NAJWYŻSZA IZBA KONTROLI
Delegatura w Białymstoku

LBI.410.002.03.2018

00069619

Pani Barbara Łapińska
Dyrektor
Specjalistycznego Psychiatrycznego Samodzielnego
Publicznego Zakładu Opieki Zdrowotnej
w Suwałkach
ul. Szpitalna 62, 16-400 Suwałki

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	Specjalistyczny Psychiatryczny Samodzielny Publiczny Zakład Opieki Zdrowotnej w Suwałkach (dalej: „Szpital" lub „ZOZ"), ul. Szpitalna 62, 16-400 Suwałki
Kierownik jednostki kontrolowanej	Barbara Łapińska, dyrektor od 1 lutego 2009 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. (data wejścia w przepisów RODO) do dnia zakończenia czynności kontrolnych. Badania kontrolne mogły dotyczyć 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[1]
Jednostka przeprowadzająca kontrolę	Najwyższa Izba Kontroli Delegatura w Białymstoku
Kontroler	Piotr Jurkin, specjalista kontroli państwowej, upoważnienie do kontroli nr LBI/17/2019 z 18 stycznia 2018 r. (akta kontroli str. 1-2)

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

II. Ocena ogólna[2] kontrolowanej działalności

OCENA OGÓLNA

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

Uzasadnienie oceny ogólnej

ZOZ wprowadził rozwiązania organizacyjne i techniczne zmierzające do zapewnienia prawidłowej ochrony i przetwarzania danych osobowych. Szpital zaktualizował dokumentację i procedury dotyczące ochrony danych osobowych przed wejściem w życie przepisów RODO[3]. Wywiązał się z obowiązku powołania Inspektora Ochrony Danych Osobowych (dalej: „IOD") i zgłoszenia tego faktu Prezesowi Urzędu Ochrony Danych Osobowych (dalej: „PUODO"). Przeprowadził także wymaganą analizę ryzyka procesów przetwarzania tych danych. Prawidłowo chroniono i przetwarzano dane osobowe pacjentów w procesie rejestracji i udzielania świadczeń w objętych oględzinami poradniach specjalistycznych oraz w Izbie Przyjęć. Właściwie udostępniano również dokumentację medyczną upoważnionym podmiotom i osobom fizycznym. Personel administracyjny oraz objęte analizą 30 pielęgniarek posiadało uprawnienia w systemie HIS[4] adekwatne do wykonywanych zadań. Wprowadzono odpowiednie zabezpieczenia fizyczne serwerowni Szpitala i pomieszczenia pracy informatyka, w których przechowywano dane osobowe przetwarzane w formie elektronicznej.

Stwierdzono jednak nieprawidłowości, które polegały m.in. na:

- przekazaniu – z naruszeniem art. 5 pkt. 1 lit. c RODO – podmiotowi świadczącemu usługi serwisowe danych osobowych pacjenta,
- nadaniu trzem (z 30 analizowanych) pracownikom uprawnień w systemie operacyjnym komputerów w zakresie nieadekwatnym do realizowanych przez nich zadań i obowiązków,
- nieprowadzeniu rejestru przetwarzania danych osobowych, wbrew wymogom art. 30 RODO,
- niezapewnieniu całemu personelowi Szpitala szkoleń związanych z wejściem w życie RODO oraz zagadnieniami dotyczącymi ochrony i bezpieczeństwa danych osobowych,
- nieprzestrzeganiu przyjętych regulacji wewnętrznych dotyczących sposobu zabezpieczania papierowej dokumentacji medycznej, na trzech objętych oględzinami oddziałach i w trzech gabinetach lekarskich,
- nieujęciu w jednej z trzech analizowanych umów powierzenia przetwarzania danych osobowych wszystkich elementów wymaganych art. 28 RODO,
- nieprowadzeniu rejestru identyfikatorów przyznanych użytkownikom poszczególnych komputerów oraz niewykonywaniu kwartalnych kontroli antywirusowych, mimo takiego wymogu wynikającego z Polityki Bezpieczeństwa Ochrony Danych Osobowych (dalej: „PBODO"),
- nadaniu dwóm pracownikom (z 30 analizowanych) uprawnień w systemie HIS Szpitala, przed udzieleniem im upoważnienia do przeważania danych osobowych,
- udzieleniu jednej osobie dostępu do systemu HIS bez upoważnienia jej do przetwarzania danych osobowych, a kolejnej – bez wymaganej przepisami PBODO, akceptacji IOD,
- odebraniu uprawnień 15 pracownikom posiadającym dostęp do systemów informatycznych Szpitala (z 26 analizowanych) od dziewięciu do 227 dni od momentu zaprzestania przez te osoby świadczenia pracy.

---

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

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

[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.

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

OBSZAR

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

Opis stanu faktycznego

1.1. W dniu 5 kwietnia 2018 r., zarządzeniem Nr 5/2018, powołano IOD, a zarządzeniem Nr 29A/2018 z 2 listopada 2018 r. powołano następną osobę na to stanowisko. Stosownie do art. 8 i art. 10 ustawy z dnia 10 maja 2018 r. o ochronie danych osobowych[6] (dalej: „u.o.d.o."), Szpital w ustalonym terminie (9 listopada 2018 r.) zawiadomił PUODO o odwołaniu i wyznaczeniu nowego IOD. Przekazane zawiadomienia zawierały wszystkie elementy określone art. 10 ust. 3 ustawy o ochronie danych osobowych.

W § 29 A regulaminu organizacyjnego określono zakres zadań przypisanych dla IOD. Do dnia rozpoczęcia niniejszej kontroli Szpital nie opublikował danych dotyczących IOD oraz informacji o sposobie i formie kontaktu w sposób ustalony w art. 37 ust. 7 RODO, co szerzej opisano w dalszej części wystąpienia, w sekcji „Stwierdzone nieprawidłowości". (akta kontroli str. 4-19, 30-31)

IOD umożliwiono wykonywanie obowiązków w sposób niezależny, stosownie do art. 38 ust. 3 RODO. W załączniku nr 1 do aneksu Nr 14/2018 z dnia 29 maja 2018 r. do zarządzenia nr 33/2012 Dyrektora Szpitala z dnia 26 listopada 2016 r., wprowadzającego regulamin organizacyjny Szpitala, wskazano IOD jako samodzielne stanowisko pracy, podlegające bezpośrednio Dyrektorowi placówki. Osoba pełniąca funkcję IOD, oprócz realizowania zadań przypisanych temu stanowisku, wykonywała również obowiązki przypisane do stanowiska ds. administracyjnych[7]. Rozdzielono tym samym zadania związane z pełnieniem funkcji IOD i przypisane do stanowiska ds. administracyjnych. (akta kontroli str. 4-5, 13-19)

Najwyższa Izba Kontroli zwraca uwagę, że osoba pełniąca obowiązki IOD nie w pełni posiadała należyte przygotowanie i kwalifikacje do pełnienia swojej funkcji. Nie zajmowała bowiem wcześniej stanowiska Administratora Bezpieczeństwa Informacji (dalej: „ABI") i odbyła jedynie dwa jednodniowe szkolenia na temat: prawnych aspektów legalnego przetwarzania danych osobowych w administracji publicznej (31 maja 2016 r.) oraz dokumentacji ochrony danych i obowiązków IOD w świetle RODO (7 grudnia 2018 r.). RODO i u.o.d.o. nie wskazują jednak konkretnych wymogów, jakie powinien spełnić IOD. Dyrektor Szpitala wyjaśniła, że: „Poprzedni pracownik pełniący funkcję IOD rozwiązał umowę o pracę praktycznie z dnia na dzień, a w związku z tym pilnie potrzebowałam osoby na to stanowisko". (akta kontroli str. 20-21, 28-31)

Do dnia zakończeni kontroli Szpital nie został uznany za operatora usługi kluczowej[8], o którym mowa w art. 5 ust 1. ustawy z dnia 5 lipca 2018 r. o krajowym systemie cyberbezpieczeństwa[9]. Szpital nie otrzymał zawiadomienia o wszczęciu wobec niego postępowania administracyjnego w sprawie uznania go za świadczącego usługę kluczową. (akta kontroli str. 4-5, 30-31)

1.2. Przed wejściem w życie RODO w Szpitalu funkcjonowały Polityka Bezpieczeństwa oraz Instrukcja Zarządzania Systemem Informatycznym Służącym do Przetwarzania Danych Osobowych wprowadzone zarządzeniem Dyrektora nr 4/2016 z 13 maja 2016 r. W dokumentach tych opisano m.in.: ogólne zasady przetwarzania danych osobowych, sposób archiwizacji i tworzenia kopii zapasowych zbiorów danych w systemie

---

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

[6] Dz. U. poz. 1000.

[7] Podziału czasu pracy dokonano odpowiednio w stosunku ½ do ½. Według wytycznych Grupy Roboczej Art. 29 ds. Ochrony Danych, zawartych w dokumencie: „Wytyczne dotyczące inspektorów ochrony danych ('DPO')", IOD nie może zajmować w organizacji stanowiska pociągającego za sobą określanie sposobów i celów przetwarzania danych. Ze względu na indywidualny charakter każdej organizacji ten aspekt powinien być analizowany osobno dla każdego podmiotu. Wytyczne dostępne na stronie internetowej https://www.giodo.gov.pl/pl/1520344/10390.

[8] Usługa kluczowa to taka, która ma kluczowe znaczenie dla utrzymania krytycznej działalności społecznej lub gospodarczej, wymieniona w wykazie usług kluczowych.

[9] Dz. U. poz. 1560.

informatycznym, zasady: [1] przetwarzania danych osobowych znajdujących się na nośnikach papierowych, [2] korzystania z poczty elektronicznej, [3] dostępu do Internetu, [4] rozpoczęcia, zawieszenia i zakończenia pracy przeznaczone dla użytkowników systemu, a także szczegółowe wytyczne w zakresie nadawania i odbierania uprawnień do przetwarzania danych oraz metody i procedury związane z zarządzaniem użytkownikiem. (akta kontroli str. 4-5)

W związku z wejściem w życie RODO, zarządzeniem nr 7/2018 Dyrektora z 17 maja 2018 r., wprowadzono zaktualizowaną PBODO oraz Instrukcję Zarzadzania Systemem Informatycznym (dalej: „IZSI") służącym do przetwarzania danych osobowych[10]. W PBODO zmiany polegały m.in. na: [1] doprecyzowaniu zasad zgłaszania naruszenia ochrony danych osobowych organowi nadzorczemu, [2] utworzeniu rejestru czynności przetwarzania, [3] określeniu zadań IOD, [4] stosowaniu domyślnej ochrony. Pozostawiono też załączniki, które wymagane były w poprzednim stanie prawnym[11] (opis struktury zbiorów danych wskazujących zawartość poszczególnych pól informacyjnych i powiązań między nimi oraz sposobu przepływu danych pomiędzy poszczególnymi systemami). W IZSI dostosowano zapisy do obowiązującego stanu prawnego. Określono w niej bowiem obowiązki IOD i usunięto zapisy dotyczące ABI oraz doprecyzowano, że dane osobowe przetwarzane w systemie informatycznym automatycznie odnotowują (po zatwierdzeniu wprowadzenia danych przez użytkownika operacji) datę pierwszego wprowadzenia danych do systemu oraz identyfikator osoby wprowadzającej dane. Postanowienia obu dokumentów obejmowały ochronę danych osobowych pracowników i pacjentów Szpitala oraz określały zasady zapewnienie bezpieczeństwa danych przetwarzanych w formie papierowej i w systemach elektronicznych.

Elementami Systemu Zarządzania Jakością, funkcjonującego w Szpitalu, były m.in. procedury: gromadzenia danych i obiegu historii choroby, a także archiwizowania dokumentacji medycznej[12], w której ujęto zapisy odnoszące się do prawa do ograniczenia przetwarzania i sprostowania danych, prawa do sprzeciwu oraz obowiązku powiadomienia o sprostowaniu lub usunięciu danych osobowych albo o ograniczeniu przetwarzania. Funkcjonowała też procedura udostępniania dokumentacji medycznej, opisująca sposób jej udostępniania wraz z określeniem organów mających do niej dostęp.
(akta kontroli str. 4-5, 32-100)

Powyższe dokumenty (PBODO oraz IZSI) zostały w całości (łącznie ze szczegółowymi informacjami dotyczącymi m.in. liczby znaków do haseł dostępowych dla użytkowników systemów informatycznych i administratora systemu oraz częstotliwość ich zmian) opublikowane w intranecie Szpitala, w zakładce „Ochrona danych osobowych" i były dostępne dla wszystkich pracowników placówki, posiadających dostęp do systemu informatycznego Szpitala, co szerzej opisano w dalszej części wystąpienia, w sekcji „Stwierdzone nieprawidłowości". (akta kontroli str. 30-31)

W dokumentach podstawowych (PBODO oraz IZSI) nie ustalono konieczności opracowania dodatkowych reguł i procedur uszczegóławiających te dokumenty. (akta kontroli str. 4-5)

1.3. Do dnia rozpoczęcia kontroli w Szpitalu IOD prowadziła: ewidencję osób upoważnionych do przetwarzania danych osobowych oraz wykaz budynków, pomieszczeń lub ich części tworzących obszar, w którym przetwarzane są dane osobowe niezgodnie z wzorami określonymi w zał. nr 1 i 8 do PBODO. Nie prowadzono natomiast: [1] rejestru czynności przetwarzania danych osobowych, [2] wykazu zbiorów danych osobowych wraz ze wskazaniem programów zastosowanych do przetwarzania tych danych, [3] opisu struktury zbiorów danych osobowych wskazujących zawartość poszczególnych pół informacyjnych i powiązania między nimi oraz sposobu przepływu danych pomiędzy poszczególnymi systemami, tj. dokumentów wymaganych przepisami RODO i PBODO, co szerzej opisano w dalszej części wystąpienia, w sekcji „Stwierdzone nieprawidłowości". W trakcie kontroli dokumenty te, poza rejestrem czynności przetwarzania oraz opisem struktury zbiorów danych osobowych wskazujących zawartość poszczególnych pól

[10] Z datą obowiązywania od 25 maja 2018 r.
[11] Ustawa z dnia 29 sierpnia 1997 r. o ochronie danych osobowych (Dz. U. z 2016 r. poz. 922, ze zm.) utraciła moc 25 maja 2018 r.
[12] Zapisy dotyczyły dokumentacji medycznej oraz pracowniczej.

informacyjnych i powiązania między nimi oraz sposobu przepływu danych pomiędzy poszczególnymi systemami, zostały założone lub zaktualizowane.

(akta kontroli str. 30-77, 271-274)

1.4. Stosownie do art. 32 RODO, 24 kwietnia 2018 r., ASI przeprowadził analizę procesów przetwarzania danych osobowych w poszczególnych systemach informatycznych Szpitala dla 17 ryzyk w odniesieniu do 46 potencjalnych sytuacji ich wystąpienia, przypisując im wartość oszacowanego ryzyka: [1] utrata zasilania – 2 pkt, [2] awaria sprzętu – 2 pkt, [3] błąd / luka systemu operacyjnego – od 3 do 4 pkt, [4] nieautoryzowana zmiana konfiguracji – od 3 do 4 pkt, [5] nieautoryzowany dostęp do systemu operacyjnego – od 3 do 4 pkt, [6] awaria sprzętu – 2 pkt, [7] utrata danych – od 1 do 2 pkt, [8] nieautoryzowana zmiana danych – 1 pkt, [9] nieczytelność zapisów – 1 pkt, [10] utrata nośnika – 1 pkt, [11] błędne wprowadzenie danych medycznych – od 2 do 3 pkt, [12] błędne wprowadzenie danych osobowych – od 1 do 2 pkt, [13] błąd czynności administracyjnych – 2 pkt, [14] kradzież danych – 1 pkt, [15] ujawnienie danych osobowych lub medycznych – 1 pkt, [16] nieautoryzowany dostęp – 1 pkt, [17] przeniesienie kodu złośliwego w wiadomościach – 1 pkt. Poziomy istotności ryzyka określono na: 1 pkt – pomijalny, 2 pkt – niski, od 3 do 6 pkt – średni, od 7 do 8 pkt – wysoki, od 9 do 10 pkt – krytyczny. Za największe ryzyko uznano: nieautoryzowany dostęp do systemu operacyjnego oraz nieautoryzowaną zmianę konfiguracji. Proponowane środki zaradcze polegały na okresowych przeglądach kont lokalnych w zakresie dostępu i posiadanych uprawnień do systemu przez poszczególnych pracowników. ASI wyjaśnił, że w związku z dużą ilością innych obowiązków, taki przegląd od końca maja 2018 roku do dnia rozpoczęcia kontroli NIK miał miejsce raz – 9 stycznia 2019 r. Dodał, że: „W tym dniu dokonałem przeglądu uprawnień dla prawie połowy zatrudnionych w tym czasie pracowników posiadających dostęp do systemów informatycznych Szpitala". Zagadnienie to omówiono szerzej w pkt. 2.4 niniejszego wystąpienia. Proponowane reakcje / działania na pozostałe zidentyfikowane ryzyka dotyczyły m.in.: wybiórczego / okresowego przeglądu konfiguracji sprzętu, stanu instalacji uaktualnień, kontroli i ograniczenia dostępu do miejsc przechowywania danych archiwalnych, szkoleń wewnętrznych.

ASI nie potrafił sprecyzować, na jakiej podstawie i z wykorzystaniem, jakich metod, została ustalona lista procesów / ryzyk związanych z przetwarzaniem danych osobowych w systemach informatycznych. Wyjaśnił, że: „Przygotowując analizę opierałem się jedynie na własnym doświadczeniu i wiedzy z pracy w Szpitalu. Nie posiłkowałem się żadnymi procedurami / dokumentami". (akta kontroli str. 22-23, 101-106, 281-282)

1.5. W ZOZ nie została wykonana ocena skutków dla ochrony danych osobowych, 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[13] zdecydowanie zalecała dokonanie DPIA[14] dla operacji przetwarzania trwających także przed 25 maja 2018 r.[15] oraz w przypadkach, gdy nie jest jasne, czy wymagana jest DPIA, gdyż jest ona „przydatnym narzędziem, które może pomóc administratorom danych w zapewnieniu zgodności z prawem ochrony danych". (akta kontroli str. 4-5, 22-23)

1.6. Jednym z zadań IOD, w myśl art. 39 ust. 1 lit. b RODO, jest prowadzenie szkoleń personelu uczestniczącego w operacjach przetwarzania danych. W dniach 27 marca i 26 kwietnia 2018[16] r. w Szpitalu przeprowadzono szkolenia: „Wprowadzenia przepisów wynikających z RODO oraz ochrony danych osobowych"[17]. Uczestniczyło w nich odpowiednio 17% i 10,7% pracowników, co szerzej opisano w dalszej części wystąpienia,

---

[13] Grupa Robocza została powołana na mocy art. 29 dyrektywy 95/46/WE. Była ona niezależnym organem doradczym w zakresie ochrony danych i prywatności.

[14] Ocena skutków planowanych operacji dla przetwarzania danych osobowych.

[15] Dokument pt.: Wytyczne dotyczące oceny skutków dla ochrony danych (DPIA) oraz ustalenia, czy przetwarzanie „z dużym prawdopodobieństwem może powodować wysokie ryzyko", do celów rozporządzenia 2016/679 https://www.giodo.gov.pl/1520281/id_art/9957/j/pl

[16] Prowadzącym szkolenie w dniu 26 kwietnia 2018 r. był m.in. pracownik Szpitala, pełniący funkcję IOD.

[17] Zajęcia miały miejsce w budynku Szpitala.

w sekcji „Stwierdzone nieprawidłowości". Dyrektor Szpitala wyjaśniła, że: „W szkoleniach tych uczestniczyli głównie kierownicy poszczególnych komórek organizacyjnych Szpitala. Omawiano na nich również projekty przepisów wewnętrznych przygotowywanych w związku z wprowadzeniem RODO, które zostały przyjęte zarządzeniem nr 7/2018 z 17 maja 2018 r. Kierownicy komórek organizacyjnych mieli obowiązek po zakończeniu szkoleń zapoznać pracowników im podległych z zagadnieniami poruszanymi w czasie ich trwania".

Zgodnie z § 5 pkt 3 PBODO, IOD zobowiązano do odbierania od pracownika m.in. oświadczenia o przeszkoleniu w zakresie danych osobowych i znajomości przepisów wprowadzonych zarządzeniem nr 7/2018 z 17 maja 2018 r. Spośród 60 objętych analizą pracowników ZOZ, 13 nie złożyło przedmiotowych oświadczeń. Nie uczestniczyli oni w szkoleniach przeprowadzonych 27 marca i 26 kwietnia 2018 r. Po wejściu w życie przepisów RODO żaden z pracowników Szpitala nie został objęty szkoleniem z tego zakresu. (akta kontroli str. 20-21, 107-116, 129-134)

1.7. Szpital nie stosował kodeksu dobrych praktyk w zakresie ochrony danych osobowych, czy medycznych, ale brał udział w tworzeniu[18] branżowego kodeksu postępowania dla podmiotów wykonujących działalność leczniczą w związku z wprowadzeniem RODO. Przedmiotowy projekt, mimo wysłania go 13 listopada 2018 r. do zatwierdzenia przez PUODO, do dnia zakończenia niniejszej kontroli nie uzyskał jego akceptacji[19]. Dyrektor wyjaśniła, że powodem niestosowania kodeksu dobrych praktyk jest jego niezatwierdzenie przez odpowiednie instytucje. (akta kontroli str. 20-21, 30-31, 276-280)

Stwierdzone nieprawidłowości

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

1. Szpital – wbrew wymogom art. 37 ust. 7 RODO – do dnia rozpoczęcia kontroli nie opublikował m.in. na swojej stronie internetowej danych IOD[20] wraz z informacją o sposobie i formie kontaktu. IOD wyjaśniła, że wynikało to z przeoczenia. W trakcie kontroli udostępniono na tablicach informacyjnych Szpitala[21] przedmiotową informację. (akta kontroli str. 4-5, 22-23, 30-31, 157-166)

2. W Szpitalu w całości opublikowano w intranecie tekst PBODO oraz IZSI wraz z załącznikami. Publikacji podlegały m.in. zasady precyzujące liczbę i złożoność znaków składających się na hasła dostępowe dla użytkowników oraz administratora systemu wraz z częstotliwością ich zmian. Takie postępowanie stwarza istotne ryzyko, że informacje te mogą zostać wykorzystane do przełamania ustanowionych zabezpieczeń. IOD wyjaśniła, że wynikało to po części z chęci ułatwienia kierownikom poszczególnych komórek organizacyjnych dostępu do tekstu tych dokumentów, ponieważ byli oni zobowiązani do zapoznania z ich treścią wszystkich podległych pracowników, w tym nieposiadających dostępu do systemu informatycznego ZOZ. Dodała, że nie miała świadomości, że może to mieć wpływ na bezpieczeństwo przetwarzania danych osobowych. (akta kontroli str. 4-5, 22-23)

3. Do dnia rozpoczęcia kontroli IOD nie prowadziła: rejestru czynności przetwarzania danych osobowych, co naruszało art. 30 RODO, a także wykazu zbiorów danych osobowych wraz ze wskazaniem programów zastosowanych do przetwarzania tych danych i opisu struktury zbiorów danych osobowych, wskazujących zawartość poszczególnych pól informacyjnych i powiązania między nimi oraz sposobu przepływu danych pomiędzy poszczególnymi systemami, tj. dokumentów wymaganych w § 4 ust. 4 pkt. 2 i 3 PBODO. Natomiast ewidencję osób upoważnionych do przetwarzania danych osobowych oraz wykaz budynków, pomieszczeń lub ich części tworzących obszar, w którym przetwarzane są dane osobowe, prowadzono niezgodnie z wzorami określonymi w zał. nr 1 i 8 do PBODO. IOD wyjaśniła, że: „Wynikało to z przeoczenia

[18] M.in. wypełniano ankiety, przesyłano uwagi do projektu kodeksu branżowego, a Dyrektor Szpitala jest członkiem Rady Naczelnej Polskiej Federacji Szpitali.

[19] Projekt medycznego kodeksu branżowego przygotowała Polska Federacja Szpitali. W dniu 13 listopada 2018 r. został on złożony prezesowi Urzędu Ochrony Danych Osobowych, w celu zatwierdzenia. http://www.rodowzdrowiu.pl/wp-content/uploads/2018/11/2018-11-13-KODEKS-BRAN%C5%BBOWY-Wniosek-o-zatwierdzenie-kodeksu-postepowania.pdf.

[20] Przedmiotowe dane opublikowano 24 stycznia 2019 r. na stronie BIP Szpitala.

[21] Tablice ogłoszeń umiejscowiono przy obu rejestracjach do poradni specjalistycznych, na Izbie Przyjęć oraz przy Oddziale Leczenia Uzależnień.

oraz dużej ilości innych obowiązków. W Szpitalu jestem zatrudniona od listopada 2018 r., wykonuję również obowiązki pracownika ds. administracyjnych. Obecnie ewidencja osób upoważnionych do przetwarzania danych osobowych oraz wykaz budynków, pomieszczeń lub ich części tworzących obszar, w którym przetwarzane są dane osobowe prowadzone są zgodnie z obowiązującymi wzorami. Założyłam i uzupełniłam również wykaz zbiorów danych osobowych wraz ze wskazaniem programów zastosowanych do przetwarzania tych danych. Jestem w trakcie przygotowywania rejestru czynności przetwarzania danych osobowych oraz opisu struktury zbiorów danych osobowych wskazujących zawartość poszczególnych pól informacyjnych i powiązania między nimi oraz sposobu przepływu danych pomiędzy poszczególnymi systemami". (akta kontroli str. 22-23, 30-31, 255-274)

4. IOD nie wywiązała się z obowiązku prowadzenia szkoleń personelu uczestniczącego w operacjach przetwarzania danych, ustalonego w art. 39 ust. 1 lit. b RODO. Obowiązek zapewnienia szkoleń osobom zaangażowanym w proces przetwarzania informacji, z uwzględnieniem zagrożenia jej bezpieczeństwa, skutków naruszenia zasad bezpieczeństwa, konsekwencji prawnych i środków zapewniających bezpieczeństwo wynika także z § 20 ust. 2 pkt 6 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[22]. Przed wejściem w życie przepisów RODO w dwóch szkoleniach z zakresu ochrony danych osobowych uczestniczyło odpowiednio 17% i 10,7% pracowników. Po wejściu w życie RODO żaden z pracowników Szpitala nie został objęty takim szkoleniem. Na podstawie list uczestników szkoleń oraz oświadczeń o przeszkoleniu w zakresie danych osobowych i znajomości przepisów wprowadzonych zarządzeniem nr 7/2018 z 17 maja 2018 r., stwierdzono, że 13 z 60 wytypowanych pracowników Szpitala nie uczestniczyło w szkoleniach przeprowadzonych 27 marca i 26 kwietnia 2018 r. oraz nie złożyło przedmiotowych oświadczeń, co może świadczyć, że nie zostali oni zapoznani z przepisami wewnętrznymi oraz nie byli przeszkoleni z zakresu ochrony danych osobowych i przepisów RODO. IOD wyjaśniła, że nie przeprowadzała szkoleń dla pracowników Szpitala z powodu krótkiego stażu pracy w ZOZ oraz wykonywania dużej ilości obowiązków na stanowisku ds. administracyjnych. Dodała: „Nie wiedziałabym co należałoby przekazać na szkoleniach, a nie chciałam tylko cytować pustych przepisów. Oczekuję na zatwierdzenie kodeksu branżowego i wtedy przygotuję szkolenie, w trakcie którego będę mogła przedstawić zachowania czy przykłady praktyczne, co robić, jak się zachować". Natomiast w kwestii braku przedmiotowych oświadczeń dodała, że: „Wyjaśnię tą sprawę i w przypadku braku stosownych szkoleń niezwłocznie zapoznam te osoby z odpowiednimi przepisami i dokumentami. (akta kontroli str. 22-23, 107-116, 120-134)

OCENA CZĄSTKOWA

Szpital wywiązał się z obowiązku opracowania dokumentacji oraz procedur uwzględniających przepisy RODO. Powołano IOD i zgłoszono ten fakt PUODO. Przeprowadzono także wymaganą analizę ryzyka procesów przetwarzania danych osobowych. Stwierdzono jednak nieprawidłowości polegające na:

- nieopublikowaniu danych IOD wraz z informacją o sposobie i formie kontaktu,
- nieprowadzeniu lub prowadzeniu niezgodnie z wzorem rejestru czynności przetwarzania, wykazu zbiorów danych osobowych oraz ewidencji osób upoważnionych do przetwarzania danych osobowych, tj. dokumentów wymaganych przepisami RODO i PBODO,
- ujawnieniu w intranecie zasad precyzujących liczbę i złożoność znaków składających się na hasła dostępowe dla użytkowników oraz administratora wraz z częstotliwością ich zmian,
- niezapewnieniu całemu personelowi Szpitala szkoleń związanych z wejściem w życie RODO oraz zagadnieniami dotyczącymi ochrony i bezpieczeństwa danych osobowych.

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

OBSZAR

2. Zapewnienie prawidłowego przetwarzania i ochrony danych osobowych

Opis stanu faktycznego

2.1. W celu właściwej ochrony danych osobowych w ZOZ funkcjonowały niżej wymienione rozwiązania.

1. Rejestracje pacjentów do jednej z pięciu poradni oraz w Izbie Przyjęć Szpitala odbywały się w wydzielonych pomieszczeniach, w których w trakcie oględzin przebywali pacjenci aktualnie się rejestrujący (pozostali oczekujący byli poza tymi pomieszczeniami). Przed wejściem umieszczono informacje: „W rejestracji może znajdować się tylko jedna osoba. Pacjentów oczekujących zapraszamy do zajęcia miejsca na krzesłach". Rejestracja do kolejnej poradni odbywała się przy okienku na korytarzu, przed którym nie wyznaczono linii dla oczekujących pacjentów. W trakcie oględzin stwierdzono, że poszczególne osoby były proszone o skorzystanie z krzeseł na korytarzu i kolejno wzywani przez rejestratorkę. Przed okienkiem zamieszczono informacje, że może znajdować się tam tylko jedna osoba.
2. Nad okienkiem do rejestracji pacjentów i przed wejściem do pomieszczeń, w których odbywała się rejestracja znajdowała się informacja, że w związku z RODO Szpital zachowuje w tajemnicy dane osobowe. Przed wejściem do Izby Przyjęć wywieszono informację, że w celu rejestracji wymagane jest posiadanie dowodu osobistego. W pozostałych dwóch rejestracjach nie wywieszono informacji tego typu, jednak w trakcie oględzin stwierdzono, że nie wymieniano nazwisk pacjentów (rejestracji dokonywano na podstawie dowodu osobistego). Przed każdym pomieszczeniem na tablicy informacyjnej znajdowała się informacja o przetwarzaniu danych osobowych. Zamieszczono na niej m.in. dane administratora, cele i podstawy przetwarzania danych, ich kategorie, odbiorców oraz pouczenie o prawie do dostępu, sprostowania, przenoszenia danych i o wnoszeniu skarg. Nie podano natomiast danych IOD oraz sposobu kontaktu z nim, co szerzej opisano w pkt. 1.1. niniejszego wystąpienia.
3. W obrębie wzroku osób rejestrujących się na świadczenia medyczne nie znajdowały się dane osobowe innych pacjentów. Ustawienia monitorów uniemożliwiały wgląd do wyświetlanych treści. Dokumenty medyczne przechowywano w zamykanych szafach. Pacjentów umawiano na godziny do konkretnego gabinetu lub lekarza.
4. Podczas rejestracji do poradni specjalistycznych pacjent otrzymywał karteczkę z datą i planowaną godziną przyjęcia. Pacjenci na wizytę oczekiwali w ogólnej poczekalni. Do gabinetów wzywani byli przez lekarzy, bez używania danych osobowych np.: „Pan Wojtek na godz. 9" lub „Zapraszam następną osobę na godz. 10.30". IOD wyjaśniła, że: „Każdorazowo lekarze wychodzą z gabinetów i zapraszają pacjentów na wizytę. Najczęściej są to kontynuacje leczenia i poszczególne osoby znają swoich lekarzy. W przypadku pierwszorazowej wizyty lekarz zaprasza taką osobę, podając numer gabinetu i godzinę w wizyty."
5. We wszystkich trzech objętych oględzinami gabinetach poradni specjalistycznych dokumentację pacjentów przechowywano we właściwy sposób. Teczki pacjentów oczekujących i wcześniej przyjętych przechowywano w szafkach za biurkami lub w szufladach biurka. Na biurku leżała jedynie odwrócona teczka pacjenta umówionego na daną godzinę. Monitory ustawiono w sposób uniemożliwiały wgląd do wyświetlanych treści. W trakcie oględzin nie stwierdzono przypadków pozostawienia gabinetów lekarskich bez nadzoru.
6. W dyżurkach pielęgniarskich na trzech[23] objętych oględzinami oddziałach szpitalnych ruch chorych[24] prowadzony był w formie elektroniczne, a na jednym z oddziałów dodatkowo na zakrywanej tablicy, ulokowanej w miejscu niewidocznym dla osób postronnych. Podręczna dokumentacja pielęgniarska przechowywana była w niezamykanych szufladach biurek, co szerzej opisano w dalszej części wystąpienia, w sekcji „Stwierdzone nieprawidłowości". Wejście do wszystkich dyżurek było zamykane na klucz. Na łóżkach w oddziałach objętych oględzinami nie stwierdzono kart

[23] Oględziny przeprowadzono na oddziałach: Psychiatrycznym, Leczenia Uzależnień i Zaburzeń Emocjonalnych oraz Psychosomatycznym.

[24] Ruch chorych to lista pacjentów danego oddziału wraz z numerami sal, w których przebywają.

medycznych. Część pacjentów nie nosiła opasek, co było zgodne z przepisami art. 36 ust. 3 i 4 ustawy z dnia 15 kwietnia 2011 r. o działalności leczniczej[25], w myśl którego w znaki identyfikacyjne nie zaopatruje się pacjentów szpitala lub oddziału psychiatrycznego. Na opasce zamieszczano kod kreskowy oraz nr księgi głównej. Wszystkie dyżurki były wyposażone w czytniki do odczytu danych na opaskach. Personel pielęgniarski, opuszczając dyżurkę pielęgniarek, blokował dostępu do systemu komputerowego.

7. W dwóch gabinetach lekarskich w oddziałach objętych oględzinami dokumentacja lekarska przechowywana była w niezamykanych szafkach, a w kolejnym – leżała obok monitora na biurku, co szerzej opisano w dalszej części wystąpienia pokontrolnego, w sekcji „Stwierdzone nieprawidłowości". Gabinety te były zamykane.
8. W Szpitalu od 17 grudnia 2008 r. funkcjonował monitoring wewnętrzny, który swoim zasięgiem obejmował: parking Szpitala, podjazd Izby Przyjęć, hol główny, hol parteru (w tym tzw. niskiego), korytarze przed wejściem do oddziałów: Psychiatrycznego (I i II), Leczenia Uzależnień oraz wejście oraz korytarz Zakładu Pielęgnacyjno-Opiekuńczego Psychiatrycznego. Monitoring rejestrował tylko obraz. Urządzenia nagrywające zainstalowano w zamykanych pomieszczeniach, a bieżący dostęp do nich posiadał jedynie informatyk. Nagrania były przechowywane przez 50 dni, po czym automatycznie usuwane (nadpisywane). Spośród 239 osób zatrudnionych w Szpitalu na 18 lutego 2019 r., 130 pracowników potwierdziło pisemnie zapoznanie się z procedurą określającą sposób i zasady funkcjonowania monitoringu w ZOZ. Do dnia rozpoczęcia kontroli NIK 109 osób nie potwierdziło faktu zapoznania się z tym dokumentem. Procedurę dotyczącą zasad i miejsc objętych monitoringiem opracowano 31 sierpnia 2018 roku, tj. 9 lat, 8 miesięcy i 14 dni od dnia jego zainstalowania. Problem ten szerzej opisano w dalszej części wystąpienia pokontrolnego, w sekcji „Stwierdzone nieprawidłowości". (akta kontroli str. 157-171, 275-276, 285-287)

2.2. Personel działów administracyjnych[26] Szpitala liczył 32[27] osoby, z których 12 posiadało dostęp do systemu HIS[28]. Osoby te były użytkownikami tego systemu, w myśl art. 24 ust. 2 pkt 2 ustawy z dnia 6 listopada 2008 r. o prawach pacjenta i Rzeczniku Praw Pacjenta[29], zgodnie z którym osoby wykonujące czynności pomocnicze przy udzielaniu świadczeń zdrowotnych, a także czynności związane z utrzymaniem systemu teleinformatycznego są uprawnione do dostępu do danych medycznych, na podstawie upoważnień administratora danych. Ponadto siedem osób miało dostęp do systemu ERP. Nie stwierdzono przypadku umożliwienia dostępu do wymienionych systemów żadnej z 30 objętych badaniem osób w zakresie szerszym niż niezbędny do wykonywanych przez nich zadań.

(akta kontroli str. 4-5, 117-156)

2.3. Żadna z 30 (z 87 ogółem) objętych analizą osób zatrudnionych w Szpitalu na stanowiskach pielęgniarki lub pielęgniarza nie posiadała w systemie HIS dostępu do danych pacjentów z innych oddziałów szpitalnych (dostęp przyznano jedynie do danych pacjentów oddziału lub oddziałów, na którym świadczyła pracę). Stwierdzono też m.in., że:

- w dwóch przypadkach uprawnienia do systemu HIS Szpitala nadano od siedmiu do 21 dni przed udzieleniem tym pracownikom upoważnienia do przetwarzania danych osobowych,
- w jednym przypadku przydzielono dostęp do systemu HIS bez upoważnienia osoby do przetwarzania danych osobowych, a w kolejnym udzielono dostępu do tego systemu bez akceptacji IOD, wymaganej przepisami PBODO, co szerzej opisano w dalszej części wystąpienia pokontrolnego, w sekcji „Stwierdzone nieprawidłowości".

---

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

[26] Dział Finansowo Gospodarczy, Sekcja Statystyki, Dokumentacji i Rejestracji z Archiwum, Sekcja Organizacyjna oraz samodzielne stanowiska: pełnomocnik dyrektora ds. jakości, specjalista ds. kontroli wewnętrznej, ASI, inspektor ds. obrony cywilnej i spraw niejawnych, kapelan szpitalny, inspektor BHP oraz p.poż.

[27] W tym m.in. opiekunowie medyczni i pracownicy socjalni.

[28] Hospital Information System – rodzaj oprogramowania do obsługi ruchu pacjentów wewnątrz podmiotu leczniczego.

[29] Dz. U. z 2017 r. poz. 1318, ze zm. Ustawa zwana dalej: *u.o.p.p.*

Upoważnienia do przetwarzania danych osobowych były udzielane dla zatrudnionych w placówce sanitariuszy oraz opiekunów medycznych. Dyrektor Szpitala wyjaśniła, że: „Te grupy zawodowe mają styczność z danymi medycznymi pacjentów Szpitala. Placówka nasza nie posiada własnego laboratorium, z czego wynika konieczność transportu chorych m.in. do Szpitala Wojewódzkim im. dr. Ludwika Rydygiera w Suwałkach na badania czy konsultacje oraz odbiór wyników."

Wszyscy pracownicy podmiotu zewnętrznego świadczący usługi sprzątania na terenie ZOZ posiadali zgodę na przebywanie w obszarze przetwarzania danych oraz - zgodnie z § 10 pkt 7 PBODO Szpitala – złożyli oświadczenie o zachowaniu w poufności informacji dla osób przebywających w obszarze przetwarzania danych.

(akta kontroli str. 20-21,117-156, 240-241, 243-244, 275-276)

2.4. Od 25 maja 2018 r. do dnia rozpoczęcia kontroli Szpital rozwiązał stosunek pracy z 26 osobami, wśród których 15 miało dostęp do systemów informatycznych placówki. We wszystkich tych przypadkach dostęp do systemów informatycznych odebrany został po upływie od dziewięciu do 227 dni od momentu zaprzestania przez poszczególne osoby świadczenia pracy, co szczegółowo przedstawiono w dalszej części wystąpienia pokontrolnego, w sekcji „Stwierdzone nieprawidłowości". (akta kontroli str. 135-136)

2.5. W Szpitalu zgłaszanie usterek dostawcy oprogramowania[30] związanego z udzielaniem świadczeń zdrowotnych (HIS i EDM) odbywało się w dwojaki sposób, tj. poprzez specjalistyczną platformę (Centralny Help Desk) oraz za pośrednictwem poczty elektronicznej. Zgłoszeń dokonywał informatyk Szpitala / ASI. Od 25 maja 2018 r. do 11 lutego 2019 r. za pośrednictwem tej platformy dokonano siedmiu zgłoszeń o zakłóceniach pracy systemu. Z wykorzystaniem poczty elektronicznej przesłano zaś 37 takich zgłoszeń. Analiza zgłoszeń wykazała, że w jednym przypadku (zrealizowanym za pośrednictwem platformy) do opisu błędu dołączono załącznik, w którym ujawniono imię i nazwisko, PESEL oraz fakt hospitalizacji pacjenta na jednym z oddziałów Szpitala, co omówiono w dalszej części wystąpienia pokontrolnego, w sekcji „Stwierdzone nieprawidłowości". W pozostałych przypadkach załączniki dołączane do zgłoszeń były zanonimizowane, a przy zgłaszaniu usterek z wykorzystywaniem poczty elektronicznej nie przekazano danych medycznych lub osobowych pacjentów.

Informatyk wyjaśnił, że nie ma wiedzy czy dostawca oprogramowania wywiązał się z obowiązku przeprowadzenia testów akceptacyjnych, określonego art. 21 ust. 1 ustawy z dnia 17 lutego 2005 r. o informatyzacji działalności podmiotów realizujących zadania publiczne[31]. (akta kontroli str. 172-176, 281-282)

2.6. W okresie objętym kontrolą obowiązywało 15 umów powierzenia danych osobowych. W dwóch z nich Szpital był podmiotem przetwarzającym, a w pozostałych – administratorem danych. Analizie poddano trzy umowy zawarte ze Szpitalem Wojewódzkim im. dr. Ludwika Rydygiera w Suwałkach; NZOZ Medyczne Laboratorium Diagnostyczne „NovaLab" w Suwałkach oraz Szpitalem Wojewódzkim im. Kardynała Stefana Wyszyńskiego w Łomży, w których podmioty te były podmiotami przetwarzającymi dane. W dwóch pierwszych umowach zamieszczono wszystkie elementy wymagane art. 28 RODO. Natomiast aneks nr 1 do umowy podpisanej ze Szpitalem Wojewódzkim w Łomży, dotyczący ochrony danych osobowych, nie spełniał wymogów przewidzianych tymi przepisami, co szerzej opisano w dalszej części wystąpienia pokontrolnego, w sekcji „Stwierdzone nieprawidłowości".

(akta kontroli str. 177-195)

2.7. Załącznikiem nr 12 do PBODO była Instrukcja postepowania w sytuacji naruszenia ochrony danych osobowych, w której określono m.in.: [1] katalog sytuacji zagrażających bezpieczeństwu danych osobowych; [2] sposób postępowania w przypadku stwierdzenia naruszeń; [3] obowiązek dokumentowania wszystkich naruszeń danych osobowych i ich okoliczności na opracowanym formularzu[32], wynikający z art. 33 ust. 5 RODO. Zgodnie z przepisem art. 33 ust. 1 u.o.d.o., w § 10 pkt 1 w Instrukcji wskazano obowiązek zgłoszenia PUODO w terminie 72 godzin, każdego przypadku naruszenia danych osobowych,

[30] Dostawcą oprogramowania AMMS (HIS i EDM) była firma JP System Sp. z o.o.
[31] Dz. U. 2017 r. poz. 570, ze zm.
[32] Formularz nosił nazwę: Zgłoszenie naruszenia ochrony danych osobowych organowi nadzorczemu.

skutkującego ryzykiem naruszenia praw lub wolności osób fizycznych. W rejestrze incydentów bezpieczeństwa i działań korygujących i zapobiegawczych[33] nie odnotowano przypadków naruszenia zasad ochrony danych osobowych pacjentów.

(akta kontroli str. 4-5, 36-77, 183-184)

2.8. W ZOZ obowiązywała procedura dotycząca udostępniania dokumentacji medycznej[34] pacjentów, w której m.in. opisano zasady udzielania takich informacji oraz określono podmioty upoważnione do jej otrzymania. Do Szpitala od 25 maja 2018 r. do 21 lutego 2019 r. wpłynęło 226 wniosków o udostępnienie dokumentacji lub danych medycznych, z tego 157 od podmiotów zewnętrznych takich, jak: Policja, ZUS, sądy, prokuratura, organy pomocy społecznej oraz jeden wniosek od komercyjnej firmy ubezpieczeniowej, a także 69 wniosków od pacjentów. Do wniosku o udostępnienie danych w zakresie leczenia i czasu pobytu pacjenta na jednym z oddziałów ZOZ, firma ubezpieczeniowa dołączyła oświadczenie o posiadaniu pisemnej zgody / upoważnienia do zasięgania informacji o stanie zdrowia, w celach związanych z ustaleniem prawa tej osoby do świadczenia ubezpieczonego i wysokości tego świadczenia oraz potwierdzoną za zgodność z oryginałem kopię przedmiotowego upoważnienia. Wszystkie wnioski zostały załatwione pozytywnie. Szpital udostępniał dokumentację i dane medyczne zgodnie z przepisami art. 24 ust. 1 i 3 u.o.p.p. oraz regulacjami wewnętrznymi. (akta kontroli str. 94-98, 197)

2.9. W Szpitalu funkcjonowała jedna serwerownia. Jej pomieszczenie nie posiadało okien, było nieoznakowane, zabezpieczone drzwiami antywłamaniowymi i przeciwpożarowymi oraz dwoma zamkami i systemem przeciwwłamaniowym. Wejście do serwerowni objęte było monitoringiem wizyjnym. Pomieszczenie wyposażono w czujniki p.poż, system klimatyzacji oraz podtrzymywania napięcia (dwa UPS-y). Przed wejściem umieszczono gaśnicę. W pomieszczeniu nie przetrzymywano niewykorzystywanych urządzeń oraz innych materiałów łatwopalnych. Serwery zainstalowano w specjalistycznych szafach, usytuowanych na podłodze technicznej. Nie prowadzono ewidencji wejść do serwerowi. Na jednym z serwów wykorzystywanych do przetwarzania danych medycznych wyodrębniono miejsce (serwery wirtualne), na których wykonywano i przechowywano kopie systemów informatycznych, wykorzystywanych przez Szpital.

Stosownie do wymogu § 9 ust. 3 IZSI, w ZOZ określono częstotliwość wykonywania kopii bezpieczeństwa użytkowanych programów, zakres danych podlegających archiwizowaniu, miejsce przechowywania kopii bezpieczeństwa oraz rodzaj nośnika wykorzystywanego do wykonywaniu kopii bezpieczeństwa. Kopie bezpieczeństwa stosowanych systemów komputerowych (HIS, EDM i ERP) były przechowywane w innej lokalizacji niż baza danych podlegająca procesowi tworzenia kopii. Kopie te wykonywano codziennie i składowano na serwerach backupowych w serwerowni, skąd ASI przenosił je (raz w tygodniu) na zewnętrzny nośnik danych. Sporządzone kopie przechowywane były w pomieszczeniu informatyka. Pomieszczenie te było zabezpieczone drzwiami antywłamaniowymi oraz dwoma zamkami. Wyposażono je również w systemem przeciwwłamaniowy oraz zainstalowano czujkę p.poż. Okno było zakratowane.

(akta kontroli str. 4-5,198-212, 233, 241, 281-283)

W trakcie oględzin 30 komputerów (po 10 użytkowanych przez pielęgniarki, lekarzy oraz pracowników administracyjnych), służących do przetwarzania danych osobowych stwierdzono, że dostęp do poszczególnych systemów informatycznych (m.in. Windows, HIS, ERP[35]) 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 wymaganą w § 18 ust. 4 pkt 1 PBODO. Na dyskach komputerów objętych oględzinami nie stwierdzono informacji zawierających dane medyczne pacjentów. W trzech przypadkach stwierdzono możliwość samodzielnego pobrania i zainstalowania dowolnego oprogramowania, co szerzej opisano w dalszej części wystąpienia

---

[33] Przedmiotowy rejestr stanowił zał. nr 2 do Instrukcji postępowania w sytuacji naruszenia ochrony danych osobowych.

[34] Procedura została zatwierdzona 17 czerwca 2017 r. i zmieniona 26 lutego 2019 r. Zmiana dotyczyła m.in. dopuszczenia formy ustnej w zakresie wniosku o wydanie dokumentacji medycznej (dotyczyło to tylko pacjentów), czy doprecyzowania, że wydanie pierwszej kopii przedmiotowej dokumentacji następuje bezzwłocznie i jest bezpłatne.

[35] W ramach ERP (program Infomedica) funkcjonowały różne moduły, m.in.: finanse i księgowość, środki trwałe, rejestry sprzedaży i zakupów, koszty, ZUS, kadry. Do każdego z modułu trzeba było logować się oddzielnie.

pokontrolnego, w sekcji „Stwierdzone nieprawidłowości". W 29 przypadkach zainstalowany program antywirusowy posiadał aktualną bazę sygnatur wirusów. Natomiast w jednym przypadku, oprogramowanie to jako ostatnią, wskazywało aktualizację z 16 grudnia 2018 r. Informatyk wyjaśnił, że: „Przy instalacji oprogramowania wystąpiła konieczność indywidualnej zmiany ustawień oprogramowania na tym komputerze. Po zakończeniu instalacji omyłkowo nie przywróciłem pierwotnych ustawień. Przeinstalowałem oprogramowanie i obecnie funkcjonuje ono prawidłowo". We wszystkich komputerach objętych analizą porty USB nie były zabezpieczone i umożliwiały odczytywanie danych z podłączonego nośnika. (akta kontroli str. 231-232, 281-282)

W Szpitalu nie przeprowadzano rejestru identyfikatorów przyznanych użytkownikom poszczególnych komputerów oraz cokwartalnych cyklicznych kontroli antywirusowych, wymaganych regulacjami IZSI, co szerzej opisano w dalszej części wystąpienia pokontrolnego, w sekcji „Stwierdzone nieprawidłowości". (akta kontroli str. 4-5)

Na obu komputerach przenośnych, wykorzystywanych w ZOZ do przetwarzania danych osobowych, nie zastosowano ochrony kryptograficznej nośników pamięci. Nie wykorzystywano także pseudonimizacji danych osobowych, jako jednego ze środków do ochrony danych pacjentów. Komputerów tych nie wykorzystywano do przetwarza danych osobowych (służyły pomocą przy organizacji szkoleń czy konferencji).
(akta kontroli str. 4-5, 241, 283)

Stwierdzone nieprawidłowości

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

1. W dyżurkach pielęgniarskich, zlokalizowanych na trzech objętych oględzinami oddziałach szpitalnych, podręczna dokumentacja pielęgniarska przechowywana była w niezamykanych szufladach biurek. Podobnie, w dwóch gabinetach lekarskich na tych samach oddziałach dokumentacja lekarska przechowywana była w niezamykanych szafkach, a w jednym przypadku pozostawiono ją na biurku pod nieobecność personelu. Naruszało to § 14 ust. 3 PBODO, zgodnie z którym kopie papierowe z danymi osobowymi przechowuje się w zamykanych na klucz, nieoszklonych szafkach, szufladach lub sejfach. IOD wyjaśniła, że: „Sądzę ze wynikało to z niefrasobliwości poszczególnych pracowników. Przypomniałam im o konieczności przestrzegania zapisów PBODO." (akta kontroli str. 22-23, 157-166)

2. Procedurę dotyczącą zasad i miejsc objętych monitoringiem opracowano 31 sierpnia 2018 roku, tj. 9 lat, 8 miesięcy i 14 dni od dnia jego zainstalowania. Ponadto spośród 239 osób zatrudnionych 18 lutego 2019 r. w Szpitalu, jedynie 130 potwierdziło pisemnie zapoznanie się z procedurą określającą sposób i zasady funkcjonowania monitoringu w ZOZ, a 109 osób nie potwierdziło tego faktu. Takie postępowanie naruszało art. 22^2 § 7 Kodeksu pracy[36], zgodnie z którym pracodawca jest zobowiązany poinformować pracowników o wprowadzeniu monitoringu, nie później niż dwa tygodnie od przed jego uruchomieniem. Pełnomocnik Dyrektora ds. zarzadzania jakością wyjaśniła, że procedura: „(...) została opracowania niezwłocznie po szkoleniu o wprowadzeniu przepisów dotyczących przedmiotowej sprawy. Jednak z uwagi na okres urlopowy pełnomocnika ds. jakości i wielu urlopów kierowników komórek organizacyjnych procedura została przekazana pracownikom w sierpniu 2018 r. Dodatkowym utrudnieniem była zmiana na stanowisku IOD." Dodała, że powodem niezapoznania 109 osób z personelu Szpitala z procedurą stosowania monitoringu był fakt przebywania kilku osób na zwolnieniach lekarskich i że: „Niewykluczone także, że zobowiązani do przekazania stosownej informacji pracownikom poszczególnych komórek organizacyjnych kierownicy lub koordynatorzy, wskutek przeoczenia nie dopełnili obowiązku (...)." (akta kontroli str. 234-238, 275)

3. Dwóm pracownikom (z 30 objętych analizą) nadano uprawnienia do systemu HIS od siedmiu do 21 dni przed udzieleniem im upoważnienia do przetwarzania danych osobowych. Kolejnej osobie udzielono dostępu do systemu HIS, mimo że nie posiadała ona upoważnienia do przetwarzania danych osobowych, a następnej udzielenie dostępu

[36] Dz. U. 2018 poz. 917, ze zm. Przepis wszedł w życie 25 maja 2018 r.

nie zostało poprzedzone akceptacją IOD, wymaganą przepisami PBODO. Naruszono w ten sposób przepis § 6 ust 1 i 6 IZSI, zgodnie z którym dostęp do systemu informatycznego przetwarzającego dane osobowe może być przyznany jedynie osobom, które uzyskały upoważnienia do przetwarzania danych osobowych, a ASI nadaje lub odbiera stosowne uprawnienia po akceptacji IOD. ASI wyjaśnił, że: „Wynikało to z przeoczenia oraz dużej ilości innych obowiązków. Jestem jedynym informatykiem w Szpitalu". Również przeoczeniem IOD wyjaśniła fakt nadania jednej osobie uprawnienia do systemów informatycznych Szpitala bez upoważnienia jej do przetwarzania danych osobowych. Dodała, że: „Obecnie osoba ta przebywa na zwolnieniu lekarskim. Po jej powrocie zostanie ona powtórnie przeszkolona i otrzyma stosowne upoważnienie. (akta kontroli str. 22-23, 213-232, 281-282)

4. Spośród 26 osób, które zakończyły zatrudnienie w Szpitalu, 15 osobom uprawnienia w systemach informatycznych odebrano dopiero po upływie od dziewięciu do 227 dni od momentu zaprzestania przez te osoby świadczenia pracy. Stanowiło to naruszenie § 6 ust. 1 IZSI w związku z § 5 ust. 10 PBODO, zgodnie z którymi dostęp do systemu informatycznego przetwarzającego dane osobowe może być przyznany jedynie osobom, które uzyskały upoważnienia do przetwarzania danych osobowych. Upoważnienie wygasa zaś wraz z rozwiązaniem umowy o pracę lub zakończeniem wykonywania czynności związanych z przetwarzaniem danych osobowych. Postępowanie takie było także niezgodne z § 20 ust. 2 pkt 4 i 5 rozporządzenia KRI. Jednocześnie art. 5 pkt 1 lit. c RODO wskazuje zasadę adekwatności i minimalizacji danych, tj. wymóg ustalenia kto i w jakim zakresie jest uprawniony do przetwarzania danych. Informatyk wyjaśnił, że: „Spowodowane to było brakiem informacji od kierowników komórek organizacyjnych, że poszczególne osoby zakończyły zatrudnienie." Dyrektor wyjaśniła, że: „Informatyk został już dopisany do karty obiegowej, tj. dokumentu wypełnianego przed odejściem pracownika ze Szpitala w celu jego rozliczenia się z firmą. W efekcie będzie miał on wiedzę kto zaprzestał świadczenia pracy i możliwość stosownej reakcji."
(akta kontroli str. 20-21, 36-91, 135-136, 281-282)

5. W jednym (z siedmiu, zrealizowanych od 25 maja 2018 r. do 11 lutego 2019 r.) zgłoszeniu serwisowym, dotyczącym zakłóceń pracy w użytkowanym przez ZOZ systemie informatycznym, za pośrednictwem specjalistycznej platformy do opisu błędu przekazano załącznik, w którym ujawniono imię i nazwisko, PESEL oraz fakt hospitalizacji pacjenta na jednym z oddziałów Szpitala. Działanie takie było niezgodne z art. 5 pkt. 1 lit. c RODO, w którym wskazano zasadę adekwatności i minimalizacji przetwarzania danych. Informatyk wyjaśnił, że wynikało to z przeoczenia i pośpiechu.
(akta kontroli str. 172-176, 281-282)

6. Jedna (z trzech) objętych analizą umów powierzenia przetwarzania danych osobowych[37] nie spełniała wymogów przewidzianych w art. 28 RODO. Dyrektor Szpitala wyjaśniła, że było to wynikiem przeoczenia. Dodała: „Zawarta umowa ze Szpitalem Wojewódzkim w Łomży była umową rezerwową na świadczenie usług rezonansu magnetycznego, z której nigdy nie skorzystaliśmy. W efekcie w trakcie kontroli została ona rozwiązana".
(akta kontroli str. 20-21, 177-196, 242)

7. W trzech komputerach (z 30 objętych oględzinami) stwierdzono możliwość samodzielnego pobrania i zainstalowania przez użytkowników dowolnego oprogramowania, mimo że żadna z osób użytkujących te komputery nie wykonywała zadań administratora. Postępowanie takie było niezgodne z § 20 ust. 2 pkt 4 rozporządzenia KRI. Informatyk wyjaśnił, że: „Takie uprawnienia były potrzebne na czas instalacji i uruchomienia programów, a potem z powodu przeoczenia nie zostały one cofnięte tym osobom. Obecnie zostało to naprawione i osobom tym nadano status użytkownika". (akta kontroli str. 213-232, 281-283)

[37] Umowę zawarto w dniu 17 maja 2018 r. ze Szpitalem Wojewódzkim im. Kardynała Stefana Wyszyńskiego w Łomży.

8. W Szpitalu nie prowadzono: rejestru identyfikatorów przyznanych użytkownikom poszczególnych komputerów oraz kwartalnych kontroli antywirusowych, wbrew wymogom przewidzianym odpowiednio w § 6 ust. 4 i § 11 ust. 6 IZSI. Informatyk wyjaśnił, że spowodowane to było przeoczeniem i dużą ilością pracy.

(akta kontroli str. 4-5, 36-91, 281-282)

OCENA CZĄSTKOWA

ZOZ wprowadził 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 pacjentów w procesie rejestracji i udzielania świadczeń w objętych oględzinami poradniach specjalistycznych oraz w Izbie Przyjęć. Właściwie udostępniano dokumentację medyczną na wnioski zainteresowanych oraz ograniczono uprawnienia w systemie HIS personelu administracyjnego i 30 objętych analizą pielęgniarek do zakresu zgodnego z wykonywanymi zadaniami. Wprowadzono także odpowiednie zabezpieczenia fizyczne serwerowni Szpitala i pomieszczenia pracy informatyka, w których przechowywano dane osobowe przetwarzane w formie elektronicznej.

Jednak na trzech objętych oględzinami oddziałach i w trzech gabinetach lekarskich na tych oddziałach pozostawiano niezabezpieczoną dokumentację medyczną, co było niezgodne z regulacjami wewnętrznymi. Stwierdzono również trzy przypadki nadania pracownikom uprawnień administratora w systemie operacyjnym komputerów, chociaż nie wykonywali oni obowiązków związanych z zarządzaniem siecią komputerową oraz nadanie uprawnień do systemu HIS trzem pracownikom, przed wydaniem im pisemnych upoważnień do przetwarzania danych osobowych. Nieterminowo odbierano też uprawnienia w systemach informatycznych byłym pracownikom Szpitala – nawet do 227 po dniu zakończenia pracy. Nie prowadzono również rejestru identyfikatorów przyznanych użytkownikom poszczególnych komputerów oraz nie wykonywano kwartalnych kontroli antywirusowych, do czego zobowiązywała IZSI. Dane jednego pacjenta przekazano zaś firmie świadczącej usługi help desk, chociaż nie było to konieczne do realizacji zgłoszenia serwisowego, czym złamano zasadę adekwatności.

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. Niepodawanie do publicznej wiadomości informacji ułatwiających nieautoryzowany dostęp do systemów informatycznych użytkowanych przez Szpital.
2. Opracowanie oraz bieżące prowadzenie dokumentów wymaganych przepisami PBODO i RODO.
3. Przestrzeganie przepisów wewnętrznych w zakresie przechowywania dokumentacji dotyczącej danych osobowych oraz przyznawania dostępu do wykorzystywanych systemów informatycznych.
4. Zapewnienie pracownikom dostępu do systemów informatycznych Szpitala, w zakresie wynikającym z realizowanych przez nie zadań i obowiązków.
5. Zapoznanie wszystkich pracowników Szpitala z opracowanymi zasadami funkcjonowania monitoringu w ZOZ.
6. Bieżące wydawanie upoważnień osobom przetwarzającym dane osobowe i ich niezwłoczne odbieranie osobom, które zaprzestały świadczenia pracy w Szpitalu.
7. Zapewnienie wszystkim pracownikom Szpitala szkoleń z zakresu ochrony danych osobowych i RODO.
8. Niepodawanie w zgłoszeniach serwisowych danych osobowych i medycznych pacjentów.

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 wykorzystania i 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:
Piotr Jurkin
Specjalista kontroli państwowej

Piotr Jurkin
.....
podpis

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

.....
podpis