NAJWYŻSZA IZBA KONTROLI
Delegatura w Białymstoku

LBI.410.002.01.2019

00067719

Pani Magdalena Joanna Borkowska
Białostockie Centrum Onkologii
im. M. Skłodowskiej-Curie w Białymstoku
ul. Ogrodowa 12, 15-027 Białystok

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	Białostockie Centrum Onkologii im. M. Skłodowskiej-Curie w Białymstoku (dalej: *Szpital* lub *BCO*), ul. Ogrodowa 12, 15-027 Białystok
Kierownik jednostki kontrolowanej	Magdalena Joanna Borkowska, dyrektor od 25 lipca 2017 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	Kontrola obejmuje okres od 25 maja 2018 r. do dnia zakończenia czynności kontrolnych. Badania kontrolne mogą dotyczyć działań sprzed tego okresu, jeśli mają 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	Paweł Tołwiński, specjalista kontroli państwowej, upoważnienie do kontroli nr LBI/9/2019 z 8 stycznia 2019 r. (akta kontroli str. 1-2)

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

II. Ocena ogólna[2] kontrolowanej działalności

OCENA OGÓLNA

Najwyższa Izba Kontroli ocenia negatywnie podjęte przez Szpital działania w celu zapewnienia prawidłowej ochrony i przetwarzania danych osobowych.

Uzasadnienie oceny ogólnej

Stwierdzono bowiem nieprawidłowości, polegające m.in. na:

- przekazaniu – z naruszeniem art. 24 ust. 2 ustawy z dnia 6 listopada 2008 r. o prawach pacjenta i Rzeczniku Praw Pacjenta[3] – podwykonawcy podmiotu świadczącego usługi serwisowe danych osobowych 29 pacjentów Szpitala, w tym danych medycznych, zawierających zakres lub wyniki badań pięciu pacjentów,
- udostępnieniu dokumentacji medycznej pacjenta, z naruszeniem przyjętych procedur wewnętrznych w tym zakresie,
- odebraniu z opóźnieniem byłym pracownikom uprawnień w systemie wykorzystywanym do przetwarzania danych medycznych, co było sprzeczne z przepisem § 20 ust. 2 pkt 5 rozporządzenia Rady Ministrów z dnia 12 kwietnia 2012 r. w sprawie Krajowych Ram Interoperacyjności minimalnych wymagań dla rejestrów publicznych i wymiany informacji w postaci elektronicznej oraz minimalnych wymagań dla systemów teleinformatycznych[4],
- niewłaściwym określeniu zakresu danych, jakie będzie przetwarzał podmiot zewnętrzny w jednej z pięciu objętych badaniem umów powierzenia przetwarzania danych osobowych,
- nieprzestrzeganiu przez personel Szpitala regulacji wewnętrznych dotyczących sposobu autoryzacji i korzystania z komputerów wykorzystywanych do przetwarzania danych medycznych pacjentów,
- niedostosowaniu regulacji wewnętrznych do przepisów RODO[5],
- dopuszczeniu czterech (z 30) objętych badaniem pielęgniarek i położnych do przetwarzania danych osobowych pacjentów, chociaż nie udzielono im upoważnień do przetwarzania danych osobowych, co naruszało § 12 Polityki Bezpieczeństwa Danych Osobowych Szpitala,
- nieterminowym zgłoszeniu Prezesowi Urzędu Ochrony Danych Osobowych[6] jednego z 11 incydentów związanych z bezpieczeństwem danych osobowych, co stanowiło naruszenie art. 33 ust. 1 RODO,
- niewprowadzeniu odpowiednich środków technicznych i organizacyjnych zapewniających właściwą ochronę danych osobowych oraz minimalizację ryzyka ujawnienia informacji osobom postronnym w procesie rejestracji pacjentów,
- niezabezpieczeniu miejsc przechowywania podręcznej dokumentacji pielęgniarskiej, zawierającej dane osobowe pacjentów, w dwóch (z trzech) objętych badaniem dyżurkach pielęgniarskich oraz dokumentacji medycznej w jednym (z trzech poddanych oględzinom) gabinecie lekarskim, co stanowiło naruszenie art. 24 ust. 1 RODO,
- przechowywaniu materiałów łatwopalnych oraz niewykorzystywanego sprzętu komputerowego w serwerowni oraz pomieszczeniu, w którym znajdowały się kopie bezpieczeństwa baz danych Szpitala.

---

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

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

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

[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 (Dz. Urz. UE L 119 z 2016 r., str. 1, ze zm.).

[6] Dalej: *PUODO.*

III. Opis ustalonego stanu faktycznego oraz oceny cząstkowe[7] kontrolowanej działalności

OBSZAR

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

Opis stanu faktycznego

1.1. Szpital z dniem 25 maja 2018 r. wyznaczył Inspektora Ochrony Danych (dalej: *IOD*), wywiązując się tym samym z obowiązku określonego w art. 8 ustawy z dnia 10 maja 2018 r. o ochronie danych osobowych[8] w związku z art. 37 RODO. Na to stanowisko powołany został pracownik BCO, pełniący dotychczas funkcję Administratora Bezpieczeństwa Informacji (dalej: *ABI*). Następnie, 15 października 2018 r. do pełnienia funkcji IOD wyznaczono nowo zatrudnioną osobę. W myśl art. 8 i art. 10 u.o.d.o., Szpital terminowo (za pośrednictwem formularzy elektronicznych) wywiązał się z obowiązku zawiadomienia PUODO o powołaniu, a następnie odwołaniu poprzedniego IOD oraz powołaniu na to stanowisko nowej osoby. Przekazane do PUODO zawiadomienia zawierały wszystkie elementy określone art. 10 ust. 1 i 3 u.o.d.o., tj. m.in.: imię, nazwisko oraz adres poczty elektronicznej i numer telefonu IOD, nazwę oraz adres siedziby i numer identyfikacyjny REGON administratora danych osobowych. Zgodnie z wymogiem określonym w art. 37 ust. 7 RODO, dane IOD oraz sposób i formę kontaktu udostępniono na stronie internetowej Szpitala[9]. (akta kontroli str. 5-14, 23-28, 562-563)

W zakresach obowiązków obu osób, które pełniły funkcję IOD, wskazano wszystkie zadania określone w art. 39 RODO. Osobom tym umożliwiono wykonywanie obowiązków w sposób niezależny, stosownie do art. 38 ust. 3 tego rozporządzenia. Samodzielne stanowisko IOD, podległe bezpośrednio Dyrektorowi Szpitala, zostało wyodrębnione w strukturze organizacyjnej BCO 1 października 2018 r., w związku ze zmianą regulaminu organizacyjnego[10]. Wraz z tą zmianą w regulaminie organizacyjnym wskazano zadania IOD, do których należało m.in.: [1] informowanie administratora danych osobowych oraz pracowników, którzy przetwarzają dane osobowe, o obowiązkach spoczywających na nich na mocy RODO; [2] monitorowanie przestrzegania RODO i innych przepisów o ochronie danych oraz polityk administratora lub podmiotu przetwarzającego w dziedzinie ochrony danych osobowych; [3] wdrożenie szkoleń z zakresu zasad ochrony danych osobowych oraz stosowania środków technicznych i organizacyjnych przy przetwarzaniu tych danych w systemach informatycznych; [4] udzielanie zaleceń co do oceny skutków dla ochrony danych oraz monitorowanie jej wykonywania zgodnie z art. 35 RODO; [5] prowadzenie dokumentacji wymaganej przepisami ustawy o ochronie danych osobowych, w tym opracowywanie i aktualizacja procedur wewnętrznych dotyczących ochrony danych osobowych; [6] przeciwdziałanie dostępowi osób do systemów, w których przetwarzane są dane osobowe; [7] nadzorowanie funkcjonowania zasad i procedur związanych z uwierzytelnianiem użytkowników w systemie informatycznym przetwarzającym dane osobowe oraz kontroli dostępu do tych danych; [8] zarządzanie hasłami użytkowników, systemami antywirusowymi i ich procedurami. (akta kontroli str. 5-14, 23-28)

Do 1 października 2018 r. w strukturze organizacyjnej BCO istniało samodzielne stanowisko ABI, które podlegało bezpośrednio Dyrektorowi Szpitala. Do jego zadań należało m.in.: [1] prowadzenie dokumentacji wymaganej przepisami o ochronie danych osobowych, w tym opracowywanie i aktualizacja procedur wewnętrznych dotyczących ochrony danych osobowych; [2] przeciwdziałanie dostępowi osób nieupoważnionych do systemów, w których przetwarzane są dane osobowe; [3] wdrożenie szkoleń z zakresu zasad ochrony danych osobowych oraz stosowania środków technicznych i organizacyjnych przy przetwarzaniu

---

[7] 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.

[8] Dz. U. poz. 1000, ze zm. Ustawa zwana dalej: *u.o.d.o.*

[9] www.onkologia.bialystok.pl

[10] Regulamin wprowadzono zarządzeniem wewnętrznym nr 94/2018 Dyrektora Białostockiego Centrum Onkologii im. M. Skłodowskiej-Curie w Białymstoku z dnia 1 października 2018 r. w sprawie wprowadzenia zmian w „Regulaminie Organizacyjnym" Białostockiego Centrum Onkologii im. M. Skłodowskiej-Curie w Białymstoku.

tych danych w systemach informatycznych; [4] nadzorowanie funkcjonowania zasad i procedur związanych z uwierzytelnianiem użytkowników w systemie informatycznym przetwarzającym dane osobowe oraz kontroli dostępu do tych danych. Dyrektor Szpitala w odpowiedzi na pytanie dlaczego zadania IOD zostały określone w regulaminie organizacyjnym z 1 października 2018 r., mimo że osoba na to stanowisko została powołana 25 maja 2018 r. wyjaśniła, że: *Zadania IOD były określone we wcześniejszych regulaminach organizacyjnych Szpitala jako zadania ABI. (...) Podkreślić należy, że stosownie do art. 48 pkt 2 ppkt 2 f ustawy z dnia 15 kwietnia 2011 r. o działalności leczniczej (Dz. U. z 2018 r. poz. 2190 t.j.) zmiana regulaminu organizacyjnego może nastąpić po uzyskaniu pozytywnej opinii Rady Społecznej Centrum, która obraduje na posiedzeniach raz na kwartał. Zmiany w Regulaminie zostały wprowadzone po posiedzeniu Rady, które odbyło się w dniu 21 września 2018 r.*" (akta kontroli str. 29-105, 342-345)

Zgodnie z wymogami art. 37 ust. 5 RODO, obie osoby realizujące zadania IOD miały należyte przygotowanie i kwalifikacje zawodowe do pełnienia swojej funkcji, tj. m.in.: jedna z tych osób była wcześniej ABI Szpitala, kolejna zaś posiadała certyfikat ukończenia kursu *Obowiązki Inspektora Ochrony Danych i Administratora w świetle RODO,* certyfikat ukończenia *Kursu opracowania Polityki Ochrony Danych Osobowych zgodnej z RODO,* zaświadczenie uczestnictwa w szkoleniu dotyczącym roli IOD w świetle krajowych i unijnych przepisów o ochronie danych osobowych. Ponadto od 8 października 2018 r. IOD został przyjęty na studia podyplomowe z zakresu bezpieczeństwa informacji i ochrony danych osobowych[11]. (akta kontroli str. 5-14, 23-28)

1.2. W dniu wejścia w życie przepisów RODO oraz u.o.d.o. (25 maja 2018 r.) Dyrektor BCO przyjął Politykę Bezpieczeństwa Danych Osobowych w Białostockim Centrum Onkologii im. Marii Skłodowskiej-Curie (dalej: *Polityka*), zgodnie z art. 24 ust. 1 i 2 RODO. W dokumencie tym wskazano, że jego celem jest: *uzyskanie optymalnego i zgodnego z wymogami obowiązujących aktów prawnych, sposobu przetwarzania informacji zawierających dane osobowe*. Jako podstawę opracowania Polityki, podano przepisy RODO oraz u.o.d.o. Określono w niej (rozdział IV) środki organizacyjne i techniczne niezbędne dla zapewnienia poufności, integralności i rozliczalności przetwarzanych danych osobowych, w tym zadania Administratora Danych Osobowych (dalej: *ADO*), IOD, informatyków Szpitala, kierowników komórek organizacyjnych oraz osób upoważnionych do przetwarzania danych osobowych, a także zakres przedmiotowy i podmiotowy jej stosowania. Ponadto w Polityce określono sposób przeprowadzania jej przeglądów i aktualizacji oraz dokumentowania faktu zapoznania się z jej treścią przez osoby upoważnione do przetwarzania danych osobowych (w formie pisemnego oświadczenia). Integralną częścią Polityki były załączniki, wśród których znalazły się m.in.: [1] wzór upoważnienia do przetwarzania danych osobowych; [2] wzór ewidencji osób upoważnionych do przetwarzania danych osobowych; [3] wykaz budynków i pomieszczeń tworzących obszar, w którym przetwarzane są dane osobowe; [4] wykaz zbiorów danych osobowych wraz ze wskazaniem programów zastosowanych do przetwarzania tych danych i miejsca przetwarzania. Analiza postanowień przyjętej Polityki oraz jej załączników wykazała, że zawierały one nieaktualne dane, co szerzej opisano w dalszej części wystąpienia, w sekcji *Stwierdzone nieprawidłowości*.

(akta kontroli str. 106-143)

W okresie objętym kontrolą Dyrektor BCO zatwierdził aktualizację Polityki (12 grudnia 2018 r.). Polegała ona na dodaniu zapisów dotyczących m.in.: kontaktu do IOD; wskazania obowiązku przeprowadzania przez IOD cyklicznej analizy ryzyka; przydzielenia informatykom zadań związanych z zarządzaniem systemami informatycznymi Szpitala (poprzednio miał je realizować IOD); opracowania instrukcji postępowania z incydentami; oceny skutków dla ochrony danych osobowych, o której mowa w art. 35 RODO; opisu operacji przetwarzania danych; oceny niezbędności oraz proporcjonalności zakresu przetwarzanych danych; opracowania klauzuli informacyjnej; sposobu przeprowadzania analizy ryzyka oraz postępowania z ryzykiem; wprowadzenia Regulaminu Ochrony Danych Osobowych (dalej: *Regulamin*) i procedury audytów. Ponadto w związku z aktualizacją

[11] Studia te prowadzono w roku akademickim 2018/2019 na Wydziale Ekonomii i Zarządzania Uniwersytetu w Białymstoku.

dodano 11 załączników, wśród których były m.in.: rejestr czynności przetwarzania, klauzule informacyjne, arkusz analizy ryzyka, Regulamin, procedura audytu, plan ciągłości działania. (akta kontroli str. 144-270, 322-329)

IOD wyjaśnił, że: *Polityka została zamieszczona w sieci wewnętrznej BCO, w zakładce RODO dla Pracowników oraz udostępniona w formie papierowej w sekretariacie Dyrektora oraz Dziale Kadr i Płac.* Natomiast treść Regulaminu oraz oświadczenia o poufności Dyrekcja BCO 3 stycznia 2019 r. (tj. 22 dni po ich przyjęciu) przekazała drogą mailową kierownikom działów. W wiadomości tej wystosowano prośbę o zapoznanie personelu z treścią przekazanych dokumentów oraz o zebranie podpisów pod oświadczeniami o poufności i przekazanie ich do IOD. IOD wyjaśnił, że przekazanie zaktualizowanej Polityki wraz z załącznikami (m.in. Regulaminem) nastąpiło po upływie 22 dni od jej przyjęcia z uwagi na grudniową przerwę świąteczną. (akta kontroli str. 143, 330-333)

Dodatkowymi dokumentami obowiązującymi w okresie objętym kontrolą dotyczącymi ochrony danych osobowych w Szpitalu były: Instrukcja zarządzania systemem informatycznym służącym do przetwarzania danych osobowych oraz procedura udostępniania dokumentacji medycznej, opisująca, w jaki sposób należy udostępniać dokumentację medyczną pacjentom oraz jakie inne organy mają do niej dostęp. Dokumenty te nie były jednak na bieżąco aktualizowane, co szerzej opisano w dalszej części wystąpienia, w sekcji *Stwierdzone nieprawidłowości.* (akta kontroli str. 298-316)

Polityka obowiązująca w okresie objętym kontrolą nie przewidywała konieczności opracowania dodatkowych reguł i procedur uszczegóławiających te dokumenty, poza tymi które były jej załącznikami. (akta kontroli str. 144-330, 582)

1.3. Rejestr czynności przetwarzania danych osobowych (dalej: *Rejestr*), o którym mowa w art. 30 RODO, został sporządzony 12 grudnia 2018 r. wraz z aktualizacją Polityki i stanowił jej załącznik. Obowiązek opracowania tego rejestru istniał jednak od 25 maja 2018 r., co szerzej opisano w dalszej części wystąpienia, w sekcji *Stwierdzone nieprawidłowości.* (akta kontroli str. 196-213)

Zgodnie z wymogami art. 30 ust. 3 RODO, rejestr prowadzony był w formie pisemnej i elektronicznej oraz zawierał wymagane elementy, określone w ust. 1 tego przepisu, w tym: nazwę oraz dane kontaktowe ADO i IOD; cele przetwarzania; opis kategorii osób, których dane dotyczą; kategorie odbiorców, którym dane osobowe zostały lub zostaną ujawnione; ogólny opis technicznych i organizacyjnych środków bezpieczeństwa, o których mowa w art. 32 ust. 1 RODO; planowane terminy usunięcia poszczególnych kategorii danych oraz informację dotyczącą ewentualnego przekazania danych osobowych do państwa trzeciego lub organizacji międzynarodowej. W Rejestrze zamieszczono dla każdej z 13 wykazanych kategorii osób, których dane dotyczą m.in.: [1] zakres, charakter i kontekst przetwarzanych danych; [2] podstawę prawną przetwarzania; [3] sposób realizacji praw osób, których dane są przetwarzane. (akta kontroli str. 196-213)

1.4. W okresie objętym kontrolą IOD, przeprowadził jedną analizę procesów przetwarzania danych osobowych pacjentów Szpitala, określoną w art. 32 RODO, która stanowiła załącznik do Polityki, przyjętej 12 grudnia 2018 r. W ramach tej analizy zidentyfikowano 48 zagrożeń (ryzyk) związanych z ochroną danych osobowych. Dla każdego z nich oszacowano wartość ryzyka (w skali od jednego do dziewięciu pkt), określoną jako iloczyn prawdopodobieństwa wystąpienia i skutku wystąpienia incydentu. Jako akceptowalną wartość ryzyka wskazano poziom 1–2 pkt. W pozostałych przypadkach wskazano odpowiednio: wartość 3–6 pkt – *ryzyko jest opcjonalne (akceptujemy lub odrzucamy)*, wartość 9 pkt – *ryzyko jest nieakceptowalne (musimy obniżyć)*. W rezultacie przeprowadzonej analizy, jako stanowiące największe zagrożenie (poziom ryzyka – 9 pkt), wskazano następujące incydenty: [1] instalację i działanie szkodliwego oprogramowania; [2] nakłanianie do wykonania czynności; [3] *phishing* i *cybersquatting*. Do sytuacji stanowiących mniejsze zagrożenie (poziom ryzyka – 6 pkt) zaliczono m.in.: [1] łatwo dostępne hasła o prostej złożoności; [2] włamania do urządzeń nieaktualizowanych; [3] ataki ransomeware; [4] nieuprawniony dostęp do infrastruktury IT oraz do programów; [5] nieuprawnione kopiowanie danych; [6] nieprzestrzeganie procedur. Na podstawie przeprowadzonej analizy opracowano *Plan*

postepowania z ryzykiem (dalej: *Plan postępowania*), w którym dla wszystkich 17 zagrożeń, dla których wartość ryzyka była większa niż 6 pkt, wskazano działania, jakie należy wdrożyć w celu ich ograniczenia, termin przeprowadzenia tych działań oraz osoby za to odpowiedzialne. Najczęstszym działaniem zaradczym była konieczność przeprowadzenia szkoleń oraz zapoznanie pracowników z Regulaminem (wskazano na potrzebę szkoleń wstępnych i okresowych), jako osoby odpowiedzialne za realizację tych zadań wskazywano IOD oraz informatyka. W Planie postępowania z ryzykiem (stanowiącym załącznik do Polityki) wskazano zrealizowanie działań zaradczych w odniesieniu do 14 z 17 stwierdzonych zagrożeń. W pozostałych trzech przypadkach dotyczących odpowiednio: [1] przeprowadzania testów penetracyjnych we własnym zakresie lub z udziałem firmy zewnętrznej, jako termin realizacji wskazano 31 marca 2019 r.; [2] uwzględnienie ochrony danych osobowych w fazie projektowania i wdrażania nowych systemów, wskazano że jest to proces ciągły realizowany poprzez szkolenia i ciągłe podnoszenie kwalifikacji, umiejętności i wiedzy przez personel Szpitala; [3] rozważania zainstalowania alternatywnej serwerowni w innym budynku oraz regularnego przeprowadzania procedury backupów i ich sprawdzania – nie podano terminu realizacji. IOD wyjaśnił, że termin realizacji stworzenia alternatywnej serwerowni nie został określony, gdyż taka potrzeba została jedynie zasygnalizowana dyrekcji. Dodał, że: *W związku z tym, iż dane archiwizowane są poza serwerownią w oddzielnym, specjalnie do tego przygotowanym i wyposażonym miejscu nie jest to sprawa pilna, a jedynie możliwa do realizacji w przypadku pozyskania przez BCO środków finansowych.* (akta kontroli str. 165-171, 244-247, 330-333)

1.5. W Szpitalu została wykonana ocena skutków dla ochrony danych (dalej: *DPIA*), o której mowa w art. 35 RODO, mimo że jest fakultatywna i taka pojedyncza (bieżąca) ocena dotyczyć powinna operacji wiążących się z wysokim ryzykiem. Również Grupa Robocza ds. Ochrony Danych[12] zdecydowanie zalecała dokonanie tej analizy dla operacji przetwarzania trwających przed 25 maja 2018 r.[13] oraz w przypadkach, gdy nie jest jasne, czy wymagana jest DPIA[14]. Analiza ta stanowiła element Polityki, przyjętej 12 grudnia 2018 r. DPIA zawierała elementy wymagane art. 35 ust. 7 RODO, w tym opis operacji przetwarzania i ocenę niezbędności oraz proporcjonalności. IOD wyjaśnił, że wykonał ocenę skutków dla ochrony danych *w celu poszerzenia wiedzy o BCO i przekazaniu dyrekcji informacji o ewentualnych skutkach incydentów mogących wystąpić w procesie przetwarzania danych osobowych.* (akta kontroli str. 144-171)

1.6. Jednym z zadań IOD, w myśl art. 39 ust. 1 lit. b RODO, jest prowadzenie szkoleń personelu uczestniczącego w operacjach przetwarzania danych. Kwestie przeprowadzania szkoleń zostały również określone w § 14 Polityki, gdzie wskazano, że IOD jest odpowiedzialny za szkolenie: każdej osoby, która ma zostać dopuszczona do przetwarzania danych osobowych, wszystkich osób upoważnionych do przetwarzania danych w przypadku zmiany zasad przetwarzania i ochrony danych osobowych lub stwierdzenia istotnych bądź powtarzalnych naruszeń zasad przetwarzania. IOD, powołany na to stanowisko 15 października 2018 r., realizując wymieniony obowiązek, 20 listopada i 3 grudnia 2018 r. przeprowadził grupowe szkolenia z zakresu ochrony danych osobowych, w których wzięły udział 64 osoby. Zakres szkolenia obejmował m.in. definicje dotyczące: RODO i u.o.d.o., legalności przetwarzania danych osobowych, obowiązku informacyjnego, zasad ujawniania oraz powierzenia danych osobowych, zasad bezpiecznego użytkowania sprzętu IT. Ponadto na jego prośbę treść Regulaminu oraz oświadczenia o poufności, zostały 3 stycznia 2019 r. przekazane drogą mailową kierownikom działów, co szerzej opisano w pkt 1.2. niniejszego wystąpienia pokontrolnego. (akta kontroli str. 143, 159-160, 432-445)

---

[12] Grupa ta powołana została na mocy art. 29 dyrektywy 95/46/WE. Była ona niezależnym organem doradczym w zakresie ochrony danych i prywatności, działającym do 25 maja 2018 r.

[13] Dokument pt.: Wytyczne dotyczące oceny skutków dla ochrony danych (DPIA) oraz ustalenia, czy przetwarzanie „z dużym prawdopodobieństwem może powodować wysokie ryzyko", do celów rozporządzenia 2016/679 – https://www.giodo.gov.pl/1520281/id_art/9957/j/pl dostęp z dnia 4 marca 2019 r.

[14] Uznano bowiem, że jest ona *przydatnym narzędziem, które może pomóc administratorom danych w zapewnieniu zgodności z prawem ochrony danych*, chociaż Prezes UODO w komunikacie[14] – wydanym na podstawie art. 35 ust. 4 RODO – wśród rodzajów operacji przetwarzania danych osobowych wymagających oceny skutków przetwarzania dla ich ochrony, nie zawarł danych medycznych przetwarzanych w szpitalach, jako wymagających oceny skutków przetwarzania.

W związku w wejściem w życie przepisów RODO, Szpital zorganizował jedno szkolenie, które odbyło się 20 kwietnia 2018 r. pt. *RODO a dokumentacja medyczna – w praktyce podmiotu leczniczego.* Wzięło w min udział 18 osób z personelu BCO, w tym 16 zatrudnionych jako pielęgniarska kadra kierownicza oraz dwie rejestratorki medyczne. Zakres szkolenia obejmował zagadnienia związane m.in. ze zmianami wprowadzonymi RODO w zakresie przetwarzania danych osobowych i sposobem weryfikacji danych pacjentów przyjmowanych do szpitala, a także z dostępem do informacji o stanie zdrowia pacjenta i udzielonych mu świadczeń opieki zdrowotnej oraz formą jej udostępniania i odpowiedzialnością za naruszenie zasad bezpieczeństwa danych osobowych.

(akta kontroli str. 438-440, 582)

Szpital nie posiadał dokumentacji, potwierdzającej objęcie szkoleniami dotyczącymi RODO pozostałej części personelu, który na 10 stycznia 2019 r. liczył 630 osób. IOD wyjaśnił, że *w ramach pełnienia swoich obowiązków, zajmuje się szkoleniami personelu. Każda nowo zatrudniona osoba przechodzi indywidualne szkolenia z zakresu bezpieczeństwa i ochrony danych osobowych. Dodatkowo zostały zorganizowane cztery grupowe szkolenia potwierdzone listami obecności (łącznie 64 osoby). Planowane są także szkolenia dla kolejnych grup pracowników. Będą to szkolenia przypominające i utrwalające wiedzę z zakresu RODO, które zostaną odnotowane w ewidencji.*

(akta kontroli str. 330-333, 427-437, 582)

Analiza akt osobowych 30 losowo wybranych pracowników BCO[15], zaangażowanych w proces przetwarzania danych medycznych pacjentów wykazała, że:

- wszyscy posiadali udokumentowany fakt zapoznania się z regulacjami wewnętrznymi Szpitala w zakresie ochrony danych osobowych,
- siedmiu uczestniczyło w zorganizowanych przez BCO szkoleniach przeprowadzonych przez podmiot zewnętrzny lub IOD,
- 23 pracowników złożyło oświadczenie o poufności (stanowiące załącznik nr 4 do Polityki), w którym m.in. stwierdzili, że zapoznano ich z przepisami dotyczącymi ochrony danych osobowych, zawartymi w RODO i u.o.d.o. (akta kontroli str. 422)

1.7. Szpital nie zobowiązał się formalnie (np. poprzez deklarację stosowania) do przestrzegania regulacji zawartych w *Kodeksie postępowania dla sektora ochrony zdrowia*[16], dla którego wniosek o przyjęcie został 13 listopada 2018 r. przedłożony[17] PUODO lub pozostałych opracowań związanych z ochroną danych osobowych, takich jak *Przewodnik po RODO w służbie zdrowia*[18] i *Wytyczne dotyczące inspektorów ochrony danych*[19]. Jak wyjaśnił IOD, *BCO formalnie nie zadeklarowało przyjęcia zasad wskazanych w poradnikach RODO, niemniej jednak większość zaleceń tam wskazanych została wprowadzona w życie, czego potwierdzeniem jest stosowanie pseudonimizacji pacjentów przyjętych do Szpitala, wyczytywanie w rejestracji pacjentów po numerach, czy też zamontowanie odpowiednich pojemników na karty gorączkowe itp.*

(akta kontroli str. 330-333)

Zgodnie z wyjaśnieniami Dyrektor Szpitala, BCO nie zostało uznane za operatora usługi kluczowej, o którym mowa w art. 5 ust. 1 ustawy z dnia 5 lipca 2018 r. o krajowym systemie cyberbezpieczeństwa[20]. (akta kontroli str. 342-345)

Stwierdzone nieprawidłowości

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

---

15 20 osób spośród personelu medycznego oraz 10 pracowników administracyjnych.
16 Treść kodeksu została opublikowana na stronie internetowej: www.rodowzdrowiu.pl.
17 Przez Polską Federację Szpitali – podmiot opracowujący ten dokument.
18 Przewodnik został 24 września 2018 r. opublikowany na stronie internetowej Ministerstwa Cyfryzacji.
19 Wytyczne zostały 10 maja 2018 r. opublikowane na stronie internetowej Urzędu Ochrony Danych Osobowych.
20 Dz. U. poz. 1560.

1. Załączniki przyjętej 25 maja 2018 r. Polityki zawierały nieaktualne dane, tj.:
   - we wzorze upoważnienia do przetwarzania danych osobowych, jako podstawę prawną podano art. 37 nieobowiązującej od 25 maja 2018 r. ustawy o ochronie danych osobowych,
   - w załącznikach nr 3 i 4 do Polityki określono, że upoważnienia do przetwarzania danych osobowych oraz do przebywania w obszarze przetwarzania danych są podpisywane m.in. przez ABI, chociaż na jego miejsce został powołany IOD.

   Ponadto aktualizacja Instrukcji, w celu dostosowania jej do przepisów RODO, nastąpiła dopiero 26 listopada 2018 r., tj. po upływie sześciu miesięcy od wejścia w życie tego rozporządzenia, a procedury udostępniania dokumentacji medycznej nie aktualizowano od 23 października 2015 r. Brak tych działań stanowił naruszenie przepisów art. 24 ust. 1 i 2 RODO, zgodnie z którymi do obowiązków ADO należy m.in. poddawanie przeglądom i aktualizacja przyjętych polityk ochrony danych i regulacji wewnętrznych w tym zakresie. Jak wyjaśniła Dyrektor Szpitala, *zarówno nieaktualna podstawa prawna znajdująca się we wzorze upoważnienia do przetwarzania danych osobowych, jak i wskazanie ABI zamiast IOD stanowią omyłkę pisarską*. Ponadto IOD wskazał, że *obecnie trwa aktualizacja procedury związanej z udostępnianiem dokumentacji medycznej Szpitala w związku ze zmianami wynikającymi z prac legislacyjnych w Sejmie dotyczącymi ustawy o zmianie niektórych ustaw zmierzającymi do dostawania obecnie obowiązujących przepisów do zapisów RODO.* (akta kontroli str. 106-125, 298-316, 337-338, 342-345)

2. Rejestr, o którym mowa w art. 30 RODO, został sporządzony 12 grudnia 2018 r., mimo że obowiązek jego opracowania istniał od 25 maja 2018 r. Dyrektor Szpitala wyjaśniła, że BCO *[...] spełniło wytyczne dotyczące powołania IOD. Jednakże powołana na to stanowisko osoba w ramach pełnienia obowiązków nie sporządziła rejestru czynności przetwarzania. W związku z zaistniałym problemem Dyrekcja postanowiła na to stanowisko powołać nową osobę, której powierzono przygotowania i aktualizację dokumentacji związanej z RODO. Rejestr został sporządzony w pierwszej kolejności, jednak zatwierdzony z całą zaktualizowaną Polityką Ochrony Danych w dniu 12 grudnia 2018 r.* (akta kontroli str. 196-213, 342-345)

OCENA CZĄSTKOWA

Szpital wywiązał się z obowiązku opracowania dokumentacji oraz procedur dotyczących ochrony danych osobowych, które nie uwzględniały jednak w pełni przepisów RODO. Ich aktualizacja i dostosowanie do tych regulacji nastąpiło dopiero po sześciu miesiącach od wejścia w życie tego rozporządzenia. Wywiązano się natomiast z obowiązku powołania IOD i terminowego zgłoszenia tego faktu PUODO. Przeprowadzono analizę procesów przetwarzania danych oraz ocenę skutków przetwarzania takich danych, mimo że nie były one obligatoryjne. Pracowników Szpitala zapoznano z regulacjami dotyczącymi ochrony danych osobowych i zagadnieniami dotyczącymi ich bezpieczeństwa oraz obejmowano szkoleniami wszystkie nowo zatrudnione osoby. Prowadzony zaś rejestr czynności przetwarzania zawierał wszystkie wymagane elementy, jednak został opracowany z blisko siedmiomiesięcznym opóźnieniem.

OBSZAR

2. Zapewnienie prawidłowego przetwarzania i ochrony danych osobowych

Opis stanu faktycznego

2.1. Oględziny czterech (z sześciu) funkcjonujących w Szpitalu rejestracji wykazały, że w celu ochrony danych osobowych pacjentów funkcjonowały niżej wymienione rozwiązania.

- Zapewniono, aby w obrębie wzroku pacjenta, znajdującego się przy oknie rejestracji, nie znajdowały się dokumenty zawierających dane osobowe innych pacjentów. Dokumenty osób już zarejestrowanych były na bieżąco przenoszone do gabinetów zabiegowych lub poradni Szpitala. Inne dokumenty medyczne dotyczące pacjenta nie były dostarczane na stanowiska osób rejestrujących. W rejestracji głównej nie zamontowano przesłon pomiędzy poszczególnymi stanowiskami, co może powodować, że osoba znajdująca się przy sąsiednim okienku słyszy informacje podawane przez osobę rejestrującą się obok. IOD wyjaśnił, że: *Pracownicy Centrum zostali przeszkoleni o konieczności zachowania poufności podczas procesu rejestracji*

pacjentów. Rejestracja odbywa się po okazaniu dowodu osobistego pacjenta oraz skierowania od lekarza rodzinnego. Pracownicy rejestracji nie wypowiadali na głos informacji zawierających dane osobowe, przekazując jedynie dane dotyczące dalszego procesu postępowania po zarejestrowaniu się do danej poradni lub gabinetu.

- W trzech rejestracjach[21] poza informacją o treści: *Przy okienku rejestracji może przebywać tylko jedna osoba,* zamieszczoną na każdym z okien rejestracji, nie wprowadzono innych rozwiązań zapewniających odstęp pomiędzy osobami przy okienku a kolejnymi osobami w kolejce, co szerzej opisano w dalszej części wystąpienia, w sekcji *Stwierdzone nieprawidłowości.*
- W głównej rejestracji BCO zamontowano dwa urządzenia, w których osoby oczekujące na rejestrację muszą pobrać odpowiedni numer. Numery te są kolejno wyświetlane na monitorach przy poszczególnych okienkach rejestracji. Po wyświetleniu danego numeru pacjent podchodzi do właściwego stanowiska rejestracji.
- W każdej rejestracji, przy wszystkich jej okienkach, umieszczono klauzule informacyjne (w formie wydruku). Jej treść była zgodna z treścią klauzuli stanowiącej załącznik do Polityki, przyjętej 12 grudnia 2018 r.
- Przy okienkach wszystkich rejestracji zamieszczono informację dla pacjentów o konieczności okazania dowodu osobistego. Identyfikacja 31 pacjentów (rejestrujących się w trakcie prowadzonych oględzin) odbyła się na podstawie dowodów osobistych okazanych rejestratorce.
- Wszystkie monitory znajdujące się w rejestracjach były ustawione w sposób, który uniemożliwiał osobom rejestrującym się wgląd w treści na nich wyświetlane. Dodatkowo na ekranach monitorów umieszczono filtry pozwalający na odczyt wyświetlanej zawartości jedynie osobie znajdującej się bezpośrednio naprzeciw monitora.
- W trzech rejestracjach[22] pacjenci po zarejestrowaniu otrzymywali przygotowane numery (zalaminowane kolorowe karty), zawierające nazwę zakładu lub rodzaju badania, nr gabinetu oraz pierwszą literę imienia i nazwiska lekarza, do którego zostali zarejestrowani.
- W rejestracji głównej BCO pacjenci po zakończonej rejestracji informowani byli, aby udać się na I lub II piętro budynku, gdzie znajdują się gabinety poradni. Tam byli obowiązani do wprowadzenia w specjalnym urządzeniu numeru pesel, po czym otrzymywali wydrukowany numer. Po wyświetleniu się tego numeru na ekranie zamieszczonym przy danym gabinecie pacjenci wchodzili na wizytę (bez wzywania przez lekarza).

(akta kontroli str. 383-387)

We wszystkich trzech objętych oględzinami gabinetach poradni specjalistycznych Szpitala[23] dokumentację pacjentów przechowywano we właściwy sposób. Pacjent wchodzący do gabinetu nie miał bowiem możliwości zapoznania się z danymi osobowymi innych osób oczekujących w kolejce lub tych, którzy odbyli już wizytę. W trakcie oględzin żaden gabinet nie został pozostawiony bez opieki, a w drzwiach do gabinetów nie zostały pozostawione klucze. (akta kontroli str. 388-389)

Oględziny dyżurek pielęgniarskich, sal chorych oraz gabinetów lekarskich na trzech oddziałach szpitalnych[24] wykazały m.in., że:

- na oddziałach znajdowały się 34 sale chorych, dysponujące 107 łóżkami,
- wszyscy 83 zaobserwowani pacjenci nosili na nadgarstku opaski informacyjne zawierające kod kreskowy, nr kartoteki oraz nazwę oddziału i Szpitala,

---

[21] Rejestracja Zakładu Radioterapii, Rejestracja Zakładu Diagnostyki Obrazowej i Rejestracja Pracowni Tomografii Komputerowej i Rezonansu Magnetycznego.

[22] Rejestracje: Zakładu Radioterapii, Zakładu Diagnostyki Obrazowej oraz Pracowni Tomografii Komputerowej i Rezonansu Magnetycznego.

[23] Oględzinami objęto trzy poradnie onkologiczne znajdujące się w pomieszczeniach nr 2.24, 2.07 i 2.08 BCO.

[24] Oględziny przeprowadzono w dyżurkach pielęgniarskich: Oddziałów: Chirurgii Onkologicznej, Onkologii Klinicznej i Radioterapii I.

- na jednym oddziale[25] nie umieszczano kart chorych przy łóżkach pacjentów, a na dwóch pozostałych karty te były umieszczone w sposób uniemożliwiający odczytanie danych na nich zapisanych, bez konieczności ich wyjęcia z zawieszek, w których się znajdowały,
- ruch chorych[26] prowadzony był w dyżurkach pielęgniarskich w miejscach niewidocznych dla osób postronnych,
- w dyżurce pielęgniarskiej jednego z oddziałów[27] podręczna dokumentacja pielęgniarska przechowywana była w zamykanych na klucz gablotach, a w dwóch pozostałych dokumentację tę zgromadzono w szafkach, które nie posiadały możliwości zamknięcia, co szerzej opisano w dalszej części wystąpienia, w sekcji *Stwierdzone nieprawidłowości*,
- dyżurki pielęgniarskie wyposażono w osiem komputerów, z których siedem było uruchomionych – na pięciu z nich pracowały pielęgniarki, a przy dwóch kolejnych nie było nikogo z obsługi, lecz dostęp do systemu operacyjnego tych urządzeń nie został zablokowany, co szerzej opisano w dalszej części wystąpienia, w sekcji *Stwierdzone nieprawidłowości*,
- na oddziałach znajdowało się pięć gabinetów lekarskich, wyposażonych w 34 komputery, z których 27 było uruchomionych – lekarze pracowali na 24 z nich, a na pozostałych trzech[28] włączony był wygaszacz ekranu, ale nie zablokowano dostępu do systemu operacyjnego, co szerzej opisano w dalszej części wystąpienia, w sekcji *Stwierdzone nieprawidłowości*,
- dokumentacja medyczna pacjentów w gabinetach lekarskich dwóch oddziałów była przechowywana w metalowych szafach zamykanych na klucz, a w jednym[29] gromadzono ją na półkach nieposiadających możliwości zamknięcia, co szerzej opisano w dalszej części wystąpienia, w sekcji *Stwierdzone nieprawidłowości*. (akta kontroli str. 378-382)

W ramach oględzin stwierdzono, że na żadnym z trzech oddziałów nie funkcjonuje monitoring wizyjny. Zamontowano go natomiast w dwóch[30] z czterech poddanych oględzinom rejestracji Szpitala. Informacja o funkcjonującym monitoringu (zawierające m.in. dane ADO, kontakt do IOD oraz podstawę prawną przetwarzania) znajdowała się na drzwiach wejściowych do pomieszczeń, w których odbywała się rejestracja. Umieszczenie kamer nie pozwalało na wgląd w dokumenty osób, okazywane podczas procesu rejestracji. Zgodnie z postanowieniami Polityki, zapisy monitoringu przechowywane są przez okres trzech miesięcy, a dostęp do niego ma ubezpieczyciel oraz firma ochrony osób i mienia. Cel, zakres oraz sposób zastosowania monitoringu został określony na piktogramach informujących o jego działaniu oraz w jednym z załączników do przyjętej Polityki. (akta kontroli str. 220, 223-229, 330-333, 378-382)

2.2. Według stanu na 10 stycznia 2019 r. personel działów administracyjnych[31] Szpitala liczył 75 osób. Analiza uprawnień w systemie AMMS[32], jakie zostały nadane 30 osobom z tej grupy wykazała, że odpowiadały one zakresom zadań i obowiązków realizowanych przez tych pracowników. I tak:

- 19 osób nie posiadało dostępu do systemu AMMS, co wynikało z ich zakresów obowiązków (nie realizowali oni zadań wymagających dostępu do danych medycznych pacjentów BCO),
- pięć osób posiadło nadane im uprawnienia w tym systemie, które pozwalały na dostęp do danych medycznych niezbędnych do wykonywania zadań przypisanych tym pracownikom (byli oni zatrudnieni w Dziale Rozliczeń lub Dziale Kontrolingu i Analiz),

---

[25] Oddział Chirurgii Onkologicznej.
[26] Ruch chorych to lista pacjentów danego oddziału wraz z numerem sali, w których przebywają pacjenci.
[27] Oddział Radioterapii I.
[28] Znajdujących się w gabinecie lekarskim Oddziału Chirurgii Onkologicznej.
[29] Oddział Radioterapii I.
[30] Rejestracji głównej BCO i Rejestracji Pracowni Tomografii Komputerowej i Rezonansu Magnetycznego.
[31] Działy: Administracyjno-Eksploatacyjny, Ekonomiczno-Finansowy, Informatyczny, Inwestycji, Kadr i Płac, Organizacyjny, Rozliczeń/Kontrolingu i Analiz, Zamówień Publicznych oraz stanowiska samodzielne w Administracji Szpitala.
[32] System typu HIS (Hospital Information System – rodzaj oprogramowania do obsługi ruchu pacjentów wewnątrz podmiotu leczniczego).

– sześć osób posiadło ograniczony dostęp do danych w systemie AMMS (np. tylko do danych statystycznych lub księgowych apteki bądź wyłącznie do informacji o sprzęcie wykorzystywanym w Szpitalu). (akta kontroli str. 375-377, 427-437)

2.3. Analiza przeprowadzona na próbie 30 (z 204) pielęgniarek i położnych zatrudnionych w Szpitalu[33] wykazała, że wszystkie posiadały dostęp w systemie AMMS do danych medycznych pacjentów tylko na oddziałach szpitalnych, na których świadczyły pracę. Cztery pielęgniarki nie posiadały jednak w swoich aktach osobowych potwierdzenia nadania im przez ADO pisemnych upoważnień do przetwarzania danych osobowych, co szerzej opisano w dalszej części wystąpienia, w sekcji *Stwierdzone nieprawidłowości*.
(akta kontroli str. 362-366, 423-424, 427-437)

W 2008 roku do przetwarzania danych osobowych nie upoważniono żadnej z 11 osób zatrudnionych na stanowiskach: salowa lub sanitariusz. Posiadali oni jedynie *Upoważnienie do przebywania w obszarze przetwarzania danych osobowych*, którego wzór stanowił załącznik do Polityki. Dokument ten zawierał m.in. oświadczenie o poufności, które zobowiązywało danego pracownika m.in. do zachowania w tajemnicy danych osobowych w sytuacji dostępu do nich podczas wykonywania czynności zleconych, zabezpieczenia tych danych przed dostępem osób nieupoważnionych oraz przekazania ich do dyspozycji osób upoważnionych. (akta kontroli str. 421, 427-437)

2.4. Od 25 maja 2018 r. do 10 stycznia 2019 r. Szpital rozwiązał stosunek pracy z 71 osobami. Spośród nich, 29 w trakcie zatrudnienia miało przyznany dostęp do systemów informatycznych, w tym do systemu AMMS. Analiza terminu odebrania uprawnień tym osobom wykazała, że:

– dziewięciu dostęp do systemu AMMS odebrano przed lub w dniu rozwiązania stosunku pracy,
– 16 osobom konto w systemie zablokowano po upływie od jednego do 11 dni od zakończenia zatrudnienia,
– czterem dostęp odebrano po upływie od 133 do 168 dni po dacie rozwiązania stosunku pracy, co szerzej opisano w dalszej części wystąpienia, w sekcji *Stwierdzone nieprawidłowości*. (akta kontroli str. 372-374, 425-426)

2.5. W myśl postanowień umów serwisowych, które obowiązywały w okresie objętym kontrolą[34], Szpital obowiązany był do zgłaszania błędów w działaniu systemu AMMS poprzez witrynę internetową help-desk'u wykonawcy, znajdującą się pod adresem www.hd.asseco.pl, a w przypadku trudności z rejestracją zgłoszenia w tej witrynie, mógł zrealizować je drogą telefoniczną pod wskazanymi numerami telefonów. (akta kontroli str. 446-475, 583-627)

Oględziny sposobu przekazania 50 (ze 169) zgłoszeń serwisowych[35], związanych z błędami lub wadliwym działaniem systemu informatycznego AMMS wykazały m.in., że: [1] wszystkie zgłoszenia serwisowe były przekazywane przez informatyków Szpitala i w dniu oględzin miały status *zamknięty* lub *rozwiązany*; [2] dostęp do archiwalnych zgłoszeń możliwy był po dokonaniu autoryzacji (wpisaniu loginu i hasła) w serwisie internetowym do tego wykorzystywanym; [3] wszystkie zrealizowano drogą elektroniczną z wykorzystaniem serwisu internetowego, który nie został wymieniony w umowach serwisowych; [4] w dziewięciu przypadkach przekazano dane osobowe pacjentów Szpitala, co szerzej opisano w dalszej części wystąpienia, w sekcji *Stwierdzone nieprawidłowości*.
(akta kontroli str. 353-361)

2.6. Szpital w okresie objętym kontrolą posiadał zawarte 99 umów dotyczących powierzenia przetwarzania danych osobowych, w których wystąpił jako podmiot powierzający przetwarzanie danych oraz 18 umów, gdzie wskazano go jako podmiot przetwarzający. Według stanu na 15 stycznia 2019 r. BCO zawarł 88 umów powierzenia przetwarzania takich

---

[33] Dane wg. stanu na 10 stycznia 2019 r.
[34] Umowy: nr 15/ODP/NAS/2017 z 1 czerwca 2017 r. wraz z aneksem z 31 maja 2018 r., nr 19/ODP/NAS/2018 z 6 lipca 2018 r. oraz nr 114/D/DZP-PN/28/2018 z 19 listopada 2018 r., których przedmiotem było m.in. objęcie nadzorem autorskim oraz opieką serwisową oprogramowania InfoMedica/AMMS.
[35] Zgłoszenia te Szpital przekazał od 25 maja 2018 r. do 25 stycznia 2019 r.

danych ze wszystkimi lekarzami zatrudnionymi na kontraktach oraz 11 umów z wykonawcami realizującymi zadania związane m.in. ze: świadczeniem usług informatycznych oraz serwisem oprogramowania, monitorowaniem obiektów BCO, badaniami z zakresu diagnostyki obrazowej, usługami laboratoryjnymi. Dyrektor Szpitala wyjaśniła, że: *Umowy powierzenia przetwarzania danych osobowych z lekarzami kontraktowymi pracującymi w BCO zgodnie z ich treścią są zawierane przez wzgląd na to, że Szpital powierza im dane pacjentów i dane te mogą opuścić BCO np. w przypadkach rozliczenia lekarza przez podmiot zewnętrzny.*

(akta kontroli str. 342-345, 415-419)

Analiza pięciu umów dotyczących powierzenia przez BCO przetwarzania danych osobowych czterem firmom świadczącym usługi serwisowe oraz jednemu lekarzowi, wykazała m.in. że:

- zawierały one postanowienia wymagane art. 28 ust. 3 RODO i stanowiły integralną część umowy na świadczenie usług zawartej z danym podmiotem zewnętrznym,
- w czterech z nich zakres danych osobowych powierzonych przez Szpital podmiotowi zewnętrznemu wynikał z rodzaju usług, które zgodnie z umową miał na rzecz BCO realizować wykonawca,
- jedna umowa dotyczyła jedynie powierzenia danych osobowych pracowników Szpitala, podczas gdy wykonawca i jego podwykonawca przetwarzał również dane pacjentów, co szerzej opisano w dalszej części wystąpienia, w sekcji *Stwierdzone nieprawidłowości.*

(akta kontroli str. 446-524)

2.7. Jednym z załączników do Polityki była *Instrukcja postępowania z incydentami*, w której określono m.in.: [1] katalog podatności i incydentów zagrażających bezpieczeństwu danych osobowych; [2] sposób postępowania w przypadku wystąpienia któregoś z takich zdarzeń; [3] wynikający z art. 33 ust. 5 RODO obowiązek dokumentowania wszystkich naruszeń danych osobowych, ich okoliczności, skutków oraz podjętych działań zaradczych na formularzu rejestracji incydentu[36]. Zgodnie z przepisem art. 33 ust. 1 u.o.d.o. w instrukcji wskazano obowiązek zgłoszenia PUODO, w terminie 72 godzin, każdego przypadku naruszenia danych osobowych, skutkującego ryzykiem naruszenia praw lub wolności osób fizycznych. (akta kontroli str. 195)

Analiza zapisów w rejestrze naruszeń ochrony danych osobowych (wg. stanu na 26 lutego 2019 r.), wykazała, że w okresie objętym kontrolą odnotowano w nim 11 incydentów, w tym: [1] jeden[37] związany z awarią sprzętu informatycznego, w wyniku którego przez 20 godzin nie był możliwy dostęp do większości systemów Szpitala dla 90% załogi BCO wykorzystującej w swojej pracy komputer (jak wskazano w zapisach rejestru, żadne dane nie zostały utracone); [2] dziewięć związanych z udostępnieniem podmiotowi zewnętrznemu danych osobowych 29 pacjentów (incydent ujawniony w trakcie przeprowadzania oględzin w ramach niniejszej kontroli NIK); [3] jeden dotyczący pożaru w dniu 19 lutego 2019 r. archiwum znajdującego się w remontowanej części Szpitala, którego przyczyną była awarii sieci elektrycznej. (akta kontroli str. 353-361, 410-413, 420)

Spośród wszystkich 11 incydentów, tylko jeden (dotyczący skutków pożaru archiwum) został zgłoszony do PUODO, gdyż – jak wskazał IOD – w jego opinii jako jedyny dotyczył naruszenia określonego w art. 33 ust. 1 RODO, skutkującego ryzykiem naruszenia praw lub wolności osób fizycznych. Zgłoszenie to zawierało wszystkie elementy wymienione w art. 33 ust. 3 tego rozporządzenia, jednak przekazane zostało z naruszeniem terminu do jego złożenia, co szerzej opisano w dalszej części wystąpienia, w sekcji *Stwierdzone nieprawidłowości.* (akta kontroli str. 15-22, 337-338, 410-413, 420)

W rejestrze skarg i wniosków BCO za okres od 25 maja 2018 r. do 5 marca 2019 r. nie odnotowano skarg i wniosków, które dotyczyłyby nieprawidłowości związanych z ochroną danych osobowych pacjentów. (akta kontroli str. 321)

---

[36] Formularz nosił nazwę: Rejestr naruszeń ochrony danych osobowych oraz incydentów bezpieczeństwa danych.

[37] Z 27 sierpnia 2018 r.

2.8. W okresie objętym kontrolą w Szpitalu funkcjonowały procedury dotyczące udostępniania danych osobowych, opracowane 30 czerwca 2011 r. i aktualizowane w latach 2014–2015. W myśl tych regulacji oraz zgodnie z przepisem art. 24 ust. 1 u.o.p.p., dokumentację medyczną udostępnia się pacjentowi lub jego przedstawicielowi ustawowemu bądź osobie upoważnionej przez pacjenta oraz podmiotom określonym w ust. 3 powołanego przepisu. W procedurach wewnętrznych wskazano też, że udostępnienie tej dokumentacji na zewnątrz Szpitala następuje w przypadku osobistego zgłoszenia się pacjenta lub przedstawienia upoważnienia w jego imieniu. Regulacje wewnętrzne BCO nakładały obowiązek prowadzenia ewidencji każdego przypadku udostępnienia dokumentacji medycznej instytucji lub innej osobie niż pacjent. (akta kontroli str. 298-302)

Według stanu na 5 lutego 2019 r. w prowadzonym przez Szpital wykazie odnotowano 307 przypadków udostępnienia dokumentacji medycznej osobom i podmiotom zewnętrznym (nie prowadzono ewidencji spraw, w przypadku których odmówiono udostępnienia dokumentacji). Wśród nich od 25 maja 2018 r. do 5 lutego 2019 r. odnotowano 28 przypadków dotyczących udostępnienia tej dokumentacji osobom fizycznym innym niż pacjent, którego udostępniana dokumentacja medyczna dotyczyła oraz 10 przypadków udostępnienia jej komercyjnym instytucjom ubezpieczeniowym. Analiza prawidłowości udostępnienia dokumentacji w odniesieniu do wszystkich tych przypadków wykazała, że:

- udostępnianie następowało w wyodrębnionym Punkcie Obsługi Pacjenta, znajdującym się w pomieszczeniu rejestracji głównej Szpitala,
- w 27 (z 28) przypadkach dokumentacja medyczna została udostępniona osobom, które posiadały upoważnienie pacjenta do dostępu do tej dokumentacji na podstawie wniosków o jej udostępnienie, określonych w regulacjach wewnętrznych BCO,
- we wszystkich 10 przypadkach instytucje ubezpieczeniowe, którym udostępniono dokumentację medyczną, posiadały upoważnienie pacjenta do dostępu do tej dokumentacji,
- w jednym przypadku udostępniono dokumentację medyczną pacjenta osobie, która nie przedstawiła upoważnienia w tym zakresie, co szerzej opisano w dalszej części wystąpienia, w sekcji *Stwierdzone nieprawidłowości.* (akta kontroli str. 346-352)

2.9. Regulacje dotyczące ochrony danych przed ich utratą w wyniku awarii, błędów lub nieuprawnionej modyfikacji zostały opisane w Regulaminie oraz w Instrukcji zarządzania systemem informatycznym służącym do przetwarzania danych osobowych[38] (dalej: *Instrukcja*). W dokumentach tych określono m.in. zasady: [1] bezpiecznego użytkowania sprzętu IT, dysków i programów; [2] zarządzania uprawnieniami, w tym procedurę rozpoczęcia, zawieszenia i zakończenia pracy; [3] uwierzytelniania w systemach i zarządzania dostępem do nich; [4] zabezpieczenia dokumentacji papierowej z danymi osobowymi; [5] korzystania z Internetu; [6] korzystania z poczty elektronicznej i ochrony antywirusowej; [7] tworzenia, przechowywania i testowania kopii bezpieczeństwa. Ponadto określono sposób postępowania w przypadku naruszenia ochrony danych osobowych oraz obowiązek zachowania poufności i ochrony danych osobowych.
(akta kontroli str. 303-316, 322-329)

Oględziny jedynej serwerowni Szpitala wykazały, m.in. że właściwie: [1] zabezpieczono dostęp do tego pomieszczenia, stosując drzwi metalowe oraz rolety antywłamaniowe we wszystkich dwóch oknach; [2] zamontowano system alarmowy oraz przeciwpożarowy; [3] w pomieszczeniu umieszczono gaśnicę oraz układ klimatyzacji; [4] w celu zapobieżenia zalaniu wszystkie urządzenia znajdowały się na tzw. podłodze technicznej, tj. powyżej poziomu posadzki; [5] na wypadek czasowego zaniku zasilania zastosowano układy podtrzymujące napięcie UPS; [6] wszystkie urządzenia informatyczne zamontowano w specjalnie do tego przystosowanych szafach typu RACK. (akta kontroli str. 367-371)

---

[38] Instrukcja została zatwierdzona 21 sierpnia 2017 r. przez Dyrektora Szpitala. Zaktualizowano ją 26 listopada 2018 r. w zakresie dostosowania do przepisów RODO.

Kopie zapasowe baz danych Szpitala, w myśl przepisów § 20 ust. 2 pkt 12 lit. b rozporządzenia KRI oraz postanowień Instrukcji, były przechowywane w specjalnie do tego przystosowanym pomieszczeniu znajdującym się w innej niż serwerownia części budynku, na jego drugiej kondygnacji. Oględziny tego pomieszczenia wykazały, że zastosowano w nim te same rozwiązania zabezpieczające co w serwerowni, za wyjątkiem zewnętrznych rolet antywłamaniowych. (akta kontroli str. 367-371)

W trakcie oględzin serwerowni oraz pomieszczenia, w którym przechowywano kopie zapasowe baz danych Szpitala stwierdzono pozostawione w nich kartonowe pudła oraz urządzenia informatyczne, które nie były podłączone do infrastruktury, co szerzej opisano w dalszej części wystąpienia, w sekcji *Stwierdzone nieprawidłowości*.
(akta kontroli str. 367-371, 582)

Oględziny 30 komputerów stacjonarnych Szpitala, w tym 20 wykorzystywanych na oddziałach Szpitala przez lekarzy, pielęgniarki i położne oraz 10 użytkowanych w dziale Administracji Szpitala, wykazały m.in., że:

- na wszystkich zainstalowany był program antywirusowy, posiadający aktualną wersję bazy sygnatur wirusów,
- w żadnym nie zostały zablokowane porty USB, umożliwiając podłączenie do nich nośników pamięci i kopiowanie danych,
- na wszystkich użytkownicy posiadali ograniczone uprawnienia w systemie operacyjnym, które nie pozwalały na wprowadzanie zmian w konfiguracji tych urządzeń oraz instalację oprogramowania,
- 18 zarządzanych było domenowo, a 12 funkcjonowało poza tym systemem,
- 25 wykorzystywanych było do przetwarzania danych medycznych w systemie AMMS, a pięć do przetwarzania danych osobowych pracowników Szpitala,
- dostęp do systemu operacyjnego wymagał podania loginu i hasła. Na 12 komputerach z tych samych danych uwierzytelniających korzystało jednak kilku użytkowników, a hasła nie posiadały odpowiedniej złożoności i nie podlegały okresowej zmianie, co szerzej opisano w dalszej części wystąpienia, w sekcji *Stwierdzone nieprawidłowości*.
(akta kontroli str. 390-409)

Jak wyjaśnił Kierownik Działu Informatyki Szpitala, do tworzenia kopii bez danych wykorzystywano specjalistyczne narzędzia, a *Archiwizacja uruchamiana jest za pomocą skryptów raz dziennie* i są nią objęte wszystkie bazy danych BCO. Dodał, że: *Jesteśmy w stanie przywrócić cały host na inną maszynę w przypadku awarii. Dodatkowo raz w tygodniu kopie baz danych migrują na dodatkowy serwer archiwizujący znajdujący się w odrębnej lokalizacji, do której mają dostęp tylko określone osoby.* Wyjaśnił także, że sprawdzanie kopii bazy danych przeprowadzane jest przy użyciu narzędzi informatycznych raz w miesiącu, a produkcyjna baza danych jest odtwarzana na platformie testowej raz na trzy miesiące. (akta kontroli str. 334-336, 339-341)

IOD wyjaśnił, że w Szpitalu stosowana jest pseudonimizacja danych osobowych pacjentów. Jako przykład podał opaski noszone przez pacjentów BCO, na których zamieszcza się jedynie kod kreskowy oraz nr historii choroby, na podstawie których – przy wykorzystaniu odpowiednich narzędzi – jest możliwe ustalenie tożsamości pacjentów.
(akta kontroli str. 330-333)

Stwierdzone nieprawidłowości

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

1. Przetwarzanie, w tym przechowywanie danych o pacjentach w niżej wymienionych przypadkach odbywało się bez wdrożenia lub przy niewłaściwym wdrożeniu środków technicznych i organizacyjnych, o których mowa w art. 24 ust. 1 RODO.

   a) W trzech rejestracjach[39], poza informacją o treści: *„Przy okienku rejestracji może przebywać tylko jedna osoba"*, zamieszczonej na każdym z okien rejestracji,

[39] Rejestracje Zakładów: Radioterapii i Diagnostyki Obrazowej oraz Pracowni Tomografii Komputerowej i Rezonansu Magnetycznego.

nie wprowadzono innych rozwiązań zapewniających odpowiedni odstęp pomiędzy osobami przy okienku, a kolejnymi osobami w kolejce. W konsekwencji w trakcie oględzin pacjenci znajdujący się w kolejce nie stosowali się do zasady dotyczącej przebywania tylko jednej osoby przy oknie rejestracji, tzn. stały w bezpośredniej odległości za osobą, która aktualnie się rejestrowała. Nikt z personelu szpitala nie zwracał się również do pacjentów w kolejce z prośbą o stosowanie się do tej zasady. Taki sposób rejestracji pacjentów mógł nie zapewniać należytej ochrony danych osobowych, w szczególności nie odpowiadał dobrym praktykom podanym w *Przewodniku po służbie zdrowia*[40], aby dążyć do minimalizacji ryzyka ujawnienia informacji osobom postronnym w procesie rejestracji, wyznaczając obszar, w którym może przebywać wyłącznie obsługiwany pacjent. IOD wyjaśnił, że: *Pracownicy Centrum zostali przeszkoleni o konieczności zachowania poufności podczas procesu rejestracji pacjentów. Rejestracja odbywa się po okazaniu dowodu osobistego pacjenta oraz skierowania od lekarza rodzinnego.* (akta kontroli str. 330-333, 383-387)

b) W dwóch (z trzech) dyżurkach pielęgniarskich oddziałów[41] podręczna dokumentacja pielęgniarska, zawierająca dane osobowe pacjentów, przechowywana była w niezamykanych pomieszczeniach, w których możliwości zamknięcia nie posiadały również szafki z danymi osobowymi pacjentów. Podobna sytuacja miała miejsce w jednym[42] z trzech poddanych oględzinom gabinetów lekarskich, w których dokumentację medyczną przechowywano na półkach nieposiadających możliwości zamknięcia. Zgodnie z art. 23 ust. 2 u.o.p.p., dane zawarte w dokumentacji medycznej podlegają ochronie. Ponadto zgodnie z postanowieniami pkt 4 Regulaminu, ochrona przed wglądem osób nieupoważnionych lub kradzieżą dokumentacji papierowej, zawierającej dane osobowe, polega m.in. na zabezpieczeniu (zamykaniu) dokumentów w szafach, biurkach i pomieszczeniach podczas nieobecności w trakcie godzin pracy. IOD wyjaśnił, że: *Dokumentacja znajdowała się w pokoju lekarskim, do którego dostęp mają tylko osoby upoważnione. Pokój zamykamy jest na klucz, co stanowi główne zabezpieczenie znajdującej się tam dokumentacji.* Dodał, że: *Do dyżurek pielęgniarskich mają wstęp tylko osoby upoważnione. Dokumentacja pozostaje pod nadzorem personelu, osoby nieupoważnione nie mają do niej dostępu.* Występowanie czasowych przypadków pozostawiania dyżurek pielęgniarskich bez nadzoru został potwierdzony w trakcie oględzin – w chwili rozpoczęcia tych czynności w dyżurce pielęgniarskiej Oddziału Radioterapii I nie było nikogo z personelu pielęgniarskiego tego oddziału, a pomieszczenie to nie posiadało możliwości zamknięcia.

(akta kontroli str. 322-333, 378-382)

2. Personel Szpitala nie stosował się do pkt 2 ppkt 10 Regulaminu, zgodnie z którym przed czasowym opuszczeniem stanowiska pracy, użytkownik zobowiązany jest wywołać blokowany hasłem wygaszacz ekranu lub wylogować się z systemu operacyjnego. Przeprowadzone oględziny wykazały bowiem, że nie zablokowano żadnego z pięciu komputerów[43], przy których nie było obecnych pracowników. W jednej zaś z dyżurek pielęgniarskich[44], w której w chwili rozpoczęcia oględzin nie było personelu, a na uruchomionym i niezablokowanym komputerze w lokalizacji *Pulpit*, w folderze *Moje dokumenty* znajdowały się pliki tekstowe zawierające nazwiska i numery sal pacjentów oddziału oraz informacje dotyczące ich diety. IOD wyjaśnił, że: *W BCO wprowadzona została polityka czystego biurka i czystego ekranu. Zasady bezpiecznego użytkowania sprzętu udostępnione zostały personelowi w formie papierowej, a także elektronicznej w zakładce RODO dla pracowników w sieci ISO Centrum. Niewylogowanie mogło być spowodowane stresem pracownika związanym z kontrolą przeprowadzaną w danej*

---

40 Przewodnik po RODO dla służby zdrowia, będący efektem prac zespołu zadaniowego ds. ochrony zdrowia, działającego w ramach Grupy Roboczej ds. Ochrony Danych Osobowych, utworzonej w Ministerstwie Cyfryzacji, opublikowany 24 września 2018 r. na stronie http://www.rpp.gov.pl/dla-pacjenta/poradniki/przewodnik-po-rodo-w-sluzbie-zdrowia/, dostęp z dnia 26 lutego 2019 r.

41 Oddziały Chirurgii Onkologicznej i Onkologii Klinicznej.

42 Oddział Radioterapii I.

43 Dwa z tych komputerów znajdowały się w dyżurkach pielęgniarskich Oddziałów: Onkologii Klinicznej i Radioterapii I, a trzy w gabinecie lekarskim Oddziału Chirurgii Onkologicznej.

44 Oddział Radioterapii I.

chwili. Natomiast w odniesieniu do niezablokowanych komputerów pozostawionych w gabinetach lekarskich wskazał, że: *Wytłumaczeniem zaistniałej sytuacji mogło być jedynie nagłe wezwanie lekarzy na oddział i kierowanie się zasadą nadrzędności zdrowia i życia ludzkiego nad ochroną danych osobowych.* (akta kontroli str. 322-333, 390-409)

3. Cztery pielęgniarki (z 30[45] poddanych analizie) posiadały dostęp i przetwarzały dane medyczne pacjentów w systemie AMMS, bez pisemnego upoważnienia do przetwarzania danych osobowych, wymaganych w § 12 Polityki. Nie odpowiadało to wymogom art. 32 ust. 4 RODO, aby administrator podjął działania w celu zapewnienia, by każda osoba fizyczna, działająca z jego upoważnienia, która ma dostęp do danych osobowych, przetwarzała je wyłącznie na jego polecenie. Dyrektor Szpitala wyjaśniła, że: *Pracownicy są upoważnieni, zostały im nadane indywidualne identyfikatory do logowania się w systemach komputerowych. Trwa przegląd akt pracowniczych w poszukiwaniu ww. upoważnień.* Przed zakończeniem kontroli NIK (1 marca 2019 r.) wydano brakujące upoważnienia do przetwarzania danych osobowych.
(akta kontroli str. 342-345, 362-366, 423-424, 427-437, 628-635)

4. Konta użytkownika w systemie AMMS, czterech (z 29) byłych pracowników Szpitala, zostały zablokowane po upływie od 133 do 168 dni po dacie rozwiązania z nimi stosunku pracy. Stanowiło to naruszenie § 20 ust. 2 pkt 5 rozporządzenia KRI, zgodnie z którym należy podejmować działania polegające na bezzwłocznej zmianie uprawnień, w przypadku zmiany zadań osób zaangażowanych w proces przetwarzania informacji. Kierownik Działu Informatyki wyjaśnił, że uprawnienia do systemu AMMS odebrano tym czterem pracownikom z opóźnieniem z powodu przeoczenia. Dodał, że: *Były pracownik, który piastował funkcję ABI, a następnie IOD nie dokonał tego w należytym czasie. Błąd został wychwycony przy cyklicznej weryfikacji uprawnień.*
(akta kontroli str. 339-341, 372-374, 425-426)

5. W dziewięciu (z 50) objętych analizą zgłoszeniach serwisowych dotyczących systemu AMMS, przesłanych od 25 maja 2018 r. do 29 stycznia 2019 r. podwykonawcy podmiotu świadczącego usługi serwisu, zamieszczono dane osobowe 29 pacjentów Szpitala, w tym w pięciu zgłoszeniach dane medyczne, zawierające zakres lub wyniki badań wykonanych pięciu pacjentom. Było to niezgodne z przepisem art. 24 ust 2 u.o.p.p., w myśl którego do przetwarzania danych zawartych w dokumentacji medycznej, w celu utrzymania i zapewnienia bezpieczeństwa systemu teleinformatycznego, gdzie przetwarzana jest dokumentacja, są uprawnione inne osoby wykonujące czynności związane z utrzymaniem systemu teleinformatycznego, w którym przetwarzana jest dokumentacja medyczna na podstawie upoważnienia administratora danych. Tymczasem Szpital z podmiotem świadczącym usługi serwisu, któremu przekazano dane pacjentów, nie zawarł umowy powierzenia przetwarzania danych, a Dyrektor BCO nie wydał temu podmiotowi upoważnienia w tym zakresie. Dyrektor Szpitala wyjaśniła, że podmiot świadczący usługi serwisu *(...) został wskazany w SIWZ jako podwykonawca ASSECO Poland S.A., na co zamawiający wyraził zgodę*. Analiza zapisów umowy i jej załączników wykazała, że nazwa podmiotu, który świadczył usługi serwisu pojawiła się jedynie w formularzu oferty (stanowiącym załącznik nr 1 do umowy), gdzie zapisano *zamierzamy powierzyć firmie (...) podwykonawstwo części zamówienia w zakresie serwisu*. Umowa ta nie zawierała szczegółowych danych dotyczących zakresu prac powierzonych podwykonawcy. (akta kontroli str. 342-345, 353-361, 446-470)

   Ponadto wszystkie 50 objętych badaniem zgłoszeń serwisowych dotyczących systemu AMMS realizowanych było drogą elektroniczną z wykorzystaniem serwisu internetowego, który nie został wymieniony w umowach serwisowych obowiązujących od 25 maja 2018 r. do 30 stycznia 2019 r. Kierownik Działu Informatyki wyjaśnił, że: *Zgłoszenia serwisowe przekazywane były do podwykonawcy wskazanego przez firmę Asseco Poland S.A. w specyfikacji istotnych warunków zamówienia. Odnosząc się do wątpliwości dotyczących sposobu przekazywania informacji do podwykonawcy (...) zostanie to ujęte*

[45] Spośród 227 pielęgniarek i położnych zatrudnionych w BCO na 10 stycznia 2019 r.

w aneksie do umowy, w którym wyszczególnione zostaną możliwe sposoby zgłaszania błędów w działaniu systemu AMMS by nie dochodziło do podobnych wątpliwości.
(akta kontroli str. 242-252, 353-361, 452-453, 446-475, 583-627)

6. W jednej[46] z pięciu objętych badaniem umów powierzenia przetwarzania danych osobowych niewłaściwie wskazano zakres danych, jakie będzie przetwarzał podmiot zewnętrzny. Umowa, w związku z którą powierzono przetwarzanie danych osobowych, dotyczyła objęcia opieką serwisową systemu AMMS i związanego z tym dostępu do danych medycznych pacjentów Szpitala. Zakres danych, jaki został wskazany w umowie powierzenia, dotyczył jedynie dostępu do danych osobowych pracowników Szpitala. W myśl przepisów art. 28 ust. 3 RODO, przetwarzanie przez podmiot przetwarzający odbywa się na podstawie umowy lub innego instrumentu prawnego, który wiąże podmiot przetwarzający i administratora oraz określa m.in. rodzaj danych osobowych oraz kategorie osób, których dane dotyczą. Dyrektor Szpitala wyjaśniła, że *Umowa powierzenia danych osobowych z dnia 19 listopada 2018 r. w związku z umową główną nr 114/D/DZP-PN/28/2018 zostanie poprawiona, nastąpiła omyłka pisarska.* (akta kontroli str. 342-345, 446-524)

7. Dane medyczne jednego (z 28) pacjenta przekazano osobie, która nie przedstawiła stosownego upoważnienia w tym zakresie. Dokumentację medyczną pełnoletniego pacjenta 30 maja 2018 r. udostępniono bowiem, na podstawie listu otrzymanego przez Szpital od osoby podającej się za matkę pacjenta. Było to sprzeczne z regulacjami wewnętrznymi BCO, wprowadzonymi instrukcją *Udostępniania dokumentacji medycznej.* W myśl jej postanowień, udostępnianie dokumentacji na zewnątrz Szpitala odbywa się na wniosek osoby upoważnionej przez pacjenta, po przedstawieniu upoważnienia w jego imieniu. Dyrektor Szpitala wyjaśniła, że: *Dokumentacja medyczna pacjenta o numerze choroby 3603/97 była przeznaczona do utylizacji zgodnie z upływem 20-letniego terminu jej przechowywania. W związku z tym Dyrekcja przychyliła się do prośby matki pacjenta na udostępnienie dokumentacji medycznej z uwagi na wskazanie jej w dokumentacji jako osoby do kontaktu.* (akta kontroli str. 342-352)

8. Wbrew regulacjom pkt 2 ppkt 1 i 4 Regulaminu, dostęp do systemu operacyjnego na 12 (z 30) poddanych oględzinom komputerach był realizowany przez kilku użytkowników (pracowników BCO), na podstawie tych samych danych uwierzytelniających (tego samego loginu i hasła). Stosowane zaś w tych przypadkach hasła nie posiadały odpowiedniej złożoności i nie podlegały okresowej zmianie. W myśl postanowień pkt 2 ppkt 5 Regulaminu, zabrania się pracy wielu użytkowników na wspólnym koncie. Dodatkowo regulacje te wprowadzają obowiązek posiadania przez użytkownika indywidualnego identyfikatora, którego nie może udostępniać innym osobom, aby mogły one pracować na jego koncie w systemie operacyjnym. Kierownik Działu Informatyki wyjaśnił, że: *Niektóre z komputerów nie zostały podłączone do systemu Active Directory. Na tych komputerach jest utworzone jedno lokalne konto bez uprawnień administracyjnych. Zostało to wdrożone przez poprzedni personel działu informatycznego w celu ułatwienia logowania do systemu medycznego. Na części komputerów zostały już wykonane prace konfiguracyjne, planowane jest podłączenie wszystkich stacji roboczych do kontrolera domeny.*
(akta kontroli str. 248-255, 339-341, 390-409)

9. Zgłoszenie do PUODO incydentu dotyczącego pożaru, jaki miał miejsce 19 lutego 2019 r. w archiwum Szpitala, znajdującym się w remontowanej jego części, nastąpiło 26 lutego 2019 r., tj. po upływie siedmiu dni od daty wystąpienia. Było to sprzeczne z przepisem art. 33 ust. 1 RODO, zgodnie z którym w przypadku naruszenia ochrony danych osobowych, administrator bez zbędnej zwłoki, nie później niż w terminie 72 godzin po stwierdzeniu naruszenia, zgłasza je organowi nadzorczemu (PUODO). IOD wyjaśnił, że: *Incydent został zanotowany w pierwszej kolejności w prowadzonym rejestrze zdarzeń. W związku z tym, iż trwały prace nad ustaleniem jakiego typu dokumentacja znajdowała się w tej części składnicy dokumentów i czy mogła się tam*

[46] Umowa ta stanowiła załącznik do umowy serwisowej nr 114/D/DZP-PN/28/2018 z 19 listopada 2018 r.

znajdować dokumentacja nieprzeznaczona do utylizacji zgodnie z terminami retencji danych po wstępnych ustaleniach zgłoszenie zostało dokonane w dniu 26 lutego 2019 r.
(akta kontroli str. 15-22, 337-338, 410-413, 420)

10. W trakcie oględzin, w pomieszczeniu serwerowni oraz w miejscu, w którym przechowywano kopie zapasowe baz danych Szpitala, znajdowały się kartonowe pudła oraz urządzenia informatyczne niepodłączone do infrastruktury. Część z tych przedmiotów była łatwopalna. Serwerownia, z uwagi na prawdopodobieństwo wystąpienia przegrzania macierzy dyskowych lub przepięcia elektrycznego, nie powinna być miejscem do ich składowania. Kierownik Działu Informatyki wyjaśnił, że: *W kartonach przechowywane były podzespoły komputerowe i serwerowe. Kartony służyły do utrzymania porządku w serwerowni. Zostanie to przeniesione w odpowiednie miejsce, by nie stwarzało zagrożenia pożarowego.*

    Po zakończeniu oględzin przedmioty te zostały usunięte z serwerowni i pomieszczenia, w którym przechowywano kopie zapasowe. (akta kontroli str. 339-340, 367-371, 582)

OCENA CZĄSTKOWA

Najwyższa Izba Kontroli ocenia negatywnie podjęte przez Szpital działania w celu zapewnienia prawidłowego przetwarzania i ochrony danych osobowych.

IV. Wnioski

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

Wnioski

1. Bieżące aktualizowanie regulacji wewnętrznych dotyczących ochrony danych osobowych oraz bezpieczeństwa informacji.
2. Wdrożenie odpowiednich środków technicznych i organizacyjnych zapewniających ochronę danych osobowych oraz minimalizację ryzyka ujawnienia informacji osobom postronnym w procesie rejestracji i podczas przechowywania papierowej dokumentacji medycznej pacjentów w dyżurkach pielęgniarskich i gabinetach lekarskich na oddziałach Szpitala.
3. Zobowiązanie i egzekwowanie od personelu BCO przestrzegania zasad określonych w Regulaminie, dotyczących blokowania dostępu do systemów operacyjnych komputerów.
4. Dokumentowanie udzielania upoważnień do przetwarzania danych osobowych, w sposób określony w regulacjach wewnętrznych.
5. Bezzwłoczne odbieranie uprawnień w systemach informatycznych byłym pracownikom Szpitala.
6. Dokonywanie zgłoszeń serwisowych w sposób zapewniający ochronę danych osobowych pacjentów oraz zgodny z postanowieniami umów zawartych w tym zakresie.
7. Określanie w umowie[47] powierzania przetwarzania danych osobowych właściwego zakresu danych, jakie będą na jej podstawie przetwarzane oraz wskazanie podmiotu (podwykonawcy), który będzie tego dokonywał.
8. Udostępnianie dokumentacji z zachowaniem przyjętych regulacji wewnętrznych w tym zakresie.
9. Nadanie wszystkim użytkownikom komputerów indywidualnych danych do autoryzacji w systemach operacyjnych oraz wprowadzenie rozwiązań uniemożliwiających pracę kilku osób na jednym koncie użytkownika.
10. Zgłaszanie PUODO incydentów z zachowaniem terminów określonych w art. 33 ust. 1 RODO.

[47] Stanowiącej załącznik do umowy serwisowej nr 114/D/DZP-PN/28/2018 z 19 listopada 2018 r.

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 uwag 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, 28 marca 2019 r.

Kontroler:

Paweł Tołwiński
specjalista kontroli państwowej

.....
podpis

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

.....
podpis