NAJWYŻSZA IZBA KONTROLI
Delegatura w Lublinie

LLU.410.003.04.2019

Pan Marek Kos
Dyrektor
Samodzielnego Publicznego
Zakładu Opieki Zdrowotnej
w Kraśniku
ul. Chopina 13, 23-200 Kraśnik

# WYSTĄPIENIE POKONTROLNE

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

NAJWYŻSZA IZBA KONTROLI
Delegatura w Lublinie
ul. Okopowa 7, 20-022 Lublin
T +48 81 461 31 20, F +48 81 461 31 11
llu@nik.gov.pl
Adres korespondencyjny: Skr. poczt. P-112, 20-001 Lublin 1

# Dane identyfikacyjne

| | |
|---|---|
| Jednostka kontrolowana | Samodzielny Publiczny Zakład Opieki Zdrowotnej w Kraśniku ul. Chopina 13, 23-200 Kraśnik (dalej „SPZOZ", „Szpital") |
| Kierownik jednostki kontrolowanej | Marek Kos – Dyrektor SPZOZ w Kraśniku od dnia 14.05.2013 r. |
| Zakres przedmiotowy kontroli | 1. Opracowanie wymaganej dokumentacji oraz procedur związanych z ochroną przetwarzanych danych osobowych.<br>2. Zapewnienie prawidłowego przetwarzania i ochrony danych osobowych. |
| Okres objęty kontrolą | Od 25 maja 2018 r. 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 kontrole | Najwyższa Izba Kontroli Delegatura w Lublinie |
| Kontrolerzy | Artur Bokiniec, główny specjalista kontroli państwowej, upoważnienie do kontroli nr LLU/46/2019 z 08.03.2019 r.<br>Mirosław Bortacki, główny specjalista kontroli państwowej, upoważnienie do kontroli nr LLU/53/2019 z 19.03.2019 r.<br>(akta kontroli tom I str. 1-5) |

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

# Ocena ogólna[2] kontrolowanej działalności

**OCENA OGÓLNA**

W Szpitalu dane osobowe w okresie od 25 maja 2018 r. do 9 kwietnia 2019 r., nie były w pełni prawidłowo chronione i przetwarzane. SPZOZ zgodnie z rozporządzeniem Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (ogólne rozporządzenie o ochronie danych)[3] opracował i wdrożył dokumentację oraz procedury dotyczące ochrony danych osobowych. Wyznaczono Inspektora Ochrony Danych (IOD) i terminowo zgłoszono ten fakt Prezesowi Urzędu Ochrony Danych Osobowych (PUODO). W SPZOZ przeprowadzono także analizę procesów przetwarzania danych oraz wykonano oceny skutków ich przetwarzania. Dokumentację medyczną pacjentów udostępniano jedynie uprawnionym podmiotom, a analizowane umowy powierzenia przetwarzania danych osobowych spełniały wymagania określone w art. 28 RODO. Szpital zapewnił także odpowiednie zabezpieczenia serwerowni, w której przechowywano dane osobowe (przetwarzane elektronicznie).

Zorganizowane szkolenia związane z ochroną danych osobowych w związku z wejściem w życie RODO dotyczyły jednie 52,5% pracowników. Nie wszystkich pracowników Szpitala zapoznano również z regulacjami dotyczącymi ochrony danych osobowych oraz z zagadnieniami dotyczącymi bezpieczeństwa. Na dwóch oddziałach szpitalnych stwierdzono niewłaściwe zabezpieczenie przechowywanej dokumentacji medycznej oraz pozostawienie komputera bez odpowiedniego zabezpieczenia. Wystąpiły również przypadki umożliwienia dostępu do systemów informatycznych Szpitala pracownikom, dla których nie nadano wymaganych upoważnień do przetwarzania danych osobowych. Ponadto stwierdzono przypadki nieuprawnionego wydania upoważnień do przetwarzania danych medycznych dla personelu pomocniczego Szpitala (sanitariusze szpitalni, personel gospodarczy, kierowcy) oraz przekazania dostawcy oprogramowania danych osobowych i medycznych pacjentów. Szpital zminimalizował ryzyko dotyczące utraty danych medycznych oraz nieuprawnionego dostępu i nieuprawnionej modyfikacji systemu informatycznego poprzez: zainstalowanie na wszystkich komputerach (30 szt.) programu antywirusowego, ograniczenie uprawnień do wprowadzania zamian w konfiguracji tych urządzeń. Dostęp do systemu operacyjnego wymagał podania hasła i loginu.

# III. Opis ustalonego stanu faktycznego oraz oceny cząstkowe[4] kontrolowanej działalności

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

Opis stanu faktycznego

**1.1.** Realizując obowiązek wynikający z dyspozycji art. 8 ustawy z dnia 10 maja 2018 r. o ochronie danych osobowych[5] i art. 37 RODO, Dyrektor SPZOZ zarządzeniem z dnia 25.05.2018 r. wyznaczył Inspektora Ochrony Danych (IOD),

[2] Najwyższa Izba Kontroli formułuje ocenę ogólną jako ocenę pozytywną, ocenę negatywną albo ocenę w formie opisowej.
[3] Dz. Urz. UE L 119 z 2016 r., str. 1, ze zm. Rozporządzenie zwane dalej: RODO.
[4] 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.
[5] Dz. U. poz. 1000, ze zm. (dalej: ustawa o ochronie danych osobowych).

którym została osoba fizyczna prowadzącą działalność gospodarczą pod firmą „Centrum Bezpieczeństwa Informatycznego Radosław Szymaszek" z siedzibą w Krasnymstawie. Do dnia 24.05.2018 r. ww. pełnił w Szpitalu obowiązki Administratora Bezpieczeństwa Informacji (ABI)[6]. Oprócz sprawowania funkcji IOD w SPZOZ w Kraśniku, ww. został wyznaczony do pełnienia tej funkcji również w trzech innych jednostkach[7], nie powodowało to jednak konfliktu interesów, ponieważ zgodnie z wyjaśnieniem Dyrektora Szpitala, SPZOZ w Kraśniku nie współpracuje z tymi podmiotami. Zakres obowiązków zleconych IOD w umowie o świadczenie usług zawierał wszystkie zadania określone w art. 39 RODO, jak również opracowanie następujących dokumentów: [1] rejestru czynności przetwarzania danych, [2] analizy ryzyka systemu informatycznego oraz danych osobowych [3] polityki ochrony danych. Szpital terminowo wywiązał się z obowiązku zawiadomienia Prezesa Urzędu Ochrony Danych Osobowych o wyznaczeniu IOD (31.07.2018 r. za pośrednictwem formularza elektronicznego). Zawiadomienie to zawierało 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[8].

IOD posiadał odpowiednie przygotowanie i kwalifikacje do pełnienia tej funkcji m.in. z uwagi na sprawowanie w okresie wcześniejszym funkcji ABI w Szpitalu oraz posiadanie Certyfikatu Systemu Zarządzania Bezpieczeństwem Informacji na zgodność z normą PN-ISO/IEC 27001, wydany przez Polskie Centrum Badań i Certyfikacji S.A. oraz Międzynarodową Sieć Jednostek Certyfikujących IQNet oraz referencje z innych podmiotów[9] za zrealizowane audyty bezpieczeństwa oraz pełnienie funkcji ABI. W umowie na pełnienie funkcji IOD zagwarantowano mu wykonywanie obowiązków w sposób niezależny, poprzez bezpośrednie podleganie w zakresie wykonywanych czynności kierownictwu Szpitala.

Minister Zdrowia pismem z dnia 08.11.2018 r. zawiadomił SPZOZ o wszczęciu z urzędu postępowania administracyjnego w sprawie uznania Szpitala za operatora usługi kluczowej[10] na podstawie ustawy z dnia 5 lipca 2018 r. o krajowym systemie cyberbezpieczeństwa[11]. Do dnia zakończenia kontroli SPZOZ nie otrzymał decyzji administracyjnej w tej sprawie.

(akta kontroli tom I str. 6-14, 15-30, 105-109, tom II str. 1-6)

**1.2.** W Szpitalu obowiązywała Polityka Ochrony Danych Osobowych, wprowadzona zarządzeniem Dyrektora SPZOZ z dnia 25.05.2018 r., w której przedstawiono zasady postępowania dotyczące bezpieczeństwa ochrony danych osobowych. W Polityce określono m.in.: [1] podmioty odpowiedzialne za ochronę danych osobowych oraz ich obowiązki, [2] podstawy przetwarzania danych osobowych, w tym, prawa osób, których dane dotyczą oraz procedurę nadawania upoważnień do przetwarzania danych osobowych, [3] środki techniczne i organizacyjne zapewniające bezpieczeństwo przetwarzania danych, [4] zasady pracy w systemach informatycznych, [5] zasady prowadzenia szkoleń z ochrony danych osobowych, [6] zasady zawierania umów powierzenia przetwarzania danych osobowych,

[6] Na podstawie umowy z 02.01.2018 r. (nr UM/ABI/BŚ/2018/01/02) na pełnienie funkcji Administratora Bezpieczeństwa Informacji oraz doradztwa informatycznego.

[7] Tj. w Wojewódzkim Ośrodku Ruchu Drogowego w Chełmie, Wojewódzkim Ośrodku Ruchu Drogowego w Zamościu i Okręgowej Spółdzielni Mleczarskiej w Krasnymstawie.

[8] www.spzoz.krasnik.pl

[9] Z 26 podmiotów.

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

[11] Dz. U. poz. 1560.

[7] sposoby zapewnienia bezpieczeństwa informacji, [8] zasady przeprowadzania audytu wewnętrznego oraz okresowych analiz ryzyka w zakresie bezpieczeństwa informacji, [9] obowiązek powiadomienia o sprostowaniu lub usunięciu danych osobowych lub o ograniczeniu przetwarzania, [10] obowiązek uwzględnienia ochrony danych w fazie projektowania i domyślnej ochrony danych, [11] zasady aktualizacji Polityki Ochrony Danych Osobowych. Załącznikami do *Polityki* były 22 załączniki zawierające procedury oraz wzory oświadczeń i dokumentów dotyczących czynności i zasad postępowania w zakresie ochrony danych osobowych. Procedury dotyczyły: prawa do dostępu do danych, sprostowania danych, prawa do bycia zapomnianym, przenoszenia danych, prawa do sprzeciwu, zgłaszania naruszeń ochrony danych osobowych. Opracowane wzory dotyczyły: [1] oświadczeń o wyrażeniu zgody na przetwarzanie danych osobowych wraz z wzorem odwołania ww. zgody, [2] klauzuli poufności, [3] wniosku o nadanie upoważnienia do przetwarzania danych osobowych, [4] ewidencji osób upoważnionych, [5] umowy powierzenia przetwarzania danych osobowych, [6] rejestru naruszeń ochrony danych, [7] zgłoszenia naruszenia ochrony danych organowi nadzorczemu, [8] zawiadomienia o naruszeniu. Dodatkowo opracowano i umieszczono w *Polityce* procedury w zakresie nadawania i odbierania upoważnień do przetwarzania danych w systemie informatycznym, procedury wykonywania konserwacji systemów oraz nośników informacji służących do przetwarzania danych. W Polityce Ochrony Danych nie określono zasad postępowania w przypadkach wystąpienia awarii lub braku zasilania oraz wystąpienia klęski żywiołowej pożaru czy powodzi, co może uniemożliwić Szpitalowi zachowanie ciągłości działania systemu przetwarzania danych osobowych, zabezpieczenia przed utratą poufności, nieuprawnionym dostępem i powinno wymusić procedurę odtwarzania systemu po wystąpieniu tego typu zdarzeń. Dyrektor wyjaśnił, że w związku z planowaną aktualizacją Polityki Ochrony Danych dokument ten zostanie uzupełniony o zasady postępowania w przypadkach wystąpienia awarii lub braku zasilania.

(akta kontroli tom I str. 31-101, tom II 1-6)

Procedury oraz instrukcje wewnętrzne związane z ochroną danych osobowych zostały zaktualizowane w związku z wprowadzonymi w SPZOZ[12] zmianami organizacyjnymi i technicznymi[13] na poszczególnych oddziałach Szpitala. Zarządzeniem Dyrektora z dnia 31.12.2018 r. wprowadzono *regulamin funkcjonowania, obsługi i eksploatacji monitoringu wizyjnego na terenie SPZOZ*[14], a zarządzeniem z dnia 11.03.2019 r. - *rejestr kategorii czynności przetwarzania danych osobowych*[15].

(akta kontroli tom I str. 135-142)

Na stronie internetowej SPZOZ w zakładce *RODO* zamieszczono informacje dla pacjentów o wprowadzonych zasadach przetwarzania danych osobowych, gdzie wskazano dane kontaktowe wyznaczonego IOD, a także zasady i cele udostępniania danych. Umieszczone zostały również klauzule informacyjne dla pacjentów, pracowników, w zakresie rekrutacji oraz dotyczące monitoringu. W stosunku do przedstawionych klauzul informacyjnych zamieszczonych w ww.

[12] Zarządzenie nr 55/2019 Dyrektora SPZOZ z dnia 31.01.2019 r. w sprawie ustalenia liczby łóżek w Szpitalu.

[13] Zmniejszenie liczby łóżek na poszczególnych oddziałach oraz przeniesienie oddziałów do budynku głównego Szpital przy ulicy Chopina.

[14] Kamery monitoringu zainstalowano w pomieszczeniach: Oddziału Ginekologiczno-Położniczym, Oddziału Noworodków, sali obserwacji po porodach powikłanych (nie podlegają nagrywaniu) w korytarzu i holu ogólnodostępnym, gabinecie endoskopii, sali wybudzeń oraz na zewnątrz budynku portierni.

[15] Zarządzenie nr 62/2019 Dyrektora SPZOZ w sprawie wprowadzenia rejestru kategorii czynności przetwarzania danych osobowych.

zakładce zastosowano możliwość ich wydruku. Podane w klauzulach treść spełniały wymagania określone w art. 13 RODO.

(akta kontroli tom I str. 246-249)

**1.3.** Realizując dyspozycję art. 30 ust. 1 RODO, Dyrektor SPZOZ zarządzeniem z dnia 25.05.2018 r. wprowadził *Rejestr czynności przetwarzania danych osobowych*[16], który prowadzono w formie pisemnej, w tym również w formie elektronicznej. Rejestr czynności przetwarzania danych osobowych sporządzony został oddzielnie dla 30 funkcjonujących w Szpitalu zbiorów danych osobowych i zawierał wszystkie elementy, o których mowa w art. 30 ust. 1 RODO: [1] nazwę zbioru danych, [2] nazwę i dane kontaktowe ADO [3] imię i nazwisko i dane kontaktowe IOD, [4] podstawy prawne upoważniające do przetwarzania danych, [5] cel przetwarzania danych, [6] opis kategorii osób, których dane są przetwarzane oraz kategorii przetwarzanych danych, [7] zakres przetwarzanych danych, [8] kategorie odbiorców, którym dane mogą być przekazywane, w tym odbiorców w państwach trzecich i organizacjach międzynarodowych, [9] źródło posiadanych danych, [10] informację o przekazaniu danych do państwa trzeciego lub organizacji międzynarodowej, [11] planowany termin usunięcia poszczególnych kategorii danych, [12] ogólny opis technicznych i organizacyjnych środków bezpieczeństwa, o których mowa w art. 32 ust. 1 RODO.

(akta kontroli tom I str. 31,100-101)

**1.4.** W SPZOZ przeprowadzono dwustopniową analizę zagrożeń i ryzyka przy przetwarzaniu danych osobowych, zgodnie z art. 32 RODO. Pierwsza analiza ryzyka sporządzona została w dniu 05.01.2018 r. Przyjęto w niej metodykę szacowania ryzyka z zastosowaniem metody RISS[17]. W analizie określono przedziały szacowania elementów dla poszczególnych ryzyk tj.: dla poufności, integralności i dostępności - od 1 do 100, dla prawdopodobieństwa wystąpienia zagrożenia i podatności - od 1 do 10. Analizę przeprowadzono odrębnie dla trzech zasadniczych obszarów:

I. ochrony przetwarzania informacji przed kradzieżą, dostępem, uszkodzeniem lub zakłóceniami w zakresie: [1] fizycznego zabezpieczenia obszaru przetwarzania danych osobowych, w którym określono dwie kategorie zagrożeń: [1.1.] nieautoryzowany dostęp do danych i sprzętu - wartość ryzyka określono jako średnie, [1.2.] kradzież (ryzyko średnie), [2] fizycznego zabezpieczenia serwerowni i dostępu do serwerowni, w którym określono pięć kategorii zagrożeń: [2.1.] pożar (ryzyko średnie), [2.2] zalanie (ryzyko średnie), [2.3.] uszkodzenie sprzętu spowodowane temperaturą lub brakiem zasilania (ryzyko średnie), [2.4.] kradzież (ryzyko średnie), [2.5.] uszkodzenie infrastruktury technicznej (ryzyko średnie);

II. Zabezpieczenia informacji w sposób uniemożliwiający nieuprawnione jej ujawnienie, modyfikacje, usunięcie lub zniszczenie w zakresie: [1] bezpieczeństwa infrastruktury sieciowej w tym utraty ciągłości działania, w którym określono dwie kategorie zagrożeń: [1.1.] utrata ciągłości działania (ryzyko średnie), [1.2.] brak dostępu do danych (ryzyko średnie), [2] bezpieczeństwa stacji roboczych, gdzie określono zagrożenia: [2.1.] zainfekowanie sprzętu (ryzyko średnie), [2.2.] uszkodzenie danych (ryzyko średnie), [2.3.] wyciek danych (ryzyko średnie), [2.4.] utrata danych (ryzyko średnie),

III. Bezpieczeństwa w systemach teleinformatycznych, w zakresie: [1] dbałości o aktualizacje oprogramowania: [1.1.] włamanie (ryzyko średnie), [1.2.] utrata

[16] Dalej: Rejestr.

[17] Metoda RISS (ang. Risk Information Security Score) opartej na algorytmie R=S*P*D gdzie R – ryzyko, S- potencjalne skutki zagrożenia, P-prawdopodobieństwo wystąpienia zagrożenia, D- podatność (stopień w jakim istniejące zabezpieczenia okażą się niewystarczające.

danych (ryzyko średnie), [1.3.] utrata integralności danych (ryzyko średnie), [2] minimalizowania ryzyka utraty informacji w wyniku awarii w zakresie: [2.1.] utraty ciągłości działania (małe ryzyko), [2.2.] utraty danych (małe ryzyko), [2.3.] utraty ciągłości pracy (małe ryzyko), [3] stosowania mechanizmów kryptograficznych w sposób adekwatny do zagrożeń lub wymogów przepisów prawa w zakresie: [3.1.] dostępu do poufnych informacji (małe ryzyko), [3.2.] wycieku danych (małe ryzyko).

Drugą analizę zagrożeń ryzyka przy przetwarzaniu danych osobowych przeprowadzono w dniu 08.03.2019 r. W jej wyniku wyodrębniono możliwe do wystąpienia kategorie zagrożeń wraz z oszacowaniem wartości ryzyka:

- dla sieci komputerowej największą wartość ryzyka przypisano: [1] podatności użytkowników na oddziaływanie inżynierii społecznej w celu złamania kodu dostępu lub wprowadzenia kodu złośliwego, brak nadzoru nad uprawnieniami użytkownika, błędy i pomyłki w zarządzaniu systemem, [2] nadmiar obowiązków administratora i działania rutynowe, niewłaściwa konfiguracja w mechanizmów bezpieczeństwa w sieci, zła konfiguracja oprogramowania, pożar;
- dla systemu teleinformatycznego określono 31 potencjalnych zagrożeń, największą wartość ryzyka przypisano: przełamaniu mechanizmów dostępu, zainstalowaniu i użytkowaniu złośliwego oprogramowania, nieuprawnionemu użytkowaniu oprogramowania, nieuprawnionej konfiguracji ustawień serwera, atakom na aplikacje serwerowe, ujawnieniu hasła administratora, awarii oprogramowania, rutynie i nadmiarowi obowiązków administratora, pomyłce w zarządzaniu systemem;
- dla stanowisk dostępowych określono 29 potencjalnych zagrożeń, największą wartość ryzyka oszacowano dla: przełamania mechanizmów dostępu, zainstalowaniu złośliwego oprogramowania, nieuprawnionych modyfikacji danych w zasobach, niepoprawnej konfiguracji ustawień stanowisk.

Przedstawiono katalog działań zaradczych, w tym wprowadzenie zapór sieciowych, wdrażanie oprogramowania typu AV na serwerach i stacjach roboczych, blokowanie portów USB na stacjach roboczych oraz możliwości samodzielnego instalowania oprogramowania przez użytkownika, rozliczenia dostępu do informacji, nośników i wydruków oraz procedury uaktualniania oprogramowania.

(akta kontroli tom I str. 144-174, 175-239)

**1.5.** W ZOZ w dniu 08.03.2019 r. została wykonana ocena skutków dla ochronnych danych, o której mowa w art. 35 RODO, chociaż jest fakultatywna i taka pojedyncza (bieżąca) ocena dotyczyć powinna operacji wiążących się z wysokim ryzykiem. Również Grupa Robocza Art. 29 ds. Ochrony Danych[18] zdecydowanie zalecała dokonanie DPIA dla operacji przetwarzania już trwających przed 25 maja 2018 r.[19] oraz w przypadkach, gdy nie jest jasne, czy wymagana jest DPIA. Uznano bowiem, że jest ona *przydatnym narzędziem, które może pomóc administratorom danych w zapewnieniu zgodności z prawem ochrony danych*, chociaż Prezes UODO w komunikacie[20] 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

[18] Grupa Robocza była niezależnym organem doradczym w zakresie ochrony danych i prywatności. Została ona powołana na mocy art. 29 dyrektywy 95/46/WE Parlamentu Europejskiego i Rady z dnia 24 października 1995 r. w sprawie ochrony osób fizycznych w zakresie przetwarzania danych osobowych i swobodnego przepływu tych danych (Dz. Urz. UE L 281 z 1995 r., str. 31, ze zm.) i działała do 25 maja 2018 r.

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

[20] Komunikat Prezesa Urzędu Ochrony Danych Osobowych z dnia 17 sierpnia 2018 r. w sprawie wykazu rodzajów operacji przetwarzania danych osobowych wymagających oceny skutków przetwarzania dla ich ochrony (M. P. poz. 827).

w szpitalach, jako wymagających oceny skutków przetwarzania. Ocena skutków dla ochrony danych osobowych zawierała wszystkie elementy wymagane art. 35 ust. 7 RODO. W sporządzonej ocenie dla wszystkich 22 zagrożeń oszacowano ryzyko na poziomie średnim.

(akta kontroli str. 210-239)

**1.6**. Po wejściu w życie przepisów RODO, w okresie od 29.06.2018 r. do 19.03.2019 r. w Szpitalu zrealizowano łącznie pięć szkoleń w zakresie przetwarzania danych osobowych oraz *Polityki Ochrony Danych,* którymi objętych zostało 381 z 726 pracowników SPZOZ (52,5% ogółu zatrudnionych). Szkolenia te obejmowały zagadnienia dotyczące m.in.: [1] reformy ochrony danych osobowych, [2] statusu i zadań inspektora ochrony danych osobowych oraz dotychczasowego administratora bezpieczeństwa informacji, [3] zabezpieczeń organizacyjnych, [4] polityki ochrony danych, [5] rejestru czynności przetwarzania danych, [6] zasad przetwarzania danych przez podmiot przetwarzający, [7] zadań i roli organu nadzorczego Urzędu Ochrony Danych Osobowych, [8] konsekwencji prawnych zasad przetwarzania danych oraz nowych zasad kontroli, w tym przedstawienie aktów prawnych w zakresie ochrony danych osobowych.

Analiza akt osobowych 30 pracowników SPZOZ[21], uczestniczących w procesie przetwarzania danych medycznych pacjentów wykazała, że:

- w siedmiu z 10 przypadkach lekarze nie posiadali udokumentowanego faktu zapoznania się z regulacjami wewnętrznymi Szpitala w zakresie ochrony danych osobowych, a na podstawie dokumentacji dotyczącej szkoleń stwierdzono, że nie uczestniczyli w żadnym szkoleniu z zakresu ochrony danych osobowych,
- dwóch lekarz posiadało certyfikat ukończenia szkolenia z dnia 14.07.2017 r. z zakresu bezpieczeństwa i ochrony informacji wg wymogów ustawy o ochronie danych osobowych (kierownik oddziału neurologii oraz Zastępca Dyrektora SPZOZ ds. medycznych), a jeden lekarz (zastępca lekarza kierującego oddziałem) uczestniczył w szkoleniu przeprowadzonym w dniu 18.03.2019 r.,
- średni personel medyczny w siedmiu z 10 przypadkach posiadał certyfikaty ukończenia szkolenia z zakresu ochrony danych osobowych, w trzech przypadkach pracownicy nie uczestniczyli w żadnym szkoleniu z zakresu ochrony danych osobowych,
- w przypadku 10 pracowników administracyjnych tylko jeden nie posiadał udokumentowania faktu zapoznania się z regulacjami wewnętrznymi Szpitala w zakresie ochrony danych osobowych,

(akta kontroli tom I str. 110-134, 240-245, 250, tom II 361-362)

**1.7.** Szpital nie zobowiązał się formalnie do stosowania kodeksu dobrych praktyk ani medycznego kodeksu branżowego. Dyrektor Szpitala wyjaśnił, że SPZOZ stosuje już wskazane rozwiązania w *projekcie kodeksu postępowania dla sektora medycznego*[22] oraz w *Przewodniku po RODO dla służby zdrowia,* wydanym przez Ministerstwo Cyfryzacji. Z uwagi jednak na fakt, że przedmiotowy projekt kodeksu postępowania do dnia dzisiejszego nie został zatwierdzony przez Prezesa Urzędu Ochrony Danych Osobowych, nie jest w sensie prawnym możliwe powoływanie się na jego treść w samych dokumentach dotyczących ochrony danych osobowych w SPZOZ. W momencie zatwierdzenia tego kodeksu postępowania w rozumieniu

[21] 20 osób spośród personelu medycznego oraz 10 pracowników administracyjnych.

[22] Opublikowanym na stronie internetowej: http://www.rodowzdrowiu.pl/.

art. 40 ust. 5 RODO, SPZOZ w Kraśniku z pewnością uwzględni również formalnie (poprzez aktualizację Polityki Ochrony Danych) postanowienia przedmiotowego Kodeksu. W odniesieniu do *Przewodnika po RODO dla służby zdrowia* wydanego przez Ministerstwo Cyfryzacji Dyrektor SPZOZ zauważył, że nie posiada on jakiegokolwiek statusu prawnego w rozumieniu RODO ani ustawy o ochronie danych osobowych i można go traktować jedynie, jako zalecane dobre praktyki. W związku z powyższym, oba ww. dokumenty są przedmiotem omówienia na szkoleniach organizowanych dla pracowników SPZOZ przez Inspektora Ochrony Danych i powinny być stosowane przez pracowników, mimo formalnego braku możliwości uwzględnienia ich w samej dokumentacji dot. ochrony danych osobowych.

(akta kontroli tom II str. 297-300)

Stwierdzone nieprawidłowości

W działalności kontrolowanej jednostki w przedstawionym wyżej zakresie stwierdzono następującą nieprawidłowość:

1. Szpital nie zapewnił przeprowadzenia przez IOD szkoleń dla całego personelu wykonującego operacje przetwarzania danych, o których mowa w art. 39 ust. 1 lit. b RODO. Po wejściu w życie przepisów RODO, w okresie od 25.05.2018 r. do 19.03.2019 r. przeszkolono jedynie 381 z 726 (52,5%) pracowników Szpitala, w tym jedynie 13 lekarzy (20%). Ponadto obowiązek zapewnienia szkoleń osobom zaangażowanym w proces przetwarzania informacji, z uwzględnieniem zagrożenia jej bezpieczeństwa, skutków naruszenia zasad bezpieczeństwa, konsekwencji prawnych i środków zapewniających jej bezpieczeństwo wynika 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[23]. Z grupy 30 pracowników, 11 osób nie posiadało udokumentowania faktu zapoznania się z regulacjami wewnętrznymi (Polityką Ochrony Danych) oraz z zagadnieniami dotyczącymi bezpieczeństwa.

Dyrektor Szpitala wyjaśnił, że proces szkolenia pracowników SPZOZ trwa nieprzerwanie od okresu wakacyjnego w 2018 r., jednak z uwagi na ograniczone możliwości lokalowe (brak odpowiednio dużej sali szkoleniowej - obecna może pomieścić jedynie do 35-40 osób jednorazowo) nie został jeszcze zakończony. Najbliższe terminy szkoleń dla pracowników organizowane przez Inspektora Ochrony Danych są zaplanowane na 12 kwietnia 2019 r. i 17 kwietnia 2019 r. (w każdym dniu odbędą się trzy tury szkoleniowe), a następnie będą zorganizowane jeszcze analogicznie dwa terminy szkoleń w maju 2019 r. i dwa terminy w czerwcu 2019 r. Tym samym proces szkoleniowy powinien zakończyć się w SPZOZ z końcem czerwca bieżącego roku.

(akta kontroli tom I str. 110-134, 240-245, 250, tom II str. 297-300)

**OCENA CZĄSTKOWA**

Szpital wywiązał się z obowiązku opracowania dokumentacji oraz procedur uwzględniających przepisy RODO. Wyznaczono IOD i terminowo zgłoszono ten fakt PUODO. Szpital przeprowadził analizę procesów przetwarzania danych oraz wykonał ocenę skutków ich przetwarzania. Opracowano rejestr czynności przetwarzania danych zawierający wszystkie wymagane elementy. W niedostatecznym jednak stopniu zapewniono szkolenia pracowników z ochrony danych osobowych w związku z wejściem w życie RODO (przeszkolono tylko 52,5%

[23]Dz. U. z 2017 r. poz. 2247. Dalej KRI.

pracowników, z czego zaledwie 13 lekarzy (20%)) oraz nie dokonano aktualizacji struktury organizacyjnej Szpitala, mimo takiej konieczności wynikającej z powołania IOD. Również nie wszystkich pracowników Szpitala zapoznano z regulacjami dotyczącymi ochrony danych osobowych oraz z zagadnieniami dotyczącymi bezpieczeństwa.

OBSZAR

## 2 Zapewnienie prawidłowego przetwarzania i ochrony danych osobowych

Opis stanu faktycznego

**2.1.** Oględziny trzech (z 4) funkcjonujących w Szpitalu rejestracji wykazały, że właściwie i zgodnie z Polityką ochrony danych chroniono dane osobowe rejestrujących się pacjentów. Rejestracja główna[24] w budynku przy ul. Chopina 13 była wyposażona w dwa okienka[25], natomiast pozostałe dwie w jedno okno. Rejestracje zorganizowane zostały w sposób uniemożliwiający wgląd w dokumenty osoby z sąsiedniego okienka lub przez innych pacjentów. W obrębie wzroku rejestrujących się pacjentów nie stwierdzono dokumentów zawierających dane osobowe innych osób, a monitory komputerów znajdujące się w rejestracji były ustawione w sposób umożliwiający wgląd jedynie pracownikom rejestracji. Dokumentacja medyczna w dwóch rejestracjach była przechowywana w zamykanych metalowych szafkach natomiast w rejestracji do Poradni Chorób Płuc i Gruźlicy oraz Poradni Onkologicznej dokumentację przechowywano w szufladach i szafkach niezamykanych na klucz. Zagadnienie to szerzej opisano w sekcji *Stwierdzone nieprawidłowości.* Przy okienkach rejestracji umieszczono informacje na temat: kto jest administratorem danych osobowych, kto pełni funkcję IOD wraz z podaniem jego danych kontaktowych, celów i podstaw przetwarzania danych osobowych i okresu przechowywania tych danych w Szpitalu. W rejestracjach przed okienkami wyznaczone zostały strefy zapewniające odstęp pomiędzy pacjentami oczekującymi w kolejce za pomocą linii odgraniczających. W trakcie oględzin wyznaczone granice stref były przestrzegane przez pacjentów. Pracownicy rejestracji nie posługiwali się nazwiskami lub innymi danymi pacjentów. Rejestratorki prosiły pacjentów o dowód osobisty i wymieniały jedynie nazwisko lekarza i godzinę umówionej wizyty. Kolejność wizyty pacjenta była ustalana na podstawie kolejnego numeru.

(akta kontroli tom II str. 19-24,31-44)

We wszystkich trzech objętych oględzinami gabinetach poradni specjalistycznych Szpitala[26] dokumentację pacjentów przechowywano na biurkach lekarzy niezapisana stroną do góry, w sposób nieujawniający jakichkolwiek danych dotyczących pacjenta. Pacjent wchodzący do gabinetu nie miał 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. Stwierdzono, że pacjenci wchodzili do gabinetu bezpośrednio po opuszczeniu go przez poprzedniego pacjenta, zgodnie z kolejnością numerków. Nie byli wzywani do gabinetów. Ekrany komputerów były ustawione w sposób uniemożliwiający odczytanie znajdujących się na nim informacji przez osoby wchodzące do gabinetu, jak i pacjenta będącego w gabinecie.

(akta kontroli tom II str. 25-30)

[24] Rejestracja do Poradni: Chirurgicznej, Chorób Kobiecych i Kobiet Ciężarnych, Gastroenterologii, Laryngologicznej, Neurologicznej, Okulistycznej, Ortopedycznej, Reumatologicznej, Chirurgii Onkologicznej.

[25] Pomiędzy oknami był róg ściany uniemożliwiający wgląd w dokumenty przedkładane przez osobę z sąsiedniego okienka lub usłyszeć rozmowę rejestratorki z pacjentem.

[26] Poradnia Chirurgiczna, Poradnia Ortopedyczna oraz Poradnia Ginekologiczna.

Przeprowadzone oględziny dyżurek pielęgniarskich, sal chorych oraz gabinetów lekarskich na trzech oddziałach szpitalnych[27] wykazały m.in., że:

-na oddziałach znajdowało się 27 sal chorych z 71 łóżkami,

-wszyscy hospitalizowani na oddziałach pacjenci (61) posiadali na nadgarstkach opaski informacyjne zawierające inicjały imienia i nazwiska, numer kartoteki lub historii choroby oraz nazwę oddziału,

-na żadnym z oddziałów nie umieszczono kart chorych przy łóżkach pacjentów,

-ruch chorych[28] prowadzony był w dyżurkach pielęgniarek i nie był widoczny dla osób postronnych,

-podręczna dokumentacja pielęgniarska przechowywana była w dyżurkach pielęgniarek na Oddziale Chorób Płuc i Gruźlicy oraz Oddziale Ortopedyczno-Urazowym w niezamykanych szafkach. Zagadnienie to zostało szerzej opisane w sekcji *Stwierdzone nieprawidłowości* natomiast na Oddziale Kardiologii w zamykanych na klucz szafkach,

-dyżurki pielęgniarskie, gabinety pielęgniarek oddziałowych oraz gabinety zabiegowe wyposażono w osiem komputerów, z których pięć było uruchomionych (pracowały na nich pielęgniarki), trzy komputery były wygaszone, a użytkownik został wylogowany z systemu operacyjnego urządzenia zostały zablokowane, a użytkownicy wylogowani z systemu operacyjnego,

-na oddziałach znajdowały się trzy gabinety lekarskie, wyposażone w dziesięć komputerów, z których dwa były uruchomione – na jednym z nich pracował lekarz, a jeden był włączony i nie został na nim zablokowany dostęp do systemu operacyjnego (Oddział Chorób Płuc i Gruźlicy), co szerzej opisano w dalszej części wystąpienia, w sekcji *Stwierdzone nieprawidłowości*,

-dokumentacja medyczna pacjentów w gabinetach lekarskich na jednym z oddziałów była przechowywana w zamykanych na klucz szafach, a w dwóch oddziałach umieszczono ją na otwartych ogólnie dostępnych półkach nieposiadających żadnej możliwości zamknięcia, co zostało opisane w sekcji *Stwierdzone nieprawidłowości*.

(akta kontroli tom I str. 251-263, tom II 363-366)

Podczas oględzin stwierdzono, że na żadnym z trzech oddziałów nie funkcjonuje monitoring wizyjny. Kamery monitoringu zamontowane zostały wewnątrz budynku Szpitala na korytarzach i holach ogólnodostępnych, gabinecie endoskopii, sali wybudzeń, Oddziale Ginekologiczno-Położniczego, Oddziale Noworodków, sali obserwacji po porodach powikłanych[29], a także na zewnątrz budynków przy portierni. Zgodnie z zapisami *Regulaminu funkcjonowania, obsługi i eksploatacji monitoringu* nagrania przechowywane były przez okres 14 dni. W przypadku uznania zapisu monitoringu za dowód w postępowaniu prowadzonym na podstawie prawa, okres przechowywania ulegał przedłużeniu do zakończenia postępowania. Celem monitoringu było zapewnienie bezpieczeństwa pracowników, pacjentów i osób odwiedzających, ochrona mienia SPZOZ, zachowanie w tajemnicy informacji, których ujawnienie mogło narazić Szpital na szkodę

(akta kontroli tom I str. 137-140, 251-263)

[27] Oględziny przeprowadzono na Oddziałach: Chorób Płuc i Gruźlicy, Ortopedyczno-Urazowy, Kardiologicznym. Objęto nimi dyżurki pielęgniarek, gabinety lekarskie, sale chorych,

[28] Lista pacjentów oddziału szpitalnego wraz z numerem sali, w których przebywają pacjenci.

[29] Z pomieszczeń sali wybudzeń, Oddziale Ginekologiczno-Położniczego, Oddziale Noworodków, sali obserwacji po porodach powikłanych nagrania nie podlegały zapisowi.

**2.2.** Według stanu na 03.04.2019 r. personel administracyjny Szpitala liczył 33 osoby. Uprawnienia administratora w systemie KS-MEDIS[30], zostały nadane pięciu osobom: Dyrektorowi SPZOZ, kierownikowi ds. medycznych i trzem informatykom. Osoby te miały dostęp do danych medycznych niezbędnych do wykonywania zadań przypisanych tym pracownikom (lekarzom), natomiast informatycy obsługujący system informatyczny KS-MEDIS, mieli w zakresach obowiązków administrowanie siecią informatyczną, siecią serwerową i infrastrukturą teleinformatyczną. Pozostali pracownicy działu administracji (28 osób) nie posiadali dostępu do systemu KS-MEDIS (nie wykonywali zadań wymagających dostępu do danych medycznych pacjentów). Dostęp do systemu KS-MEDIS posiadał również średni personel medyczny łącznie 37 osób w tym sekretarki medyczne, rejestratorki, statystycy medyczni.

(akta kontroli tom I str. 290, 291-296, tom II str. 363-366)

Szpital jest na etapie wdrażania systemu zarzadzania siecią z wykorzystaniem usługi Active Directory. Na dzień 09.04.2019 r. do ww. usługi przyłączono 16 sztuk (8,2%) ze 196 komputerów zainstalowanych w sieci SPZOZ. Dostęp do funkcjonującego systemu dla każdego pracownika posiadającego upoważnienie ADO nadawano indywidualnie, wykorzystując inicjały pracownika. Dostęp do systemów informatycznych (dziedzinowych i operacyjnych) następował metodą dwuetapową poprzez uwierzytelnienie loginu oraz hasła. Użytkownik samodzielnie generował hasło dostępu do systemu, którego złożoność określona została w Polityce Ochrony Danych[31], a zmiana i odświeżanie następowało co 90 dni.

(akta kontroli tom I str. 291-291, tom II str. 16)

**2.3.** Analiza upoważnień wydanych dla średniego personelu medycznego przeprowadzona na próbie 30 (z 295) pielęgniarek i położnych zatrudnionych w Szpitalu[32] wykazała, że wszystkie przetwarzały dane w systemie KS-MEDIS (moduł do danych medycznych pacjentów zakresie procesów pielęgnowania), tylko i wyłącznie na oddziałach szpitalnych, na których świadczyły pracę. Na podstawie analizy przechowywanych w komórce informatycznej SPZOZ upoważnień do przetwarzania danych ustalono, że udokumentowane uprawnienia do przetwarzania danych w systemie KS-MEDIS posiadało część personelu: 208 pielęgniarek na 269 zatrudnionych, 22 położne na 26 zatrudnionych oraz 51 lekarzy na 65 zatrudnionych w Szpitalu. Zagadnienie to szerzej opisano w sekcji *Stwierdzone nieprawidłowości*.

W okresie od 2013 r. do końca 2018 r. Dyrektor SPZOZ wydał 25 upoważnień do przetwarzania danych osobowych dla personelu niższego (sanitariusze szpitalni, personel gospodarczy, kierowcy), w tym dla siedmiu sanitariuszy szpitalnych, 16 kierowców i dwóch osób personelu gospodarczego (starszej salowej gospodarczej i pomocy gospodarczej). Żadne z tych upoważnień nie zostało anulowane. Upoważnienia te wydano na podstawie art. 37 ustawy z dnia 29 sierpnia 1997 r. o ochronie danych osobowych[33]. Szczegółowo zagadnienie to opisano w sekcji *Stwierdzone nieprawidłowości*.

(akta kontroli tom I str. notatka, 264-288, 318-370,)

**2.4.** Po 25.05.2018 r. Szpital rozwiązał stosunek pracy z 31 osobami, z czego 28w trakcie zatrudnienia miało przyznany dostęp do systemów informatycznych Szpitala, w tym 17 do systemu KS-MEDIS. Badanie przyznanych uprawnień do

[30] SPZOZ posiada licencje firmy KAMSOFT S. A. Katowice ul. 1 Maja 133 na używanie oprogramowania KS-MEDIS tj. system typu HIS (Hospital Information System – rodzaj oprogramowania do obsługi ruchu pacjentów wewnątrz podmiotu leczniczego).

[31] Polityka Ochrony Danych (pkt. 12. 2) login oraz hasło minimum osiem znaków małe i duże litery.

[32] Dane wg stanu na dzień 28.02.2019 r.

[33] Dz. U. z 2018 r. poz. 1000 ze zm.

pracy w programach informatycznych przetwarzających dane Szpitala oraz terminów ich cofnięcia wykazało, że:

- w dniu zaprzestania pracy przez pracownika (rozwiązania stosunku pracy) w karcie obiegowej zaznaczano wylogowanie z systemu i cofniecie uprawnień,
- w 28 przypadkach data ostatniego logowania pracownika do systemu informatycznego nie była późniejsza, niż data zaprzestania świadczenia pracy w Szpitalu**,**
- z grupy 31 osób, z którymi w ww. okresie rozwiązano stosunek pracy ponownie zatrudnionych zostało 14 osób, które powtórnie uzyskały upoważnienia do przetwarzania danych.

(akta kontroli tom I str. 289, tom II 93-165)

**2.5** W dniu 10.05.2018 r. SPZOZ zawarł z firmą KAMSOFT S. A. umowę na świadczenie stałego serwisu eksploatacyjnego (SSE). W związku z faktem, że wykonanie umowy wiązało się z koniecznością powierzenia przetwarzania danych osobowych administrowanych przez Szpital, zawarto dodatkowo umowę powierzenia danych osobowych. SPZOZ przesyłał zgłoszenia serwisowe za pomocą internetowego systemu zgłoszeń KS-MRK, zaznaczając status zgłoszenia[34]. W przypadku trudności ze zdalnym przesłaniem zgłoszenia w ww. witrynie, mógł zrealizować je drogą telefoniczną pod wskazanymi w umowie numerami. W okresie od 25.05.2018 r. do 20.03.2019 r. drogą elektroniczną z wykorzystaniem ww. internetowego systemu zgłoszeń, przekazano dziewięć zgłoszeń serwisowych, z czego: [1] cztery dotyczyły błędów lub wadliwego działania w systemie KS-MEDIS, [2] dwa dotyczyły błędów w systemie KS-ZZL (Moduł Zarządzanie Zasobami Ludzkimi), [3] po jednym w systemach KS-SOLAB (Moduł Badania Laboratoryjne), KS-FKW (Moduł Finansowo-Księgowy), KS-HFW (Moduł Sprzęt). Analiza sposobu przekazania wszystkich dziewięciu zgłoszeń serwisowych, związanych z nieprawidłowym działaniem systemu informatycznego KS-MEDIS wykazały m.in., że:

- zgłoszenia serwisowe były przekazywane w formie elektronicznej przez informatyków Szpitala, w przypadku ośmiu z nich udzielono odpowiedzi i rozwiązano problem, w jednym przypadku na problem zgłoszony w dniu 20.03.2019 r. nie uzyskano odpowiedzi,

- wszystkie zgłoszenia zrealizowano drogą elektroniczną z wykorzystaniem serwisu internetowego,

- w dwóch przypadkach, podmiotowi świadczącemu usługi serwisowe w systemie informatycznym (KS-MEDIS), przekazano dane osobowe pacjentów: imię, nazwisko, nr PESEL oraz dane dotyczące świadczeń zdrowotnych z podaniem rozpoznania. Zagadnienie to szerzej opisano w sekcji *Stwierdzone nieprawidłowości.* Szpital z tym podmiotem zawarł umowę powierzenia przetwarzania danych..

(akta kontroli tom I str. 300-317, 371-375)

**2.6.** Szpital w okresie objętym kontrolą posiadał zawarte 24 umowy dotyczące powierzenia przetwarzania danych osobowych, w których wystąpił jako podmiot powierzający przetwarzanie danych. Szpital zawarł 17 umów powierzenia przetwarzania takich danych ze wszystkimi lekarzami zatrudnionymi na kontraktach oraz 7 umów z wykonawcami realizującymi zadania związane m.in. ze świadczeniem usług medycznych na rzecz Szpitala. Analiza pięciu umów dotyczących powierzenia przez Szpital przetwarzania danych osobowych

[34] Dysfunkcja, usterka, stan awaryjny, stan krytyczny – potwierdzony zawsze faksem.

z lekarzami wykazała m.in. że: zawierały one wszystkie postanowienia wymagane art. 28 ust. 3 RODO i stanowiły integralną część umowy na świadczenie usług. Zakres danych osobowych powierzonych przez Szpital wynikał z rodzaju usług, które zgodnie z umową miał być realizowany na rzecz Szpitala.

W przypadku 107 umów, w których Szpital był usługodawcą na rzecz innych podmiotów nie zawarto umów dotyczących powierzenia Szpitalowi przetwarzania danych osobowych. Dyrektor Szpitala wyjaśnił, że *zgodnie z licznymi opiniami prawnymi specjalistów ds. ochrony danych osobowych w powołanych przypadkach mamy do czynienia z sytuacją, w której podmiot Y jest de facto podwykonawcą usługi dla podmiotu X. Jednocześnie każdy podmiot występuje tutaj jako administrator danych osobowych pacjenta. Powyższe oznacza, że nie istnieje tutaj relacja administrator - procesor opisana w art. 28 RODO, albowiem każdy z podmiotów określa cel i zakres przetwarzanych danych. Tym samym zawarcie umowy powierzenia nie jest tutaj konieczne ani wskazane (tak w: Lokaj Maciej „Czy pomiędzy dwoma podmiotami wykonującymi działalność leczniczą należy zawrzeć umowę powierzenia przetwarzania danych osobowych w związku ze zleceniem wykonania badań diagnostycznych/laboratoryjnych na rzecz pacjentów innego PWDL?", LEX 2019).*

(akta kontroli tom II str. 45-91, 297-300)

**2.7.** W Rejestrze naruszeń ochrony danych nie odnotowano w okresie od 25.05.2018 r. do 13.03.2019 r. żadnych zdarzeń, na których okoliczność należałoby sporządzić protokół uchybień lub protokół zagrożenia. W ww. okresie do Szpitala nie wpłynęły skargi i wnioski, które dotyczyłyby nieprawidłowości związanych z ochroną danych osobowych pacjentów. Rejestr został uzupełniony w trakcie kontroli o zdarzenia ujawnione podczas kontroli dotyczące nieodpowiedniego przechowywania dokumentacji medycznej w gabinetach lekarskich oraz niezabezpieczenia gabinetu lekarskiego podczas nieobecności lekarza.

(akta kontroli tom I str. 444, tom II str. 15, 371-373)

**2.8.** W okresie objętym kontrolą w Szpitalu obowiązywały: *Instrukcja udostępniania danych osobowych z* dnia 29.11.2013 r. oraz *Procedura prawo dostępu do danych*, stanowiąca załącznik nr 5 do *Polityki ochrony danych*. W myśl tych regulacji oraz zgodnie z art. 26 ust. 1 ustawy o prawach pacjenta, dokumentacja medyczna udostępniana była pacjentowi, jego przedstawicielowi ustawowemu, osobie upoważnionej przez pacjenta oraz podmiotom określonym w ust. 3 ww. przepisu. Według stanu na 31.03.2019 2019 r. udostępnienie dokumentacji medycznej osobom i podmiotom zewnętrznym miło miejsce w 1509 przypadków z tego: 850 na wniosek pacjenta, 379 na wniosek osoby upoważnionej, 280 na wniosek instytucji. Analiza prawidłowości udostępnienia dokumentacji medycznej instytucjom (30 spraw), firmom ubezpieczeniowym (67 spraw) oraz osobom fizycznym innym niż pacjent (30 spraw) wykazała, że dokumentację udostępniono wyłącznie upoważnionym podmiotom (osobom) lub przedstawicielowi ustawowemu, zgodnie z *Instrukcją udostępniania dokumentacji medycznej* oraz art. 26 ust. 1 ustawy o prawach pacjenta. W okresie od 1.05.2018 r. do 31.03.2019 r. nie wystąpiły przypadki odmowy wydania informacji z dokumentacji medycznej oraz nie było skarg na udostępnianie dokumentacji.

(akta kontroli tom II str. 166-296)

**2.9.** W celu minimalizacji ryzyka utraty danych, będących następstwem awarii błędów lub nieuprawnionej modyfikacji, Szpital wprowadził i stosował rozwiązania i regulacje prawne ograniczające niebezpieczeństwo ich wystąpienia. Ochrona

danych prowadzona była zgodnie z zasadami i uregulowaniami określonymi w *Polityce Ochrony Danych* i polegała na:

- wprowadzeniu klauzul informacyjnych dotyczących przetwarzania danych osobowych w celu realizacji obowiązków prawnych ciążących na SPZOZ,
- określeniu zasad i procedur dotyczących: korzystania z oprogramowania, z internetu, przesyłania dokumentów za pośrednictwem poczty elektronicznej, bankowości elektronicznej,
- opracowaniu zasad zarządzania oprogramowaniem komputerowym oraz sposoby zabezpieczenia systemu, bezpiecznego użytkowania sprzętu IT,
- zasady sporządzania i zarządzania kopiami zapasowymi baz danych,
- określeniu technicznych środków zabezpieczających.

Pomieszczenie serwerowni było:
- zabezpieczone przed dostępem osób nieuprawnionych (drzwi wejściowe metalowe, przed drzwiami dodatkowa krata zewnętrzna zamykana na kłódkę, w oknach kraty stalowe),
- wyposażone w system kontroli wejścia oraz urządzenia podtrzymywania napięcia UPS, gaśnice przeciwpożarowe i klimatyzacyjne,
- oddzielny serwer do tworzenia kopii zapasowych baz danych, które przechowywano na serwerze innym niż serwer dla bazy danych, oba serwery zlokalizowane były w odrębnych szafach w tym samym pomieszczeniu, posiadały również odrębne źródła zasilania głównego oraz awaryjnego, lokalizacja taka wynikała z braku wolnych pomieszczeń w budynku administracyjnym SPZOZ. Planowany był remont serwerowni i wydzielenie drugiego pomieszczenia serwerowni,
- stan okablowania, w tym przewody elektryczne i połączenia komputerowe bez oznak zniszczenia lub mechanicznego przetarcia.

Kopie bezpieczeństwa tworzone były automatycznie z częstotliwością jeden raz dziennie dla pełnego backupu oraz raz w tygodniu i raz w miesiącu na zewnętrzny napęd. Co trzy godziny zapisywana była kopia przyrostowa. Raz w miesiącu dokonywano sprawdzenia poprawności wykonywania tych kopii. Tworzono dwie kopie bezpieczeństwa dla danych medycznych zintegrowanego systemu informatycznego oraz danych pracowników i kontrahentów. Nośnikiem przechowywania kopii zapasowych był serwer kopii zapasowych. Druga kopia tworzona była na serwerze kopii zapasowej tzw. backup.

Oględziny 30 komputerów, w tym 20 użytkowanych przez personel medyczny (po 10 przez lekarzy i personel pielęgniarski) oraz 10 przez personel administracyjny wykazały, że:
- na 20 komputerach zainstalowano system Windows 10 Professional, a na pozostałych Windows 7 Professional (10 szt.),
- na wszystkich zainstalowany był program antywirusowy, posiadający aktualną wersję bazy sygnatur wirusów,
- we wszystkich komputerach nie zostały zablokowane porty USB, umożliwiając podłączenie do nich nośników pamięci, natomiast brak było możliwości kopiowanie danych z komputera na ten nośnik, na dyskach komputerów w lokalizacji *Pulpit, Moje dokumenty* nie znaleziono plików zawierających dane osobowe i medyczne pacjentów,

- na wszystkich komputerach użytkownicy posiadali ograniczone uprawnienia w systemie operacyjnym, które nie pozwalały na wprowadzanie zmian w konfiguracji tych urządzeń oraz instalację dodatkowego oprogramowania,
- wszystkie komputery posiadały dostęp do sieci Szpitala poprzez konto lokalne na podstawie hasła o odpowiedniej złożoności, nadanego indywidualnie dla każdego komputera.

Szpital posiadał dziesięć; komputerów przenośnych, które nie były wyposażone w systemy ochrony kryptograficznej dysku twardego, na komputerach tych nie przechowywano danych osobowych.

(akta kontroli tom I str. 31-101, tom II str. 7-8)

Stwierdzone nieprawidłowości

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

1. Przeprowadzone oględziny wykazały, że 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:

- w jednym przypadku drzwi do gabinetu lekarskiego nie zostały zamknięte na klucz (były uchylone) i jeden z komputerów nie był zabezpieczony, nie wylogowano użytkownika oraz nie włączono wygaszacza ekranu (lekarz wpisywał dane do systemu KS-MEDIS i wyszedł z gabinetu)[35],

- w jednym przypadku teczka z dokumentacją medyczną trzech pacjentów została pozostawiona w gabinecie lekarskim na biurku (w gabinecie nie było personelu lekarskiego[36], a drzwi do gabinetu były zamknięte),

- w dwóch przypadkach dokumentacja medyczna pacjentów hospitalizowanych na oddziałach była umieszczona na otwartych półkach[37],

- w rejestracji do poradni Onkologicznej oraz Poradni Chorób Płuc i Gruźlicy dokumentacja medyczna znajdowała się w pomieszczeniu rejestracji (zamykanym na klucz) i umieszczona była w szafkach niezamykanych na klucz,

- w rejestracji do poradni w Przychodni specjalistycznej na ul. Niepodległości 25 znajdowała się niezabezpieczona przed dostępem osób trzecich dokumentacja medyczna (złożona w pudełkach). Poradnia jak również gabinety były zamykane na klucz.

W złożonych wyjaśnieniach Dyrektor podał, że stwierdzone w trakcie przeprowadzonych oględzin nieprawidłowości w zakresie przetwarzania danych o pacjentach zostały niezwłocznie po ich stwierdzeniu uwzględnione w rejestrze naruszeń ochrony danych osobowych SPZOZ w Kraśniku (w załączeniu kopia Rejestru naruszeń ochrony danych osobowych SPZOZ w Kraśniku) zgodnie z pkt 4 Procedury zgłaszania naruszeń ochrony danych osobowych, stanowiącej załącznik nr 18 do Polityki Ochrony Danych SPZOZ w Kraśniku. Jednocześnie podał, że stwierdzone nieprawidłowości podczas oględzin oddziałów i rejestracji do poradni specjalistycznych zostały w trakcie kontroli usunięte. Lekarze kierujący oddziałami oraz pielęgniarki oddziałowe złożyły w tym zakresie stosowne oświadczenia o usunięciu nieprawidłowości.

(akta kontroli tom I str. 137-140, 251-263, 445-446, tom II str. 19-44, 297-300)

[35] Gabinet lekarski na Oddziale Chorób Płuc i Gruźlicy.
[36] Gabinet lekarski na Oddziale Ortopedyczno-Urazowym.
[37] Gabinety lekarskie Oddziału Chorób Płuc i Gruźlicy i Oddziału Ortopedyczno-Urazowym.

2. W okresie od 2013 r. do końca 2018 r. Dyrektor SPZOZ wydał 25 upoważnień do przetwarzania danych osobowych dla personelu pomocniczego, tj. dla siedmiu sanitariuszy, 16 kierowców i dwóch osób personelu gospodarczego (starszej salowej gospodarczej i pomocy gospodarczej). W indywidualnych zakresach obowiązków analizowanej grupy pracowników nie stwierdzono zapisów umożliwiających dostęp przez nich do danych osobowych, w tym danych medycznych. Wydanie upoważnień dla ww. personelu było sprzeczne z art. 32 ust. 4 w związku z art. 5 pkt 1 lit. c RODO, w nawiązaniu do treści motywu 39 RODO dane osobowe powinny być przetwarzane w sposób zapewniający im odpowiednie bezpieczeństwo i odpowiednią poufność, w tym ochronę przed nieuprawnionym dostępem do nich i do sprzętu służącego ich przetwarzaniu oraz przed nieuprawnionym korzystaniem z tych danych i z tego sprzętu.

Dyrektor Szpitala wyjaśnił, że przedmiotowe upoważnienia do przetwarzania danych osobowych zostały wydane pracownikom faktycznie przetwarzającym te dane w trakcie swojej pracy dla SPZOZ. Konieczna zmiana dla tych osób zakresów obowiązków znajdujących się w aktach osobowych zostanie niezwłocznie przeprowadzona.

NIK nie podziela zdania Dyrektora, że ww. pracownicy SPZOZ powinni mieć upoważnienia do przetwarzania danych osobowych i medycznych, a tym bardziej wglądu do dokumentacji medycznej, ze względu na przepisy art. 9 ust. 1 i 2 RODO, uzależniające dostęp do tzw. szczególnych kategorii danych, w tym danych dotyczących zdrowia, od spełnienia określonych, szczególnych warunków (np. zapewnienia opieki zdrowotnej lub leczenia). Postanowienia z art. 24 ust. 2 i art. 26 ust. 1 ustawy o prawach pacjenta, wskazują, że dokumentację medyczną można ujawnić tylko określonym podmiotom, w tym podmiotom leczniczym, osobom wykonującym zawód medyczny uczestniczącym w udzielaniu świadczeń medycznych lub właściwym organom. Zasady te określa również art. 40 i art. 41 ustawy z dnia 5 grudnia 1996 r. o zawodach lekarza i lekarza dentysty[38]. Nie mają też zastosowania przepisy art. 24 ust. 2 pkt 2 ustawy o prawach pacjenta, dotyczące osób wykonujących czynności pomocnicze przy udzielaniu świadczeń zdrowotnych, które są uprawnione do dostępu do danych medycznych, na podstawie upoważnień administratora danych. Zgodnie z art. 5 ust. 1 i art. 6 ust. 1 RODO przetwarzanie danych powinno być ograniczone do tego, co jest niezbędne do celów przetwarzania. Sprzątanie pomieszczeń nie stanowi celu przetwarzania, uzasadniającego dostęp do danych. Podobnie przewóz pacjentów powinien być zorganizowany w sposób uniemożliwiający personelowi Działu dostęp do danych medycznych transportowanych wraz z pacjentem. W zakresie pozostałych danych, niebędących danymi medycznymi, nie ma zakazu udostępniania innym osobom takich danych i udzielenia im upoważnień, ale musi wynikać to z wykonywania obowiązków związanych z dostępem do takich danych.

(akta kontroli tom I str. 264-288, 318-370, tom II str. 297-300)

3. W dwóch przypadkach, z dziewięciu objętych analizą, zgłoszeniach serwisowych dotyczących systemu informatycznego KS-MEDIS, przesłanych po 25.05.2018 r. podmiotowi świadczącemu usługi serwisowe, zamieszczono dane osobowe pacjentów Szpitala (nazwiska i imiona, numer PESEL) oraz dane medyczne, zawierające rozpoznanie, zakres lub wyniki badań, co było niezgodne z wynikającą z art. 5 ust. 1 lit. c) RODO zasadą adekwatności i minimalizacji danych. Szpital z podmiotem świadczącym usługi serwisu, któremu przekazano dane pacjentów, zawarł umowy powierzenia przetwarzania danych.

[38] Dz. U. z 2018 r. poz. 617, ze zm.

W wyjaśnieniu Dyrektor podał, że podmiot świadczący na rzecz SPZOZ w Kraśniku usługi informatyczne w zakresie dostarczania i serwisowania systemu informatycznego KS-MEDIS został upoważniony do przetwarzania danych osobowych przez SPZOZ w Kraśniku na podstawie par. 11 umowy na świadczenia usług stałego serwisu eksploatacyjnego USSE/996682/01 (załącznik U110101 Zasady powierzenie danych osobowych) zawartej przez Szpital z KAMSOFT S.A. z siedzibą w Katowicach. Ze świadczonymi przez ten podmiot usługami serwisowymi dot. przedmiotowego systemu informatycznego jest nieodłącznie związana konieczność porozumiewania się pracowników Szpitala na odległość z tą firmą w postaci przesyłania tzw. „zrzutów ekranu" z komputerów służbowych SPZOZ w Kraśniku na wypadek zaistnienia jakichkolwiek awarii. Podczas obecnie trwającej aktualizacji tego oprogramowania personel Szpitala jest informowany o konieczności ograniczania przesyłanych w ten sposób treści związanych z danymi osobowymi (w tym w szczególności danymi szczególnych kategorii dotyczącymi zdrowia w rozumieniu art. 9 ust. 1 RODO) do niezbędnego minimum.

(akta kontroli tom I str. 300-317, 371-375, tom II str. 363-366)

4. Stwierdzono, że 69 pielęgniarek, 4 położne oraz 14 lekarzy nie posiadało udokumentowanego uprawnienia do przetwarzania danych w systemie KS-MEDIS służącym do przetwarzania danych medycznych. 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.

W złożonym wyjaśnieniu Dyrektor Szpitala podał, że **p**rzedmiotowe braki w samych upoważnieniach zostały uzupełnione (uprawnienia zostały uaktualnione).

(akta kontroli tom II str. 363-366)

5. Uprawnienia do przetwarzania danych osobowych po 25.05.2018 r., w 23 przypadkach z 31, nadano pomimo złożenia wniosków przez nieuprawnione osoby, tj. przez pracowników, a nie przez bezpośrednich przełożonych osób upoważnianych, co było niezgodne z zapisami Polityki Ochrony Danych (pkt 7.4 Procedura nadawania upoważnień do przetwarzania danych osobowych ppkt 1), które jednoznacznie określały, że osobą upoważnioną do złożenia wniosku o nadanie upoważnienia jest bezpośredni przełożony pracownika.

W złożonym wyjaśnieniu Dyrektor podał, że upoważnienia do przetwarzania danych osobowych nadane z naruszeniem zapisów Polityki Ochrony Danych (w zakresie osoby występującej z wnioskiem o nadanie upoważnienia) zostały skorygowane poprzez uzupełnienie odpowiednich wniosków wypełnionych przez bezpośrednich przełożonych osób upoważnianych. Jednocześnie należy podkreślić, że we wszystkich przypadkach samo nadanie przedmiotowych upoważnień odbywało się prawidłowo, a procedura wnioskowania o nadanie takich upoważnień jest nieobligatoryjna w świetle przepisów RODO, a także ustawy z dnia 10 maja 2018 r. o ochronie danych osobowych. Wobec powyższego, niedopatrzenia dotyczące wadliwych wniosków o nadanie upoważnień do przetwarzania danych nie spowodowały jednoczesnego naruszenia powszechnie obowiązujących przepisów o ochronie danych osobowych przez Szpital.

(akta kontroli tom II str. 45-91, 297-300, 363-366)

**OCENA CZĄSTKOWA** Szpital wdrożył rozwiązania organizacyjne i techniczne mające na celu zapewnienie prawidłowej ochrony i przetwarzania danych osobowych. Nie w pełni prawidłowo chroniono i przetwarzano dane osobowe w skontrolowanych trzech poradniach

specjalistycznych (niewłaściwie przechowywano dokumentację medyczną) natomiast na oddziałach szpitalnych stwierdzono niedostateczne zabezpieczenie przechowywanej dokumentacji medycznej oraz pozostawienie komputera bez prawidłowego zabezpieczenia). Wszystkim byłym pracownikom Szpitala w dniu odejścia z pracy zablokowano dostęp do przetwarzania danych osobowych. Wystąpiły przypadki nieprawidłowego udokumentowania posiadania uprawnienia do przetwarzania danych w tym systemie oraz stwierdzono nieuprawnione wydania upoważnień do przetwarzania danych medycznych dla personelu pomocniczego Szpitala (sanitariusze szpitalni, personel gospodarczy, kierowcy) oraz przekazania dostawcy oprogramowania danych osobowych i medycznych pacjentów. Dokumentację medyczną udostępniono uprawnionym podmiotom, a analizowane umowy powierzenia przetwarzania danych osobowych spełniały wymagania określone w art. 28 RODO. Serwerownia Szpitala, w której przechowywano dane osobowe (przetwarzane elektronicznie) była prawidłowo zabezpieczona. Sukcesywnie wprowadzono uregulowania w zakresie ograniczenia i minimalizacji ryzyka dotyczącego utraty danych medycznych oraz nieuprawnionego dostępu i nieuprawnionej modyfikacji systemu informatycznego m. in poprzez instalowanie na wszystkich komputerach (30 szt.) programu antywirusowego, wprowadzaniu ograniczeń dotyczących uprawnień do modyfikowania zamian w konfiguracji komputerów.

# Uwagi i wnioski

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

Wnioski

# Wnioski

1. Przeprowadzenie szkoleń dotyczących ochrony danych osobowych dla wszystkich pracowników Szpitala zaangażowanych w proces przetwarzania danych.
2. Wdrożenie odpowiednich środków technicznych i organizacyjnych zapewniających ochronę danych osobowych oraz minimalizację ryzyka ujawnienia informacji osobom postronnym w zakresie przechowywania dokumentacji medycznej oraz pracy z systemami informatycznymi.
3. Nadawanie upoważnień do przetwarzania danych osobowych zgodnie z indywidualnymi zakresami obowiązków pracowników.
4. Niepodawanie w zgłoszeniach serwisowych danych osobowych i medycznych pacjentów.
5. Dopuszczenie pracowników do przetwarzania danych osobowych po wydaniu stosownych upoważnień w tym zakresie.

# 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 Lublinie. 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

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.

Lublin, 19 kwietnia 2019 r.

Kontroler

Artur Bokiniec
Główny specjalista kontroli państwowej

.....
*podpis*

Dyrektor

Delegatury Najwyższej Izby Kontroli
w Lublinie
Edward Lis

.....
*podpis*