niż pacjent (30 spraw) wykazała, że dokumentację udostępniono wyłącznie upoważnionym podmiotom (osobom) lub przedstawicielowi ustawowemu, zgodnie z PBODO oraz art. 26 ust. 1 ustawy z dnia 6 listopada 2008 r. o prawach pacjenta i Rzeczniku Praw Pacjenta[18].

(akta kontroli str. 128-134, 355-356)

2.9. Regulacje dotyczące ochrony danych przed ich utratą w wyniku awarii, błędów lub nieuprawnionej modyfikacji zostały opisane w PBODO oraz w Planie ciągłości działania, sporządzonym w wyniku analizy ryzyka przetwarzania danych osobowych, opisanej w pkt 1.4 wystąpienia pokontrolnego. W dokumentach tych określono m.in.: [1] zasady korzystania z portali internetowych oraz poczty elektronicznej; [2] zasady zarządzania oprogramowaniem komputerowym; [3] zasady sporządzania i zarządzania kopiami zapasowymi baz danych; [4] stosowane metody i środki uwierzytelniania w systemach informatycznych; [5] zasady pracy Szpitala w przypadku awarii systemów informatycznych lub zasilania elektrycznego; [6] zasady aktualizacji i konserwacji oprogramowania systemowego; [7] ewidencjonowanie wykorzystywanego oprogramowania.

(akta kontroli str. 58-170, 202-204)

Oględziny jedynej serwerowni Szpitala wykazały, że dostęp do tego pomieszczenia, znajdującego się na pierwszym piętrze, zabezpieczono, stosując antywłamaniowe drzwi przeciwpożarowe. W korytarzu przed serwerownią oraz w pomieszczeniu naprzeciwko serwerowni umieszczono gaśnice. Serwerownię wyposażono w dwa układy podtrzymywania napięcia UPS, alarm z czujnikiem ruchu, czujniki dymu, otwarcia drzwi i temperatury oraz w klimatyzację. Wszystkie urządzenia informatyczne zamontowano w specjalnie do tego przystosowanych szafach, które stały na podłodze technicznej powyżej powierzchni posadzki pomieszczenia.

W trakcie oględzin serwerowni ustalono, że kopie zapasowe baz danych systemów informatycznych Szpitala były wykonywane zgodnie z harmonogramem przewidzianym w PBODO. Były one jednak przechowywane jedynie na macierzach dyskowych

[18] Dz. U. z 2017 r. poz. 1318, ze zm. Ustawa zwana dalej: *ustawą o prawach pacjenta.*

w serwerowni, co szerzej opisano w dalszej części wystąpienia, w pkt 3 sekcji *Stwierdzone nieprawidłowości.* (akta kontroli str. 160, 357-359)

Zgodnie z Planem ciągłości działania, Szpital wyposażono w agregat prądotwórczy o odpowiedniej mocy, który posiadał funkcję autostartu. (akta kontroli str. 202-204, 357-359)

W trakcie oględzin 30 komputerów (po 10 użytkowanych przez pielęgniarki, lekarzy oraz pracowników administracyjnych), służących do przetwarzania danych osobowych stwierdzono, że Szpital wprowadził rozwiązania minimalizujące ryzyko utraty lub nieuprawnionej modyfikacji danych osobowych za pośrednictwem tych urządzeń. We wszystkich 30 przypadkach dostęp do poszczególnych systemów informatycznych możliwy był po wprowadzeniu indywidualnego loginu i hasła użytkownika. Nie stwierdzono przypadków wykorzystywania tych samych danych autoryzacyjnych (loginu i hasła) przez kilku użytkowników. We wszystkich przypadkach hasła posiadały liczbę znaków nie mniejszą niż wymagana PBODO. Na wszystkich komputerach objętych oględzinami uniemożliwiono ich użytkownikom instalowanie oprogramowania, a program antywirusowy posiadał aktualną bazę sygnatur wirusów. W przypadku wszystkich 20 komputerów użytkowanych przez pielęgniarki lub lekarzy oraz w przypadku trzech (z 10) komputerów użytkowanych przez pracowników administracyjnych, zgodnie z PBODO, dostęp do Internetu ograniczono do wybranych stron internetowych.

(akta kontroli str. 88-93, 360-378)

Dyrektor Szpitala wyjaśniła, że: *w Szpitalu wykorzystywany jest jeden komputer przenośny, a pamięci przenośnych na chwilę obecną Szpital nie posiada i nie wykorzystuje. Wspomniany komputer przenośny nie posiada ochrony kryptograficznej nośników pamięci (dysków twardych), służy on do przetwarzania danych osobowych, jednakże jest on użytkowany, jak komputer stacjonarny, tzn. stoi zawsze w jednym miejscu na biurku w jednym z pomieszczeń biurowych administracji szpitala zamykanym na klucz, użytkowany jest przez jednego użytkownika, podłączony jest do stacjonarnych urządzeń peryferyjnych (tj. zewnętrzna klawiatura, mysz, dodatkowy monitor, sieć lan), nie jest przenoszony, a co za tym idzie nie jest użytkowany poza budynkiem Szpitala.* Z wyjaśnień Dyrektor Szpitala wynika też, że w Szpitalu poza opaskami identyfikacyjnymi pacjentów nie stosuje się innych metod pseudonimizacji danych osobowych. (akta kontroli str. 379-385)

Stwierdzone nieprawidłowości

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

1. W trakcie przeprowadzanych 19 lutego 2019 r. oględzin poradni rehabilitacji leczniczej dokumentacja medyczna pacjentów przyjętych i oczekujących na wizytę znajdowała się na biurku lekarza przyjmującego, co umożliwiało odczytanie danych osobowych pacjentów (imię, nazwisko, pesel, adres zamieszkania) przez osoby nieuprawnione. Takie postępowanie mogło łamać prawa pacjentów określone w art. 13 ustawy o prawach pacjenta oraz naruszało postanowienia PBODO (pkt 5.5.2), zgodnie z którą do obowiązków osób upoważnionych do przetwarzania danych osobowych należy zakrywanie dokumentów w taki sposób, aby osoby obsługiwane nie mogły zapoznać się z ich treścią oraz bieżąca praca wyłącznie z dokumentami niezbędnymi do wykonania aktualnego zadania. Dyrektor Szpitala wyjaśniła, że: *niezabezpieczenie przez lekarza dokumentacji zawierającej dane dotyczące zdrowia w gabinecie poradni rehabilitacyjnej, było incydentem, który na co dzień się nie zdarza, co potwierdzają pracownicy poradni. Lekarz, który w dniu kontroli pracował w poradni, zwykle rygorystycznie przestrzega zasad ochrony danych osobowych zawartych w dokumentacji medycznej, nad którą pracuje. Został on pouczony przez IOD o przestrzeganiu zasady czystego biurka, zawartej w PBODO i przyjął uwagi do wiadomości.*

   (akta kontroli str. 81-83, 270-272, 379-385)

2. Cztery (z 30 analizowanych) osoby 26 lutego 2019 r. posiadały dostęp w systemie informatycznym HIS do danych osobowych pacjentów z innych komórek organizacyjnych Szpitala niż komórka, w której wykonywały zadania. Było to sprzeczne z PBODO (pkt 5.2.1), w której założono, że osoby upoważnione, realizując powierzone im zadania, zbierają i przetwarzają dane osobowe wyłącznie w ilości i w zakresie niezbędnym do osiągnięcia celu przetwarzania, jakim jest realizowane zadanie.

Naruszało to również przepis § 20 ust. 2 pkt 4 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[19]. Zgodnie z tym przepisem kierownictwo podmiotu publicznego jest obowiązane do podejmowania działań zapewniających, że osoby zaangażowane w proces przetwarzania informacji posiadają stosowne uprawnienia i uczestniczą w tym procesie w stopniu adekwatnym do realizowanych przez nie zadań oraz obowiązków, mających na celu zapewnienie bezpieczeństwa informacji. Dyrektor Szpitala wyjaśniła, że: *ww. osobom podczas wdrożenia systemu omyłkowo zostały nadane uprawnienia w sposób szerszy niż to jest konieczne do realizowanych obowiązków. Po ujawnieniu ww. sytuacji uprawnienia natychmiast zostały skorygowane tym osobom jak również uprawnienia pozostałych pracowników zostaną poddawane okresowym sprawdzeniom przez bezpośrednich przełożonych aby zapobiec występowaniu takiej sytuacji w przyszłości.*

(akta kontroli str. 77-78, 295-310, 379-385)

3. Kopie zapasowe baz danych systemów informatycznych Szpitala były przechowywane w tym samym pomieszczeniu, w którym przechowywano dane produkcyjne i nie były przesyłane na macierze dyskowe Urzędu Marszałkowskiego Województwa Podlaskiego w Białymstoku. Było to sprzeczne z procedurą tworzenia kopii zapasowych systemów informatycznych Szpitala (załącznik nr 6.7.1 PBODO) i § 20 ust. 2 pkt 12 lit. b rozporządzenia KRI. Stwarzało też ryzyko utraty wszystkich danych w przypadku poważnych zdarzeń takich, jak pożar czy włamanie. Dyrektor Szpitala wyjaśniła, że: *podczas wdrożenia projektu „Podlaski System Informacyjny e-Zdrowie", w którym szpital uczestniczy (jest partnerem projektu), wykonawca wdrożenia systemów kopii zapasowych biorąc pod uwagę ograniczenia sprzętowe (brak bibliotek taśmowych w podmiotach leczniczych biorących udział w projekcie) w kluczowych założeniach tego systemu określił, że oprócz kopii tworzonych na lokalne macierze danych znajdujące się w podmiotach leczniczych będzie wykonywana raz w tygodniu replikacja kopii zapasowych do Platformy Regionalnej za pomocą łączy WAN wybudowanych w ramach projektu. Szpital nie miał powodów aby myśleć, że jest inaczej. Dopiero w odpowiedzi na zapytanie złożone w związku z pojawiającymi się wątpliwościami do wykonawcy z dnia 18 lutego 2019 r. otrzymaliśmy informację, że „Kopie zapasowe nie są przesyłane do platformy regionalnej" oraz, że w dokumentacji przetargowej nie było takiego wymogu. Wymogu takiego faktycznie nie było, ale kluczowe założenie przez samego wykonawcę już tak. O fakcie, że wykonawca od tego odszedł nikt Szpitala oficjalnie nie poinformował. W związku z zaistniałą sytuacją oraz brakiem możliwości uruchomienia replikacji do Platformy Regionalnej ze względu na zbyt małą przepustowość łącza WAN, Szpital podjął działania w celu zwiększenia bezpieczeństwa przetwarzanych danych i w tym celu projektowane jest rozwiązanie polegające na zakupie dedykowanej pamięci sieciowej (NAS), która umieszczona zostanie poza pomieszczeniem głównej serwerowni szpitala (planowane pomieszczenie po starej serwerowni zabezpieczone drzwiami przeciwwłamaniowymi, UPS oraz klimatyzacją), a na którą to będą przeprowadzane repliki kopii zapasowych. Szpital dołoży wszelkich starań aby projektowane rozwiązanie wdrożyć jak najszybciej.*

(akta kontroli str. 160, 270-272, 379-385)

OCENA CZĄSTKOWA

W Szpitalu wdrożono rozwiązania organizacyjne i techniczne zmierzające do zapewnienia prawidłowej ochrony i przetwarzania danych osobowych. Nie były one jednak w pełni przestrzegane. Prawidłowo chroniono i przetwarzano dane osobowe w skontrolowanych trzech oddziałach szpitalnych, w dwóch (z trzech) poradniach specjalistycznych oraz w rejestracji ogólnej do poradni specjalistycznych. Personel administracyjny Szpitala oraz 87% objętych analizą pielęgniarek i położnych przetwarzało dane osobowe w systemie HIS adekwatnie do realizowanych zadań i obowiązków, a wszystkim byłym pracownikom Szpitala zablokowano do dostęp do takich danych. We wszystkich 33 skontrolowanych sprawach dokumentację medyczną udostępniono uprawnionym podmiotom, a pięć analizowanych umów powierzenia przetwarzania danych osobowych spełniało wymagania

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

określone w art. 28 RODO. W sposób właściwy zastosowano fizyczne zabezpieczenia serwerowni Szpitala, w której przechowywano dane osobowe przetwarzane w formie elektronicznej oraz zminimalizowano ryzyko ich utraty lub nieuprawnionej modyfikacji za pośrednictwem wszystkich 30 objętych kontrolą komputerów. Stwierdzono jednak cztery przypadki nadania pracownikom uprawnień w systemach informatycznych Szpitala w zakresie większym od realizowanych przez nich zadań i obowiązków, a personel jednej poradni specjalistycznej Szpitala nie przestrzegał przyjętych regulacji wewnętrznych dotyczących sposobu zabezpieczania papierowej dokumentacji medycznej. Z kolei kopie zapasowe baz danych systemów informatycznych Szpitala przechowywano w jednym pomieszczeniu z danymi produkcyjnymi.

IV. Wnioski

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

Wnioski

1. Uaktualnianie w razie potrzeby polityk ochrony danych osobowych Szpitala, zgodnie z art. 24 ust. 1 i 2 RODO.
2. Ewidencjonowanie osób upoważnionych do przetwarzania danych osobowych, zgodnie z PBODO.
3. Egzekwowanie od personelu Szpitala przestrzegania zasad określonych w PBODO, dotyczących zabezpieczania papierowej dokumentacji medycznej.
4. Nadawanie pracownikom uprawnień w systemach informatycznych Szpitala w stopniu adekwatnym do realizowanych przez nich zadań oraz obowiązków, stosownie do PBODO oraz § 20 ust. 2 pkt 4 rozporządzenia KRI.
5. Przechowywanie kopii zapasowych elektronicznych baz danych Szpitala w innym pomieszczeniu niż to, w którym przechowuje się dane produkcyjne.

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 Białymstoku. 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 od otrzymania wystąpienia pokontrolnego, o sposobie wykonania wniosków pokontrolnych oraz o podjętych działaniach lub przyczynach niepodjęcia tych działań.

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

Białystok, 1 kwietnia 2019 r.

Kontroler:

Marcin Kiersnowski
Specjalista kontroli państwowej

M. Kiersnowski
.....
podpis

p.o. DYREKTORA DELEGATURY
Najwyższej Izby Kontroli w Białymstoku
z up. WICEDYREKTOR
Robert Skwarko

.....
podpis