NAJWYŻSZA IZBA KONTROLI
Delegatura w Zielonej Górze

LZG. 410.002.04.2019

Łukasz Kaczmarek
Prezes Zarządu
NZOZ Szpital im. Prof. Z. Religi Sp. z o.o.
ul. Nadodrzańska 6
69-100 Słubice

WYSTĄPIENIE POKONTROLNE

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

NAJWYŻSZA IZBA KONTROLI
Delegatura w Zielonej Górze
ul. Podgórna 9a, 65-213 Zielona Góra
T +48 68 410 66 00, F +48 68 410 66 39
lzg@nik.gov.pl

I. Dane identyfikacyjne

Jednostka kontrolowana	Niepubliczny Zakład Opieki Zdrowotnej Szpital im. Prof. Z. Religi sp. z o. o., ul. Nadodrzańska 6, 69-100 Słubice (dalej: *Szpital* lub *Jednostka).*
Kierownik jednostki kontrolowanej	Łukasz Kaczmarek – Prezes Zarządu Spółki od 12.01.2019 r. do nadal. W okresie objętym kontrolą funkcję kierownika jednostki poprzednio pełnili: Maciej Pawliński – Prezes Zarządu Spółki od 19.10.2018 r. do 11.01.2019 r. Małgorzata Krasowska-Marczyk – Prezes Zarządu Spółki od 20.09.2016 r. do 18.10.2018 r.[1] (akta kontroli: str. 3-8)
Zakres przedmiotowy kontroli	1. Opracowanie wymaganej dokumentacji oraz procedur związanych z ochroną przetwarzanych danych osobowych. 2. Zapewnienie prawidłowego przetwarzania i ochrony danych osobowych.
Okres objęty kontrolą	Od 25 maja 2018 r. (data wejścia w życie przepisów RODO[2]) do dnia zakończenia czynności kontrolnych[3].
Podstawa prawna podjęcia kontroli	Art. 2 ust. 2 ustawy z dnia 23 grudnia 1994 r. o Najwyższej Izbie Kontroli[4]
Jednostka przeprowadzająca kontrolę	Najwyższa Izba Kontroli Delegatura w Zielonej Górze
Kontroler	Krzysztof Hofman, specjalista k. p., upoważnienie do kontroli nr LZG/30/2019 z 1 lutego 2019 r. (akta kontroli str. 1-2)

[1] W okresie od 20 października 2018 r. do 12 stycznia 2019 r. do czasowego wykonywania czynności Prezesa Zarządu Szpitala Rada Nadzorcza oddelegowała członka Rady Nadzorczej – Macieja Pawlińskiego (Uchwała Rady Nadzorczej Nr.2/X/2018 z 19 października 2018 r.).

[2] 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.), dalej *RODO*.

[3] Badania kontrolne mogą dotyczyć działań sprzed tego okresu, jeśli mają związek z zagadnieniami będącymi przedmiotem kontroli.

[4] Dz. U. z 2019 r. poz. 489, dalej: *ustawa o NIK*.

II. Ocena ogólna[5] kontrolowanej działalności

OCENA OGÓLNA

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

Uzasadnienie oceny ogólnej

Jednostka wywiązała się z obowiązku opracowania dokumentacji oraz procedur uwzględniających przepisy RODO. Jednak ich dostosowanie do nowych regulacji nastąpiło dopiero po ponad siedmiu miesiącach od wejścia w życie RODO, a część z niej nie była w pełni kompletna. Wywiązano się także z obowiązku powołania na stanowisko IOD osoby posiadającej odpowiednie przygotowanie i kwalifikacje zawodowe oraz terminowo zawiadomiono o tym fakcie Prezesa Urzędu Ochrony Danych Osobowych. Opracowany terminowo Rejestr czynności przetwarzania, a także przeprowadzona analiza ryzyka procesów przetwarzania danych nie były jednak kompletne, gdyż nie objęły wszystkich operacji przetwarzania danych.

Nie w pełni zrealizowano także obowiązek przeszkolenia pracowników Szpitala uczestniczących w procesie przetwarzania danych osobowych z zagadnień dotyczących bezpieczeństwa danych oraz obowiązywania przepisów RODO, gdyż tylko niespełna 15% tych pracowników zostało objętych udokumentowanymi szkoleniami.

W Szpitalu wdrożono rozwiązania organizacyjne i techniczne zmierzające do zapewnienia prawidłowej ochrony i przetwarzania danych osobowych. Prawidłowo chroniono i przetwarzano dane osobowe w skontrolowanych trzech oddziałach szpitalnych, trzech poradniach specjalistycznych, a także w punktach rejestracji do poradni szpitalnych oraz szpitalnej izbie przyjęć.

Personelowi Szpitala nie zapewniono jednakże odpowiedniego dostępu do danych medycznych. Stwierdzono w toku kontroli przypadki pisemnych upoważnień, wydanych w oparciu o nieaktualne przepisy, braku wymaganej precyzji i adekwatności poprzez pozostawienie zbyt szerokich uprawnień, nadawania upoważnień personelowi, który nie realizował zadań związanych z przetwarzaniem danych osobowych, a także odbierania ze znacznym opóźnieniem możliwości dostępu do tych systemów byłym pracownikom Szpitala.

Szpital nie we wszystkich wymaganych przypadkach zawierał także umowy powierzenia przetwarzania danych a prowadzony wykaz podmiotów z którymi zawarto takie umowy był niekompletny. Natomiast w pięciu analizowanych umowach powierzenia przetwarzania zamieszczono postanowienia wymagane art. 28 RODO.

Szpital prawidłowo natomiast udostępniał uprawnionym podmiotom dokumentację medyczną pacjentów, a funkcjonujący w Jednostce wykaz udostępniania tych danych był zgodny z obowiązującymi wymogami.

W administrowanych przez Szpital komputerach poddanych badaniom nie zapewniono pełnej zgodności z Polityką Bezpieczeństwa. Należy zauważyć, że sposób użytkowania i zabezpieczenia wykorzystywanych w Szpitalu komputerów nie gwarantował – wskutek m.in. nieprzestrzegania wymogów dotyczących obowiązujących haseł oraz możliwości instalowania dowolnego oprogramowania – pełnej ochrony przetwarzanych na tych komputerach danych osobowych pacjentów.

Stan użytkowanej serwerowni i pomieszczenia, w którym Szpital przechowuje kopie danych nie zapewniał maksymalnej ochrony przed skutkami zdarzeń losowych, jednak Szpital jest w trakcie wdrażania nowych rozwiązań w zakresie infrastruktury informatycznej, co powinno wpłynąć na poprawę stanu zabezpieczenia przetwarzanych w nim danych .

Podkreślenia wymaga, że jeszcze w toku kontroli podjęto lub zadeklarowano działania zmierzające do usunięcia stwierdzonych nieprawidłowości.

---

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

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

OBSZAR

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

Opis stanu faktycznego

1.1. Zgodnie z przyjętą i zatwierdzoną przez Prezesa Zarządu 14 stycznia 2019 r. Polityką Bezpieczeństwa Informacji - administratorem danych osobowych (dalej *ADO*) przetwarzanych w Jednostce[7] jest Zarząd Szpitala[8].

Zarząd Szpitala powołał IOD z dniem 7 maja 2018 r.[9] (zlecił usługę podmiotowi zewnętrznemu).

Była Prezes Szpitala wyjaśniła, że w okresie przygotowań do wdrożenia RODO, w Szpitalu brak było osoby, która byłaby w stanie opracować niezbędne analizy i procedury, stąd wystąpiła konieczność wparcia działań Szpitala przez zewnętrznego IOD.

(akta kontroli str. 101-104, 198-205, 233-237, 707-712)

Zawiadomienie dotyczące powołania IOD zostało przesłane elektronicznie do PUODO w dniu 20 lipca 2018 r., tj. zgodnie z terminem określonym w przepisie art.158 ust.5 ustawy z dnia 10 maja 2018 r. o ochronie danych osobowych[10] (dalej: *u.o.d.o.*), co szerzej opisano w dalszej części wystąpienia, w sekcji „Stwierdzone nieprawidłowości".

(akta kontroli str. 105-107)

Zgodnie z art. 37 ust. 5 RODO, IOD miał należyte przygotowanie i kwalifikacje zawodowe do pełnienia swojej funkcji. W szczególności posiadał on ukończone studia podyplomowe, kursy i certyfikaty w zakresie organizacji systemu obronnego i bezpieczeństwa, a także certyfikat poświadczający uczestnictwo w szkoleniu związanym z ochroną danych osobowych w placówkach służby zdrowia[11].

(akta kontroli str. 109-113)

Dane IOD oraz sposób i formę kontaktu Szpital opublikował 28 maja 2018 r. stosownie do wymogu z art. 37 ust. 7 RODO na swojej stronie internetowej. Ponadto na terenie Szpitala (wejście do Szpitala, korytarze, okolice rejestracji, Izby Przyjęć) rozmieszczono dedykowane tematyce RODO klauzule informacyjne dla pacjentów.

(akta kontroli str. 108, 385)

Zgodnie z zawartą przez Szpital umową zakres praw i obowiązków IOD objął wszystkie zadania określone w art. 39 RODO. Zgodnie z zawartą umową IOD zapewniono niezależność, gdyż podlega on wyłącznie kierownictwu Szpitala, co wypełnia wymogi art. 38 ust. 3 RODO.

(akta kontroli str. 101-104)

---

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

7 Przetwarzanie danych osobowych w Szpitalu odbywa się na podstawie ustawy z 6 listopada 2008 r. o prawach pacjenta i Rzeczniku Praw Pacjenta (Dz. U. z 2017 r. poz.1318) oraz w niektórych kategoriach na podstawie zgody osób, których dane są przetwarzane.

8 W Polityce Bezpieczeństwa przetwarzania danych osobowych wprowadzonej zarządzeniem nr 72/2014 Prezesa Szpitala dnia z 1 grudnia 2014 r. jako administratora danych (ADO) wskazano Prezesa/Dyrektora NZOZ Szpitala Powiatowego w Słubicach. Zarządzeniem tym wprowadzono także obowiązującą Instrukcję udostępniania dokumentacji medycznej.

9 Zarząd Szpitala 8 maja 2018 r. zawarł umowę w podmiotem zewnętrznym, któremu powierzono realizację obowiązków IOD wynikających z rozporządzenia RODO.

10 Dz. U. poz. 1000, ze zm.

11 IOD brał udział m.in. w szkoleniu pn. „Ochrona danych osobowych w placówkach służby zdrowia zgodnie z RODO – przygotowanie do stosowania nowego rozporządzenia w sprawie ochrony (…) danych osobowych".

Szpital nie został dotychczas[12] uznany (nie otrzymał decyzji administracyjnej od właściwego organu do spraw cyberbezpieczeństwa) za operatora usługi kluczowej, o którym mowa w art.5 ust.1 ustawy z dnia 5 lipca 2018 r. o krajowym systemie cyberbezpieczeństwa[13].

(akta kontroli str. 713)

1.2. W dniu wejścia w życie przepisów RODO oraz u.o.d.o. (25 maja 2018 r .) w Szpitalu obowiązywała Polityka Bezpieczeństwa i Instrukcja Udostępniania Dokumentacji Medycznej wprowadzone w życie Zarządzeniem Prezesa Zarządu Szpitala nr 72/2014, która nie została zaktualizowana w związku z wejściem w życie rozporządzenia RODO[14], co szerzej opisano w dalszej części wystąpienia, w sekcji „Stwierdzone nieprawidłowości".

(akta kontroli str. 198-271)

W dniu 14 stycznia 2019 r. Prezes Zarządu Szpitala podpisał nową Politykę Bezpieczeństwa (dalej: *Polityka*), w której określono m.in.:

- osoby odpowiedzialne za ochronę danych osobowych w Szpitalu oraz ich zadania (ADO, ASI, IOD);
- sposób upoważniania do przetwarzania danych osobowych;
- sposób formułowania umów o powierzenie przetwarzania danych osobowych;
- zasady przetwarzania danych osobowych;
- ogólne zasady bezpieczeństwa przy przetwarzaniu danych osobowych;
- instrukcję postępowania w przypadku naruszenia ochrony danych osobowych;
- zasady kontroli przetwarzania i stanu zabezpieczenia danych osobowych;
- środki techniczne i organizacyjne niezbędne dla zachowania poufności; integralności i rozliczalności przetwarzanych danych osobowych.

W ośmiu załącznikach zawarto wzory dokumentów związanych ze stosowaniem Polityki, (m.in. w załączniku nr 7 zawarto Instrukcję Zarządzania Systemem Informatycznym służącym do przetwarzania danych osobowych).

(akta kontroli str. 198-232)

Zbiory danych i obszary przetwarzania danych osobowych zostały ujęte w opracowanej przez IOD w maju 2018 r. „Analizie ryzyka przetwarzania danych osobowych w NZOZ Szpital im. prof. Z. Religi w Słubicach sp. z o.o."[15] oraz podpisanej przez aktualnego Prezesa Zarządu „Ocenie skutków przetwarzania danych"[16]. Ponadto w Szpitalu opracowano do 25 maja 2018 r.[17]:

- Rejestr czynności przetwarzania danych osobowych[18],
- Rejestr Incydentów naruszenia ochrony danych osobowych[19] oraz
- Wykaz podmiotów, z którymi zostały zawarte umowy powierzenia przetwarzania danych osobowych[20].

(akta kontroli str. 114-176)

---

12 Według stanu na 31 marca 2019 r.

13 Dz. U. 2018 r. poz. 1560.

14 Polityka ta bazowała na niezaktualizowanych podstawach prawnych z 2014 r. i obejmowała m.in. nieaktualne bazy danych i użytkowanych programów takie jak HERZ (zastąpiony w 2016 roku przez SWD PRM czy Fontel i Silcan (niefunkcjonujący od kilku lat zbiór nagrań telefonicznych) oraz także niefunkcjonujące od kilku lat Rejestratory wideo SOR 1 i 2 oraz w korytarzu do Poradni Szpitalnych. Szpital od kilku lat nie przetwarza danych za pomocą ww. programów i sprzętu.

15 Analiza ta wskazała trzy zbiory danych pacjentów i pracowników Szpitala zawartych w programach: ESKULAP, RUM, SIMPLE Kadry, Płatnik.

16 W Ocenie skutków uwzględniono zbiory danych w programach: ESKULAP, RUM, SIMPLE Kadry, Płatnik, oraz IMPAX i ROCHE.

17 Dokumenty te zostały przez IOD przygotowane i odebrane przez Szpital.

18 W rejestrze tym uwzględniono zbiory danych zawarte w programie ESKULAP, ROCHE, SIMPLE ERP, PROCOMMERCE RUM, PŁATNIK oraz IMPAX.

19 Rejestr ten obejmuje 30 niewypełnionych dotychczas pozycji.

20 Przekazany w toku kontroli Wykaz umów powierzenia przetwarzania zawierał jedynie sześć pozycji.

Aktualnie w Szpitalu obowiązują następujące regulacje wewnętrzne dotyczące ochrony przetwarzanych danych osobowych:

1/ Instrukcja zarządzania systemem informatycznym do przetwarzania danych osobowych w Szpitalu[21];
2/ Polityka[22];
3/ Instrukcja udostępniania dokumentacji medycznej.[23]

(akta kontroli str. 198-271)

Ponadto w związku z wejściem w życie przepisów RODO w Szpitalu opracowano i wprowadzono do stosowania (od 25 maja 2018 r.) nowy wzór upoważnienia[24] do przetwarzania danych osobowych zawierający oświadczenie osób wykonujących pracę w Szpitalu[25] o zapoznaniu się z treścią i zobowiązaniu do przestrzegania i stosowania postanowień u.o.d.o. oraz RODO.

(akta kontroli str. 196-197)

Poza ASI[26] i Koordynatorem Działu Organizacyjnego, personelowi Szpitala nie udostępniono dokumentów opracowanych przez IOD w związku z wdrożeniem RODO. W szczególności pracownikom Szpitala nie udostępniano Polityki oraz „Instrukcji Zarządzania Systemem Informatycznym", natomiast informacja o zasadach polityki bezpieczeństwa i procedurach obowiązujących w zakresie przetwarzania danych osobowych była przekazana przez IOD w trakcie realizowanych przez niego szkoleń dla personelu Szpitala, co szerzej opisano w dalszej części wystąpienia, w sekcji „Stwierdzone nieprawidłowości".

(akta kontroli str. 714)

1.3. Rejestr czynności przetwarzania danych osobowych przetwarzanych w Szpitalu, o którym mowa w art. 30 RODO (dalej *Rejestr*) opracowany w maju 2018 roku obejmował wszystkie elementy wskazane w art. 30 ust.1 RODO oraz prowadzony był zgodnie z art.30 ust. 3 RODO w formie pisemnej (w tym elektronicznej), natomiast nie ujęto w nim wszystkich operacji przetwarzania danych jakie miały miejsce w Szpitalu[27], co szerzej opisano w dalszej części wystąpienia, w sekcji „Stwierdzone nieprawidłowości".

(akta kontroli str. 140-149)

1.4. W okresie objętym kontrolą IOD przeprowadził (ADO zatwierdził) jedną analizę procesów przetwarzania danych osobowych pacjentów Szpitala (dalej: Analiza), o której mowa w art. 32 RODO. Analiza została ograniczona do przetwarzania tych danych w zbiorach danych osobowych zawartych w systemach/programach elektronicznych: ESKULAP, ROCHE, SIMPLE ERP, PROCOMERCE RUM, PŁATNIK oraz IMPAX, co szerzej opisano w dalszej części wystąpienia, w sekcji „Stwierdzone nieprawidłowości".

Analiza ta nie objęła w szczególności przetwarzania danych osobowych dokonywanego w formie papierowej (dotyczy to m.in. bieżącego wypełniania i przekazywania dokumentacji medycznej pacjentów oraz dokumentacji personelu Szpitala[28] oraz niektórych operacji

---

21 Wprowadzona zarządzeniem wewnętrznym Dyrektora Szpitala nr 20/2011 z 29 kwietnia 2011 r.

22 Podpisana przez obecnego Prezesa Zarządu 14 stycznia 2019 r.

23 Wprowadzona Zarządzeniem nr 72/2014 z 1 grudnia 2014 r.

24 Zgodnie z treścią upoważnienie to było ważne na czas trwania zatrudnienia w Szpitalu. Wzór ten był jednakże stosowany do nowo przyjmowanych pracowników lub nowego personelu zatrudnianego w oparciu o umowy cywilnoprawne. W Szpitalu nie aktualizowano wcześniej wystawionych upoważnień do przetwarzania danych osobowych wystawione dla personelu już świadczącego pracę/usługi w Szpitalu.

25 Upoważnienie stosowano zarówno w przypadku osób zatrudnionych na podstawie umowy o pracę, jak i osób wykonujących pracę na podstawie umów cywilnoprawnych.

26 Administrator Systemów Informatycznych.

27 W rejestrze czynności przetwarzania nie ujęto m.in. przetwarzania danych osobowych pacjentów na terminalu WOŚP czy też wyłącznie papierowych zleceń transportu medycznego. Ujęto w nim natomiast operacje dokonywane w systemach/programach elektronicznych: ESKULAP, ROCHE, SIMPLE ERP, PROCOMERCE RUM, PŁATNIK oraz IMPAX.

28 W szczególności dotyczy to zleceń transportu medycznego, dla którego przetwarzanie danych osobowych następuje poza systemem typu HIS - ESKULAP, wyłącznie w formie papierowej.

dokonywanych w formie elektronicznej (wysyłanie wyników badań przesiewowych słuchu noworodków poprzez dedykowany terminal WOŚP)[29].

(akta kontroli str. 116-139)

W ramach ww. Analizy zidentyfikowano 5 zagrożeń (ryzyk) związanych z ochroną danych osobowych w pięciu grupach miejsc przetwarzania danych[30]. Dla każdego z nich oszacowano wartość ryzyka (w skali od 0 do 4 punktów) poprzez określenie parametrów dotyczących prawdopodobieństwa materializacji oraz skutków zdarzeń. Ryzyka określone na poziomie niższym lub równym poziomu maksymalnego 9,6 podlegały automatycznej akceptacji, ryzyka w przedziale od 9,6 do 38,4 monitorowaniu a powyżej 38,4 określono jako wymagające wdrożenia procesu interwencyjnego.

W rezultacie przeprowadzonej Analizy, jako stanowiące największe zagrożenie (poziom ryzyka – 48 pkt) wskazano: 1/ ryzyko utraty danych wynikające z organizacji i zabezpieczeń technicznych oraz 2/ ryzyko utraty danych wskutek awarii systemu teleinformatycznego. Wysokie ryzyka określone w zakresie teleinformatyki dotyczyły głównie organizacji serwerowni („pomieszczenie niedostosowane stwarzające duże zagrożenie dla sprzętu technicznego – brak skutecznego chłodzenia, ryzyko awarii zasilania, brak monitorowania. Zastrzeżenia IOD dotyczyły także braku bieżącej kontroli nad logowaniami personelu w systemie (udostępnianie haseł). W analizie nie wskazano koniecznych działań interwencyjnych, natomiast zapisano, że będą one realizowane na bieżąco przez ADO na podstawie audytów IOD.

(akta kontroli: str. 116-139)

IOD wyjaśnił, że wobec istotnych ryzyk w obszarze informatycznym całą uwagę skupiono na tym obszarze, natomiast do czasu wdrożenia nowych rozwiązań informatycznych wstrzymał się z wykonywaniem kolejnych audytów.

(akta kontroli: str. 421-424)

Informacje dotyczące stanu zabezpieczenia pomieszczeń serwerowni oraz użytkowanych w Szpitalu komputerów przedstawiono w pkt. 2.9. niniejszego wystąpienia.

1.5. Szpital nie był zobowiązany do wykonania oceny skutków dla ochrony danych (dalej: DPIA), o której mowa w art. 35 RODO. Obowiązek wykonania tej oceny dotyczy bowiem planowanych operacji przetwarzania dla ochrony danych osobowych przed rozpoczęciem ich przetwarzania, a Szpital, wraz z wejściem w życie RODO, nie rozpoczął przetwarzania nowych kategorii danych, w szczególności z użyciem nowych technologii, a także w Szpitalu nie funkcjonował systemu monitoringu wizyjnego.

Pomimo braku obowiązku w Szpitalu opracowano w drugiej połowie 2018 roku „Ocenę skutków przetwarzania dla ochrony danych" dla sześciu zbiorów danych: ESKULAP, ROCHE, SIMPLE ERP, PROCOMMERCE RUM, PŁATNIK, IMPAX. W „Ocenie skutków przetwarzania" podpisanej przez IOD i aktualnego Prezesa Zarządu wskazano, iż operacje przetwarzania są niezbędne oraz proporcjonalne w stosunku do celów a środki planowane do ograniczenia ryzyka opracowane zostaną w Polityce Bezpieczeństwa[31]. We wnioskach wskazano, iż „z uwagi na akceptowalny poziom ryzyka oraz adekwatność przetwarzanych danych osobowych, od konsultacji z Organem Nadzorczym odstąpiono".

(akta kontroli str. 158-176)

1.6. Jednym z zadań IOD, w myśl art. 39 ust. 1 lit. b RODO jest prowadzenie szkoleń personelu uczestniczącego w operacjach przetwarzania danych. W okresie objętym kontrolą IOD przeprowadził trzy udokumentowane szkolenia dla personelu Szpitala z zakresu ochrony danych osobowych w związku z wejściem w życie przepisów RODO:

---

[29] Szpital nie ma uprawnień administratora do komputera na którym wprowadzane są wyniki badań i dane matki i noworodka (PESEL oraz imię i nazwisko) do Centralnego Ośrodka Badań Słuchu w Poznaniu.

[30] 1/ Miejsca udzielania świadczeń medycznych, 2/ pozostałe pomieszczenia medyczne, 3/ pomieszczenia administracyjne, 4/ pomieszczenia kierownictwa oraz 5/ serwerownia i pomieszczenia informatyki.

[31] Nowa Polityka Bezpieczeństwa została podpisana przez obecnego prezesa Zarządu 14 stycznia 2019r.

- 25 maja 2018 r. dla 20 osób pełniących funkcje kierownicze w komórkach organizacyjnych Szpitala;
- 30 maja 2018 r. dla 23 osób z personelu administracyjnego i średniego personelu medycznego;
- 24 września 2018 r. dla 6 osób w POZ w Rzepinie, w tym kierownika, 4 pielęgniarek oraz 1 rejestratorki.

Udokumentowanym szkoleniem bezpośrednim przez IOD objęto zatem jedynie 49 osób z ponad 339 osobowego personelu Szpitala (14,45% personelu Szpitala), co szerzej opisano w dalszej części wystąpienia, w sekcji „Stwierdzone nieprawidłowości".

(akta kontroli str. 177-187)

1.7. Szpital nie zobowiązał się formalnie (np. poprzez deklarację stosowania) do przestrzegania regulacji zawartych w Kodeksie postępowania dla sektora ochrony zdrowia, dla którego wniosek o przyjęcie został 13 listopada 2018 r. przedłożony PUODO lub pozostałych opracowań związanych z ochroną danych osobowych, takich jak *Przewodnik po RODO w służbie zdrowia* i *Wytyczne dotyczące inspektorów ochrony danych.*

Była Prezes Zarządu wyjaśniła, że w październiku 2018 roku do personelu Szpitala skierowano *„Przewodnik po RODO w Służbie Zdrowia*" opracowany przez Ministerstwo Zdrowia oraz Ministerstwo Cyfryzacji. W przewodniku tym zawarto odpowiedzi na najczęściej zadawane pytania dotyczące przetwarzania danych osobowych w systemie ochrony zdrowia. Powyższy Przewodnik został przekazany personelowi Szpitala w formie elektronicznej w dniu 1 października 2018 roku.

(akta kontroli str. 272-290)

Stwierdzone nieprawidłowości

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

1/ Wbrew wymogom określonym w art. 24 ust.1 i 2 oraz art. 30 i art. 32 RODO Szpital nierzetelnie i z opóźnieniem aktualizował dokumentację i procedury związane z przetwarzaniem danych osobowych, tj.:

a) Politykę Bezpieczeństwa (nowa Polityka Bezpieczeństwa na potrzeby RODO została zatwierdzona dopiero w styczniu 2019 roku, a do tego czasu obowiązywała Polityka Bezpieczeństwa z 2014 r., która zawierała nieaktualne dane i informacje[32]);

b) Rejestr czynności przetwarzania danych, zawierał jedynie dane przetwarzane w sześciu głównych programach informatycznych; w Rejestrze nie ujęto natomiast informacji o przetwarzaniu danych na terminalu WOŚP[33] i przetwarzaniu danych dokonywane w formie papierowej[34]);

c) Analizę ryzyka przetwarzania danych osobowych w Szpitalu z maja 2014 r., która nie objęła wszystkich procesów przetwarzania danych osobowych w Szpitalu (nie uwzględniono przetwarzania danych w formie papierowej oraz przetwarzania danych poprzez terminal WOŚP).

(akta kontroli str. 116-149, 233-271)

Odnośnie b) i c) IOD wyjaśnił, że przygotowując swoje analizy i oceny bazował na informacjach przekazanych przez personel Szpitala. Dodał, że po zdiagnozowaniu istotnych

[32] W Polityce Bezpieczeństwa z 2014 roku pozostawiono m.in. nieaktualne wykazy obszarów oraz zbiorów przetwarzania danych osobowych takich jak HERZ czy FONTEL, SILCAN.

[33] Fakt przetwarzania danych na Terminalu WOŚP ujawniono dopiero w toku kontroli NIK. Pracownicy Szpitala nie potrafili wyjaśnić, czy przetwarzanie tych danych odbywa się w oparciu o umowę zawartą przez Szpital z podmiotem do którego przekazywane są wyniki badań przesiewowych słuchu u noworodków (wraz z danymi matki i dziecka).

[34] Dotyczy to zleceń transportu medycznego wystawianych w formie papierowej poza systemami informatycznymi Szpitala.

ryzyk w obszarze informatycznym, gdzie przetwarzanych jest większość danych osobowych w Szpitalu skoncentrowano się na tym obszarze. W jego ocenie w Szpitalu nie istnieją istotne ryzyka w zakresie przetwarzania danych w formie papierowej oraz dodał, że wstrzymał się z kolejnym audytem systemu ochrony danych szpitala do czasu wdrożenia nowych rozwiązań informatycznych związanych z projektem e zdrowie.

(akta kontroli str. 421-424)

Odnośnie a), b) i c) była Prezes Zarządu Szpitala wyjaśniła, że w maju 2018 roku przygotowano podstawowe dokumenty na potrzeby wdrożenia RODO i miały być one uzupełniane i aktualizowane, jednak brak realizacji niektórych zadań przez pracowników Szpitala oraz zapowiadane zmiany w Zarządzie Szpitala uniemożliwiły weryfikację stanu realizacji zadań w tym obszarze. Priorytetem było przygotowanie dokumentacji (wykazów, rejestrów, procedur) i pozyskanie środków na poprawę i dostosowanie infrastruktury informatycznej Szpitala, tak by można było wprowadzić skuteczny nadzór nad danymi osobowymi przetwarzanymi w głównych programach informatycznych Szpitala. Dodała, że schematu organizacyjnego Szpitala nie zaktualizowały[35] także osoby pełniące funkcję Prezesa Zarządu Szpitala po jej odejściu.

(akta kontroli str. 707-712)

2/ IOD nie wywiązał się w pełni z obowiązku prowadzenia szkoleń personelu uczestniczącego w operacjach przetwarzania danych, wynikającego z art. 39 ust. 1 lit. b RODO. Udokumentowanymi szkoleniami w zakresie obowiązywania przepisów RODO objęto niespełna 15% personelu Szpitala. Pozostali pracownicy mieli korzystać z przygotowanych dla nich w maju 2018r. materiałów informacyjnych i szkoleniowych zamieszczonych w Intranecie Szpitala. Nie weryfikowano jednak, ile osób spośród personelu Szpitala skorzystało z tej formy szkolenia. Szkolenia przeprowadzone przez IOD w 2018 roku nie objęły także rozwiązań wskazanych w Polityce Bezpieczeństwa wprowadzonej w styczniu 2019 roku.

(akta kontroli str. 421-424)

IOD wyjaśnił, że szkoleń było około dziesięć, jednak był problem z zebraniem personelu medycznego na szkolenie i zdecydowano się na kontynuację szkolenia z RODO w formie e-lerningu. Nie zwracał on uwagi na sposób dokumentowania realizowanych szkoleń. Na stronie intranetowej Szpitala zamieszczono materiały szkoleniowe i informacyjne dla personelu Szpitala, jednak IOD nie posiada informacji ile osób faktycznie skorzystało z tej formy szkolenia.

(akta kontroli str. 182-187, 422, 715-722)

OCENA CZĄSTKOWA

Szpital wywiązał się z obowiązku opracowania dokumentacji oraz procedur uwzględniających przepisy RODO. Jednak ich dostosowanie do nowych regulacji nastąpiło dopiero po ponad siedmiu miesiącach od wejścia w życie RODO, a część z niej nie była w pełni kompletna. Wywiązano się także z obowiązku powołania na stanowisko IOD osoby posiadającej odpowiednie przygotowanie i kwalifikacje zawodowe oraz terminowo dokonano zgłoszenia tego faktu do PUODO. Opracowany terminowo Rejestr czynności przetwarzania, a także przeprowadzona analiza ryzyka procesów przetwarzania danych nie były kompletne, gdyż nie objęły wszystkich operacji przetwarzania danych.

Nie w pełni zrealizowano także obowiązek przeszkolenia pracowników Szpitala uczestniczących w procesie przetwarzania danych osobowych z zagadnień dotyczących bezpieczeństwa danych oraz obowiązywania przepisów RODO, gdyż tylko niespełna 15% tych pracowników zostało objętych udokumentowani szkoleniami.

[35] W Biuletynie Informacji Publicznej (dalej BIP) Szpitala na dzień 1 kwietnia 2019 r. figurował nieaktualny od 1 listopada 2017 r. zapis o stanowisku „specjalisty ds. IT i ochrony danych osobowych" (aktualnie „specjalisty ds. IT). Schemat organizacyjny Szpitala nie uwzględnia ani IOD, ani ABI ani ASI (którym jest osoba na stanowisku specjalisty ds. IT).

OBSZAR

2. Zapewnienie prawidłowego przetwarzania i ochrony danych osobowych.

2.1. Przeprowadzone oględziny trzech objętych badaniem rejestracji w Szpitalu [36] wykazały, że w celu właściwej ochrony danych osobowych pacjentów funkcjonowały poniżej wymienione rozwiązania:

- w każdej rejestracji umieszczono klauzule informacyjne spełniające wymogi art. 13 RODO (naklejone karty na szybę lub ścianę) ogólnodostępne dla osób rejestrujących się;
- zapewniono, aby w obrębie wzroku pacjenta znajdującego się przy stanowisku rejestracji nie znajdowały się dokumenty zawierających dane osobowe innych pacjentów. Dokumenty osób już zarejestrowanych były na bieżąco przenoszone do gabinetów zabiegowych lub poradni Szpitala;
- wszystkie komputery (cztery) znajdujące się w rejestracjach było ustawione w sposób uniemożliwiający wgląd w treści na nich wyświetlane osobom rejestrującym się;
- pacjenci poradni urazowo-ortopedycznej otrzymywali numerki, w pozostałych przypadkach w rejestracji wskazywano ustnie nr gabinetu;
- 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;
- identyfikacja pacjentów odbywała się na podstawie okazanych rejestratorce dowodów tożsamości wg kolejności przyjścia do rejestracji (brak urządzeń elektronicznych wspomagających proces rejestracji);
- w każdej z rejestracji znajdowały się zamykane na klucz szafki do przechowywania dokumentacji pacjentów;
- przed okienkiem rejestracji Poradni RTG oraz dwoma okienkami do wspólnej Rejestracji do Poradni Chirurgii Ogólnej oraz Chirurgii Urazowo-Ortopedycznej pacjenci zachowywali odległość od osoby dokonującej rejestracji zgodnie z pisemną instrukcją dla rejestrujących się zamieszczoną przy okienkach do ww. rejestracji.

(akta kontroli str. 693-696)

We wszystkich trzech objętych oględzinami gabinetach poradni specjalistycznych Szpitala[37], dokumentację pacjentów przechowywano we właściwy sposób, tj. pacjent wchodzący do gabinetu nie miał możliwości zapoznania się z danymi osobowymi innych osób oczekujących w kolejce lub tych, którzy odbyli już wizytę. Ponadto w trakcie oględzin, nie zaobserwowano, aby którykolwiek gabinet został pozostawiony bez opieki oraz nie stwierdzono przypadków pozostawienia klucza w drzwiach i opuszczenia przez personel gabinetu poradni. Wywoływanie pacjentów wszystkich poradni odbywało się w sposób gwarantujący im anonimowość, tj. pacjenci wchodzili do gabinetu poradni wg otrzymanego numeru (Poradnia urazowo-ortopedyczna) lub kolejności przyjścia (pacjenci ustalali kolejność wejść samodzielnie bez wywoływania).

(akta kontroli str. 697-699)

Przeprowadzone oględziny dyżurek pielęgniarskich, sal chorych oraz gabinetów lekarskich na trzech oddziałach szpitalnych[38] wykazały m.in., że:

- na oddziałach znajdowało się łącznie: 19 sal chorych (49 łóżek), trzy gabinety lekarskie oraz trzy dyżurki pielęgniarskie;

---

[36] Tj.: 1. Izby Przyjęć Szpitala, Rejestracji do Poradni RTG i wspólnej Rejestracji do Poradni Chirurgii Ogólnej i Chirurgii Urazowo-Ortopedycznej.

[37] Oględzinami objęto trzy poradnie: 1. Poradnia chirurgii urazowo-ortopedycznej, 2. Poradnia chirurgii ogólnej 3. Poradnia gastroenterologiczna.

[38] Oględzin objęto trzy oddziały szpitalne (sale chorych, dyżurki pielęgniarskie, gabinety lekarskie) tj.: 1. Oddział Chorób Wewnętrznych 2. Oddział Szpitalno-Ratunkowy (SOR), 3. Oddział Ginekologiczno-Położniczo-Noworodkowy.

- w przypadku wszystkich 23 zaobserwowanych pacjentów nie stwierdzono braku na nadgarstku pacjenta opaski informacyjnej zawierającej numer historii choroby i nazwę Oddziału[39];
- na dwóch oddziałach[40] nie stwierdzono umieszczania kart z danymi pacjentów na lub przy łóżkach pacjentów, natomiast na zajętych łóżkach (14) na Oddziale Chorób wewnętrznych, zamieszczono odwrócone karty z imieniem i nazwiskiem pacjentów w sposób uniemożliwiający odczytanie tych danych dla osób przebywających w tych salach (w tym osób postronnych np. odwiedzających chorych);
- ruch chorych[41] prowadzony był w dyżurkach pielęgniarskich w miejscu niewidocznym dla osób postronnych;
- we wszystkich dyżurkach pielęgniarskich podręczna dokumentacja pielęgniarska przechowywana była w zamykanych na klucz szafkach, nie stwierdzono nieprawidłowości w zakresie sposobu użytkowania i zabezpieczenia komputerów w dyżurkach (ogółem trzy);
- w gabinetach lekarskich dokumentacja medyczna przechowywana była w zamykanych na klucz szafkach, nie stwierdzono nieprawidłowości w zakresie sposobu użytkowania i zabezpieczenia komputerów w gabinetach.

Ponadto w ramach przeprowadzonych oględzin stwierdzono, że w Szpitalu (na żadnym z oddziałów, rejestracji, poradni) nie funkcjonował monitoring wizyjny.

(akta kontroli str. 684-699)

2.2. Według stanu na 4 kwietnia 2019 r. personel działów administracyjnych[42] Szpitala liczył 70 osób. Analiza uprawnień nadanych 30 osobom z tej grupy w systemie ESKULAP[43], wykazała, że sześciu osobom nadano uprawnienia w systemie medycznym, przy czym odpowiadały one zakresom zadań i obowiązków realizowanych przez tych pracowników. I tak:

- 24 osoby z 30 badanych nie posiadały dostępu do systemu ESKULAP, co wynikało z ich zakresów obowiązków (nie realizowali oni zadań wymagających dostępu do danych medycznych pacjentów Szpitala),
- 6 osób z 30 badanych posiadło nadane uprawnienia w tym systemie, które pozwalały im na dostęp do danych medycznych niezbędny z punktu widzenia realizowanych przez nich zadań (ograniczony dostęp do zakresu zadań np. tylko do apteki szpitalnej, magazynu leków).

(akta kontroli str. 189-194,429-519)

2.3. Analiza przeprowadzona na próbie 30 pielęgniarek i położnych (ze 134)[44] wykazała, m.in. że:

- 28 osób posiadało pisemne upoważnienia ADO[45] do przetwarzania danych osobowych, w tym 4 upoważnienia zawierały nieaktualne podstawy prawne, co szerzej opisano w dalszej części wystąpienia, w sekcji „Stwierdzone nieprawidłowości";
- 1 osoba miała nadane uprawnienia w systemie ESKULAP[46], pomimo braku pisemnego upoważnienia ADO do przetwarzania danych osobowych co szerzej opisano w dalszej części wystąpienia, w sekcji „Stwierdzone nieprawidłowości".

---

39 Opaski wypisywane byłe ręcznie i zwierały wyłącznie nazwę Oddziału oraz nr historię choroby, po którym identyfikowano pacjenta.

40 Tj.: Oddział Ginekologiczno-Położniczo-Noworodkowy, Oddział Szpitalno-Ratunkowy (SOR).

41 Ruch chorych to lista pacjentów danego oddziału wraz z numerem sali, w których przebywają.

42 Biuro Zarządu, Dział Kadr, Dział Księgowości, Dział Administracyjno-Gospodarczy, Dział Zamówień Publicznych, Dział Rozliczeń i Analiz, stanowiska samodzielne w Administracji Szpitala.

43 System typu HIS (*Hospital Information System* – rodzaj oprogramowania do obsługi ruchu pacjentów wewnątrz podmiotu leczniczego).

44 Na umowę o pracę oraz umowy cywilnoprawne (zlecenie) - stan na 4 kwietnia 2019 r.

45 Pisemnego upoważnienia ADO do przetwarzania danych osobowych nie posiadała pielęgniarka przypisana według karty stanowiskowej do Oddziału Ortopedycznego oraz pielęgniarka przypisana do Nocnej i Świątecznej Opieki Pacjenta (umowa cywilnoprawna).

– 5 osób (tj. 16,7% próby), posiadało nadane uprawnienia do komórek innych niż stanowiska wskazane przez dział kadr;
– 7 osób (tj. 23,3% próby), oprócz dostępu do danych medycznych pacjentów w komórkach organizacyjnych, na których według dokumentów kadr świadczyły pracę, posiadało nadane uprawnienia do innych komórek organizacyjnych Szpitala (zbyt szeroko nadane uprawnienia), co szerzej opisano w dalszej części wystąpienia, w sekcji „Stwierdzone nieprawidłowości".

(akta kontroli str. 520-629, 723-738)

Ustalono, że żadnej osobie spośród osób zatrudnionych lub wykonujących na podstawie umów cywilnoprawnych[47] zadania salowej lub sprzątaczki[48] nie nadano uprawnień w systemie ESKULAP, natomiast upoważnienia ADO do przetwarzania danych osobowych w zakresie wynikającym z zajmowanego stanowiska nadano ośmiu salowym, co szerzej opisano w dalszej części wystąpienia, w sekcji „Stwierdzone nieprawidłowości".

(akta kontroli str.429-519)

2.4. W okresie od 25 maja 2018 r. do 31 grudnia 2018 r. Szpital rozwiązał stosunek pracy/umowę cywilnoprawną z 14 osobami. Spośród nich, trzy osoby w trakcie zatrudnienia/świadczenia zadań miało przyznany dostęp do systemów informatycznych, w tym systemu ESKULAP. Przeprowadzona analiza terminu odebrania uprawnień wszystkim ww. osobom wykazała, że:

– w przypadku wszystkich trzech osób dostęp do systemów informatycznych dotyczył danych medycznych;
– w trzech ww. przypadkach dostęp do systemu ESKULAP został zablokowany w toku kontroli NIK (w dniach 4 i 5 marca 2019 r.), tj. po upływie od 68 do 220 dni od daty rozwiązania stosunku pracy/umowy cywilnoprawnej[49], co szerzej opisano w dalszej części wystąpienia, w sekcji „Stwierdzone nieprawidłowości".

(akta kontroli str. 678-680)

2.5. W myśl postanowień umowy serwisowej Szpital obowiązany był do zgłaszania błędów w działaniu systemu ESKULAP poprzez witrynę internetową help-desk'u wykonawcy znajdującą się pod adresem http://helpdesk.konsultant-it.pl .

Przeprowadzone oględziny sposobu przekazania 48 (100%) zgłoszeń serwisowych z okresu od 25 maja 2018 r. do 12 marca 2019 r. związanych z błędami lub wadliwym działaniem systemu informatycznego ESKULAP wykazały m.in., że:

– wszystkie zgłoszenia serwisowe były przekazywane przez ASI, przy czym w dniu oględzin 41 zgłoszeń miało status „zamknięty", a 7 zgłoszeń[50] (przekazane w dniach 5 września, 23 listopada, 4 grudnia 2018 oraz 28 i 31 stycznia oraz 5 i 12 marca 2019 r.) status „aktywne/podjęte",
– wszystkie zgłoszenia zrealizowano drogą elektroniczną z wykorzystaniem ww. serwisu internetowego, przy czym w przypadku jednego ze zgłoszeń przekazywano dane osobowe pacjenta (imię i nazwisko) co szerzej opisano w dalszej części wystąpienia, w sekcji *„Stwierdzone nieprawidłowości"*.

(akta kontroli str. 681-683)

2.6. Szpital w okresie objętym kontrolą posiadał 7 umów dotyczących powierzenia przetwarzania danych osobowych, w których wystąpił jako podmiot powierzający

---

46 Dotyczyło to jednej pielęgniarki (uprawnienia nadano 3 lipca 2018 r.) i jednej sekretarki medycznej (uprawnienia nadano 18 lipca 2016 r.).
47 Ogółem 33 osoby - stan na 13 marca 2019 r.
48 W toku kontroli nie stwierdzono wystawienia pisemnych upoważnień do przetwarzania danych osobowych lub nadania uprawnień w systemach medycznych Szpitala osobom sprzątającym.
49 Czwarta osoba zmieniła jedynie formę zatrudnienia (nadal świadczy pracę na podstawie umowy cywilnoprawnej).
50 Pięć z tych zgłoszeń oznaczonych było jako gwarancyjne, jedno wdrożeniowe i jedno serwisowe.

przetwarzanie danych, 1 umowy gdzie wskazano go jako podmiot przetwarzający dane osobowe oraz 2 umowy o wzajemnym powierzeniu przetwarzania danych osobowych.

(akta kontroli str. 393-396)

Ustalono, że umowy dotyczące powierzenia przetwarzania danych zawierano z podmiotami (wykonawcami) realizującymi na rzecz Szpitala zadania związane m.in. ze: świadczeniem usług informatycznych oraz serwisu oprogramowania, badaniami z zakresu diagnostyki obrazowej, usługami laboratoryjnymi, współpracy i konsultacji medycznych.

Analiza pięciu umów (porozumień)[51] dotyczących powierzenia przez Szpital przetwarzania danych osobowych pięciu wykonawcom, ww. usług wykazała m.in. że:

- zawierały one wymagane postanowienia określone w art. 28 ust. 3 RODO i stanowiły integralną część umowy na świadczenie usług zawartej z danym podmiotem zewnętrznym,
- w każdej z pięciu umów powierzenia wskazany zakres danych osobowych, jaki został powierzony przez Szpital podmiotowi zewnętrznemu, wynikał z rodzaju usług, jakie zgodnie z umową na ich świadczenie miał na rzecz Szpitala realizować wykonawca.

Analiza dokumentacji Szpitala dotyczącej zlecanych podmiotom zewnętrznym badań z okresu 25.05.2018 – 31.12.2018 r. wykazała, że Szpital zlecał badania przekazując dane pacjentów także do innych podmiotów (czterech) bez zawierania umowy powierzenia danych, co szerzej opisano w dalszej części wystąpienia, w sekcji „Stwierdzone nieprawidłowości".

(akta kontroli str. 294-366, 370-383, 397-403)

Analiza wykazu zawartych umów wykazała, że ujęto w nim 6 spośród 10 zawartych umów co szerzej opisano w dalszej części wystąpienia, w sekcji „Stwierdzone nieprawidłowości".

(akta kontroli str. 305-315, 367-369, 393-396)

2.7. W obowiązującej w Szpitalu Polityce Bezpieczeństwa zawarto m.in. „Instrukcję Postępowania w sytuacji naruszenia ochrony danych osobowych i danych istotnych" a także wzór raportu dokumentującego przypadek naruszenia bezpieczeństwa danych. Analiza zapisów ww. Instrukcji wskazuje, że w Szpitalu wprowadzono m.in.:

- obowiązek niezwłocznego zgłoszenia do IOD informacji o naruszeniu bezpieczeństwa danych oraz przeprowadzenie postępowania wyjaśniającego z udziałem IOD w terminie 72 godzin od stwierdzenia naruszenia;
- obowiązek zgłoszenia organowi nadzoru każdego przypadku naruszenia ochrony danych osobowych skutkującego ryzykiem naruszenia praw lub wolności osób fizycznych w terminie 72 godzin po stwierdzeniu naruszenia (art. 33 ust. 1 RODO).

(akta kontroli str. 215-216, 226)

W okresie objętym kontrolą w Szpitalu nie odnotowano przypadków (incydentów) naruszenia ochrony danych osobowych.

(akta kontroli str.150-156, 421-424)

2.8. W Szpitalu obowiązuje „Instrukcja udostępniania dokumentacji medycznej" wprowadzona zarządzeniem Prezesa Szpitala nr 72/2014 z 1 grudnia 2014r. (nie została ona zaktualizowana w związku z wdrażaniem RODO). Ponadto na stronie internetowej Szpitala udostępniono wniosek o udostępnienie dokumentacji medycznej.

(akta kontroli str. 233, 258-271)

W myśl tych regulacji oraz zgodnie z przepisem art. 26 ust. 1 oraz ust. 3 ustawy z dnia 6 listopada 2008 r. o prawach pacjenta i Rzeczniku Praw Pacjenta[52] (dalej: *u.o.p.p.*), dokumentację medyczną udostępnia się pacjentowi lub jego przedstawicielowi

[51] Badanem objęto umowy zawarte z Ventamed Sp. z o.o., SPS dla NiPCh, Konsultant IT sp. z o.o., Starmedica oraz Konsultant Komputer sp. z o.o.

[52] Dz. U. z 2017 r. poz. 1318, ze zm.

ustawowemu, bądź osobie upoważnionej przez pacjenta oraz podmiotom określonym w ust. 3 ww. przepisu. Ponadto w procedurach wewnętrznych określono m.in. wzór wniosku o udostępnienie dokumentacji medycznej.

W okresie objętym kontrolą w Szpitalu informacje o udostępnieniu dokumentacji medycznej każdorazowo ujmowano w wykazie, o którym mowa w art. 27 ust. 4 u.o.p.p.

W okresie od 25 maja 2018 r. do 14 marca 2019 r. do Szpitala wpłynęło 111 pisemnych wniosków o udostępnienie dokumentacji medycznej, z czego tylko w jednym przypadku Szpital nie udostępnił dokumentacji na wniosek sądu, gdyż pacjent nie był leczony w Szpitalu (błędnie skierowany wniosek). Spośród 110 przypadków udostępnienia przez Szpital dokumentacji na pisemny wniosek, 17 dotyczyło komercyjnych podmiotów sektora ubezpieczeniowego a 10 osobom fizycznym – pacjentom.

(akta kontroli str. 258-260, 667-671)

Badanie 17 przypadków udostępnienia dokumentacji medycznej podmiotom sektora ubezpieczeniowego wykazało, że:

- Szpital udostępniał dokumentację medyczną wyłącznie poprzez przesłanie drogą pocztową oryginałów lub uwierzytelnionych odpisów dokumentacji - zgodnie z przyjętą w Szpitalu Instrukcją udostępniania dokumentacji medycznej (Szpital nie udostępniał dokumentacji medycznej w formie elektronicznej);
- we wszystkich 17 przypadkach dotyczących udostępnienia dokumentacji podmiotom sektora ubezpieczeniowego, Szpital dysponował pisemną zgodą pacjenta na udostępnienie dokumentacji medycznej ww. podmiotom;
- wszystkie zbadane wnioski o udostępnienie dokumentacji medycznej złożone zostały przez podmioty uprawnione do żądania wydania dokumentacji medycznej pacjentów;
- osoba udostępniająca dane w imieniu Szpitala każdorazowo posiadała wymagane upoważnienie.

(akta kontroli str. 258-260, 667-671)

2.9. Regulacje dotyczące ochrony danych przed ich utratą w wyniku awarii, błędów lub nieuprawnionej modyfikacji zostały opisane w Polityce Bezpieczeństwa (rozdział 6, 9 oraz załącznik nr 4- Środki techniczne i organizacyjne niezbędne dla zapewnienia poufności, integralności i rozliczalności przetwarzanych danych osobowych i danych istotnych) oraz w *Instrukcji Zarządzania Systemem Informatycznym służącym do przetwarzania danych osobowych*[53] (dalej: *Instrukcja*).

W dokumentach tych określono m.in.: [1] stosowane metody i środki uwierzytelnienia oraz procedury związane z ich zarządzaniem i użytkowaniem; [2] procedury rozpoczęcia, zawieszenia i zakończenia pracy przeznaczone dla użytkowników systemu informatycznego służącego do przetwarzania danych; [3] procedury tworzenia kopii zapasowych zbiorów danych oraz programów i narzędzi służących do ich przetwarzania; [4] sposób, miejsce i okres przechowywania nośników informacji zawierzających dane osobowe oraz kopii zapasowych; [5] sposób zabezpieczenia systemu informatycznego służącego do przetwarzania danych osobowych przed działalnością oprogramowania, którego celem jest uzyskanie nieuprawnionego dostępu do systemu informatycznego służącego do przetwarzania danych osobowych; [6] sposób odnotowania informacji o odbiorcach, którym dane osobowe zostały udostępnione, dacie i zakresie tego udostępnienia; [7] procedury wykonywania przeglądów i konserwacji systemów oraz nośników informacji służących do przetwarzania danych osobowych; [8] pozostałe zasady ochrony systemu informatycznego służącego do przetwarzania danych osobowych.

(akta kontroli str. 198-232)

[53] Stanowiącej załącznik nr 7 do Polityki Bezpieczeństwa.

Oględziny jedynej serwerowni Szpitala[54] wykazały, m.in. że właściwie: [1] zabezpieczono dostęp do tego pomieszczenia, stosując drzwi na zamek otwierany kluczem (w pomieszczeniu brak jest okien); [2] w pomieszczeniu umieszczono gaśnicę typu D (wolnostojącą) oraz układ klimatyzacji; [3] na wypadek czasowego zaniku zasilania zastosowano układy podtrzymujące napięcie UPS (1 szt.); [4] wszystkie urządzenia informatyczne zamontowano w specjalnie do tego przystosowanych szafach typu RACK [5] w serwerowni nie pozostawiono w niej elementów, materiałów, urządzeń niezwiązanych z funkcjonowaniem serwerowni, które mogłyby wywołać ryzyko pożaru lub sprzyjać jego rozprzestrzenieniu. Ponadto ustalono, że w serwerowni brak jest tzw. podłogi antystatycznej oraz tzw. podłogi technicznej, natomiast widoczne były rury mogące stanowić potencjalne zagrożenie zalaniem.

(akta kontroli str. 700-706)

Kopie zapasowe baz danych Szpitala, w myśl przepisów § 20 ust. 2 pkt 12 lit. b rozporządzenia KRI oraz postanowień Instrukcji, były przechowywane w pomieszczeniu znajdującym się w innym niż serwerownia budynku Szpitala[55].

Oględziny tego pomieszczenia wykazały, że przyjęte w nim rozwiązania i stwierdzony stan faktyczny nie zapewniały pełnego bezpieczeństwa przechowywanych w nim kopii baz danych z uwagi na: [1] drzwi do pomieszczenia zamykane były na jeden zamek patentowy a okna (dwa) nie posiadały żadnych zabezpieczeń; [2] pomieszczenie nie jest objęte systemem kontroli dostępu i było użytkowane jako pomieszczenie biurowe dla pracowników Działu Logistyki; [3] w pomieszczeniu brak było, systemu klimatyzacji; [4] w pomieszczeniu umiejscowiono rury CO, które w razie awarii mogłyby zalać szafy, w których przechowywane są kopie danych.

(akta kontroli str. 700-706)

W Szpitalu dotychczas nie wdrożono jeszcze środków eliminujących lub ograniczających ryzyko zdarzeń[56], a serwerownia i objęte oględzinami pomieszczenie na przechowywanie kopii zapasowych baz danych nie posiadały systemu alarmowego, przeciwwłamaniowego ani przeciwpożarowego.

(akta kontroli str. 700-706)

ASI wyjaśnił, że Szpital od 2011 roku starał się pozyskać środki finansowe poprawienie stanu infrastruktury informatycznej Szpitala, jednak udało się je uzyskać dopiero w 2018 roku w ramach Projektu E-Zdrowie. Projekt ten jest w trakcie realizacji.

(akta kontroli: str. 411)

W docelowej wizji informatyzacji Szpitala w ramach projektu Lubuskie e-Zdrowie[57] wskazano m.in., że w ramach tego projektu w Szpitalu przewidywana jest m.in. przebudowa serwerowni, zakup serwera i macierzy dyskowej wraz z oprogramowaniem systemowym, wdrożenie domeny z uwzględnieniem polityki bezpieczeństwa oraz zakup licencji i oprogramowania HIS wraz z wdrożeniem. Do dnia zakończenia niniejszej kontroli ww. projekt był w trakcie przygotowania[58].

(akta kontroli str. 410-412)

---

[54] Jedyna Serwerownia umiejscowiona w Budynku głównym Szpitala (na drzwiach brak było oznaczeń informujących o przeznaczeniu tego pomieszczenia) , w której znajdowały się serwery z bazami danych medycznych, w tym dane osobowe pacjentów Szpitala oraz pracowników.

[55] Pomieszczenie umiejscowione w odrębnym budynku administracyjnym Szpitala oddalonym około 20-30 m od budynku głównego Szpitala, w którym przechowywane są kopie zapasowe baz danych, w tym danych osobowych pacjentów.

[56] Przyjęte w Szpitalu rozwiązania nie spełniają wymogów art.56 ust.1 ustawy z dnia 28 kwietnia 2011 r. o systemie informacji w ochronie zdrowia.

[57] Opracowanym na zlecenie Urzędu Marszałkowskiego Województwa Lubuskiego, wersja sierpień 2018 r.

[58] http://bip.lubuskie.pl/zamowienia_publiczne/11/487/E2_80_9ESwiadczenie_uslugi_nadzoru_sprawowanego_w_imieniu_Zamawiajacego_w_zakresie_prawidlowosci_realizacji_Projektu_pod_nazwa__E2_80_9ELubuskie_e-Zdrowie_E2_80_9D_2C__0D_0Aw_charakterze_Inzyniera_Kontraktu__E2_80_9D_0D_0A/ - dostęp 21.03.2019 r.

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

- na komputerach z dostępem do programów medycznych Szpitala hasła były zgodne z wymogami Polityki Bezpieczeństwa i podlegały okresowej zmianie;
- żaden z 30 komputerów nie był zarządzany domenowo;
- na 3 komputerach zainstalowany był system operacyjny Windows XP, a na jednym Windows Vista, dla których producent oprogramowania zakończył wsparcie techniczne odpowiednio 8 kwietnia 2014 r. oraz 11.04.2017r., a po tym dniu producent przestał dostarczać aktualizacje zabezpieczeń, poprawki niezwiązane z zabezpieczeniami, bezpłatne lub płatne opcje asystowanej pomocy technicznej i aktualizacje zawartości technicznej online, co znacznie wpływa na bezpieczeństwo tych systemów operacyjnych. W związku z tym w Szpitalu istnieje potencjalna możliwość, iż urządzenia te stwarzają ryzyko dla bezpieczeństwa infrastruktury informatycznej jednostki, które może skutkować nieprawidłowościami w przyszłości;
- na 27 z 30 badanych komputerów użytkownicy mieli dostęp do uprawnień administratora[59], które pozwalały na wprowadzanie zmian w konfiguracji tych urządzeń oraz instalację oprogramowania, co szerzej opisano w dalszej części wystąpienia, w sekcji „Stwierdzone nieprawidłowości";
- na 27 komputerach z 30 objętych badaniem[60] zainstalowany był program antywirusowy z aktualną bazą sygnatur wirusów;
- w 28 komputerach nie zostały zablokowane porty USB, umożliwiając podłączenie do nich nośników pamięci i kopiowanie danych;
- 22 komputerów było wykorzystywanych do przetwarzania danych osobowych, w tym w systemie ESKULAP 20 (dane medyczne), a 2 do przetwarzania danych osobowych pracowników Szpitala (SIMPLE-Księgowość i SIMPLE –Kadry);
- na 16 komputerach użytkowanych wspólnie przez personel medyczny, użytkownicy logowali się do systemu operacyjnego z użyciem wspólnego loginu i hasła, co szerzej opisano w dalszej części wystąpienia, w sekcji „Stwierdzone nieprawidłowości";
- w 15 przypadkach hasło do systemu operacyjnego Windows było niezgodne z zasadami przyjętymi w Polityce Bezpieczeństwa Szpitala (zbyt mała liczba znaków lub brak spełnienia wymogów złożoności hasła), co szerzej opisano w dalszej części wystąpienia, w sekcji „Stwierdzone nieprawidłowości".

(akta kontroli str. 630-666)

Kopie zapasowe baz danych – stosownie do wymogów określonych w Polityce – wykonywane były raz na dobę poprzez zrzut na Serwer Backup'owy oraz dodatkowo na szyfrowane, zewnętrzne dyski twarde przechowywane w szafie pancernej w odrębnym od serwerowni budynku. W Szpitalu nie stosowano pseudonimizacji danych ani ochrony kryptograficznej nośników pamięci.

(akta kontroli str. 713)

Stwierdzone nieprawidłowości

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

1. Administrator danych osobowych w Szpitalu wadliwie udzielał pisemnych upoważnień do przetwarzania danych osobowych a Administrator systemów informatycznych wadliwie nadawał uprawnienia do systemów informatycznych Szpitala. I tak, badanie uprawnień

---

[59] Na jednym komputerze zabezpieczono dostęp do uprawnień administratora hasłem ASI, a dwa komputery poddane badaniom administrowane były przez podmioty zewnętrzne (Fundacja WOŚP oraz Roche Diagnostics Polska sp. z o. o.), które udostępniły Szpitalowi komputery w ramach zawartych umów o świadczenie usług medycznych.

[60] W jednym wypadku brak było możliwości ustalenia czy na komputerze zainstalowano taki program – Szpital posiada tylko uprawnienia użytkownika, a na jednym komputerze w Laboratorium nie było dostępu do programów medycznych). W jednym przypadku program antywirusowy zainstalowano na komputerze z dostępem do programu Eskulap w trakcie oględzin - Komputer lekarski na Oddziale szpitalno-ratunkowym (SOR).

nadanych 30 osobom z personelu niemedycznego oraz 30 osobom z personelu medycznego (położne i pielęgniarki) wykazało, że:

a) ośmiu salowym niezgodnie z zakresem realizowanych zadań wystawiono pisemne upoważnienia ADO do przetwarzania danych osobowych, w tym dwóm do przetwarzania danych w systemach informatycznych Szpitala[61];

b) 4 z 29 pisemnych upoważnień do przetwarzania danych osobowych wydane przez ADO pielęgniarkom i położnym Szpitala zawierało niezaktualizowane podstawy prawne, (przywołano art.37 ustawy z dnia 29 sierpnia 1997r. o ochronie danych osobowych (Dz.U.2016r. poz.922);

c) dwóm pielęgniarkom[62] ADO nie wydał pisemnych upoważnień do przetwarzania danych osobowych, mimo, iż zakres ich obowiązków wskazywał, że mogą przetwarzać dane osobowe;

d) jednej pielęgniarce[63] ASI nadał uprawnienia w systemie ESKULAP pomimo braku wydania przez ADO pisemnego upoważnienia do przetwarzania danych osobowych;

e) 5 pielęgniarkom (tj. 16,7% badanej próby) ASI nadał uprawnienia do innych komórek organizacyjnych Szpitala, niż wynikało to z dokumentów kadrowych (karty stanowiskowe, umowy cywilnoprawne)[64];

f) 7 pielęgniarkom (tj. 23,3% badanej próby), oprócz dostępu do danych medycznych pacjentów w komórkach organizacyjnych, na których świadczyły pracę, ASI pozostawił nadane uprawnienia do innych komórek organizacyjnych Szpitala (zbyt szeroko nadane uprawnienia) [65].

Powyższe stanowiło naruszenie art.5 ust.1 lit.c RODO (zasada adekwatności przetwarzania danych osobowych i minimalizacji danych) oraz § 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 (dalej: rozporządzenie KRI), zgodnie z którym należy podejmować działania polegające na bezzwłocznej zmianie uprawnień, w przypadku zmiany zadań osób zaangażowanych w proces przetwarzania informacji.

(akta kontroli str. 497, 507, 509,678-680, 723-738)

Ad a), b) i c) Prezes Zarządu Szpitala wyjaśnił, że obszar nadawanych upoważnień i uprawnień w systemach informatycznych do przetwarzania danych osobowych wymaga przeglądu i aktualizacji, w związku z czym w Szpitalu zadanie to zostanie przypisane osobie, której zadaniem będzie uporządkowanie we współpracy z IOD i ASI dokumentacji dotyczącej przetwarzania danych osobowych w Szpitalu.

(akta kontroli str. 413-415)

---

61 Salowe te nie posiadały jednak uprawnień nadanych przez ASI do systemu ESKULAP.

62 Pielęgniarka przypisana do Oddziału Ortopedycznego (nie posiadała także nadanych uprawnień przez ASI do programu ESKULAP) oraz pielęgniarka przypisana do Nocnej i Świątecznej Opieki Pacjenta, która miała nadane przez ASI uprawnienia do tego obszaru w programie ESKULAP.

63 Pielęgniarka przypisana do Nocnej i Świątecznej Opieki Pacjenta (NiŚOP).

64 1/ Pielęgniarka przypisana do OIOM miała nadane uprawnienia do Bloku operacyjnego, 2 / Pielęgniarka przypisana do ZRM miała nadane uprawnienia do Izby Przyjęć i SOR, 3/ Pielęgniarka przypisana do ZRM miała nadane uprawnienia do Oddziału Pediatrycznego, 4/ Pielęgniarka przypisana do ZRM miała nadane uprawnienia do Oddziału Chirurgii Ogólnej, 5/ Pielęgniarka przypisana do ZRM miała nadane uprawnienia do Izby Przyjęć i Oddziału Chirurgii Ogólnej.

65 1/ Położna przepisana do Poradni w Słubicach posiadała nadane uprawnienia do Poradni w Górzycy, 2/ Pielęgniarka przypisana do OIOM posiadała uprawnienia także do Bloku Operacyjnego; 3/ pielęgniarka przypisana do Oddziału Chirurgii posiadała także uprawnienia do Oddziału Ginekologiczno-Położniczego, 4/ pielęgniarka przypisana do OIOM posiadała uprawnienia do Bloku Operacyjnego, 5/ pielęgniarka przypisana do SOR posiadała uprawnienia do Izby Przyjęć i Nocnej i Świątecznej Opieki Pacjenta, 6/ Pielęgniarka przypisana do OIOM posiadała uprawnienia także do Bloku Operacyjnego,7/ pielęgniarka przypisana do Oddziału Chirurgii posiadała także uprawnienia do Oddziału Ginekologiczno-Położniczego.

Ad. d) e) i f) ASI wyjaśnił, że przyczyną tego stanu była niewłaściwa komunikacja z komórką kadr Szpitala.

(akta kontroli str. 410-412)

2. Konta użytkownika w systemie ESKULAP, trzech byłych pracowników Szpitala, zostały zablokowane dopiero w toku kontroli NIK (w dniach 4 i 5 marca 2019 r.), tj. po upływie od 68 do 220 dni od daty rozwiązania stosunku pracy/umowy cywilnoprawnej.

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.

(akta kontroli str. 678-679)

Administrator systemów informatycznych wyjaśnił, że przyczyną tego stanu był brak otrzymania stosownej informacji z działu kadr Szpitala.

(akta kontroli str. 410-412)

3. Sposób użytkowania i zabezpieczenia wykorzystywanych w Szpitalu komputerów (badaniami objęto 30 komputerów) nie gwarantował pełnej ochrony danych osobowych pacjentów i był niezgodny postanowieniom Polityki Bezpieczeństwa Szpitala, gdyż:

   a) w 16 przypadkach (na 30 zbadanych) użytkownicy korzystali ze wspólnych loginów i haseł;

   b) w 15 przypadkach hasło do systemu operacyjnego Windows, było niezgodne z przyjętymi zasadami (zbyt mała liczba znaków lub hasło nie spełniało wymogów złożoności);

   c) w 27 przypadkach użytkownicy mieli uprawnienia administratora do systemu komputerowego, tym samym posiadali oni możliwość instalacji dowolnego oprogramowania jako administrator (na 20 z tych komputerów był dostęp do programu medycznego ESKULAP);

   d) na 2 komputerach lekarskich, użytkownicy przetwarzali dane osobowe pacjentów poza programem ESKULAP (w folderze moje dokumenty stwierdzono pliki zawierające dane medyczne (wypisy, historie chorób, plan zabiegów, dane pacjentów);

   e) na 2 komputerach w chwili oględzin nie był zainstalowany program antywirusowy, przy czym na komputerze z dostępem do programu Eskulap[66] program ten zainstalowano w trakcie oględzin - Komputer lekarski na Oddziale szpitalno-ratunkowym (SOR).

(akta kontroli str. 630-653)

W myśl przepisu § 20 ust. 2 pkt 7 i 9 rozporządzenia KRI, kierownictwo podmiotu publicznego jest obowiązane do podejmowania działań zapewniających ochronę przetwarzanych informacji przed ich kradzieżą, nieuprawnionym dostępem, uszkodzeniami lub zakłóceniami, a także zabezpieczenia przetwarzanych informacji w sposób uniemożliwiający nieuprawnionemu jej ujawnienie, modyfikację, usunięcie lub zniszczenie. Dodatkowo, zgodnie z przepisem § 20 ust. 2 pkt 12 ww. rozporządzenia, zapewnienie odpowiedniego poziomu bezpieczeństwa w systemach teleinformatycznych polega w szczególności na dbałości o aktualizację oprogramowania, minimalizowaniu ryzyka utraty informacji w wyniku awarii oraz ochronie przed błędami, utratą, nieuprawnioną modyfikacją. W myśl art. 5 ust. 1 lit. f RODO, dane osobowe muszą być przetwarzane w sposób zapewniający odpowiednie bezpieczeństwo danych osobowych, w tym ochronę przed niedozwolonym lub niezgodnym z prawem przetwarzaniem oraz przypadkową utratą, zniszczeniem lub uszkodzeniem, za pomocą odpowiednich środków technicznych lub organizacyjnych („integralność i poufność"). Opisane działania były także niezgodne z postanowieniami Polityki Bezpieczeństwa oraz z § 20 ust. 2 pkt. 7 lit. a i § 21 ust. 2 pkt 3, w związku z § 20 ust. 1 rozporządzenia KRI, gdyż bez przyznania indywidualnych loginów

[66] Na drugim komputerze (komputer w Laboratorium) brak było dostępu do programów i danych medycznych.

użytkownikom, nie jest możliwa prawidłowa rozliczalność systemów. Taki sposób autoryzacji nie pozwala na ustalenie, która z osób fizycznych używających tego samego (jednego) loginu, przetwarzała w systemach (w tym przypadku w systemie operacyjnym) dane podlegające prawnej ochronie.

Ad a) i b) i e) Administrator systemów informatycznych w Szpitalu wyjaśnił, że jest to wynikiem ograniczeń finansowych Szpitala, braku wdrożenia zarządzania domenowego oraz fakt, iż głównym celem zabezpieczeń były programy medyczne, a nie systemy operacyjne komputerów. W przypadku programów medycznych logowanie następuje za pomocą indywidualnych loginów i haseł zgodnie z przyjętą w Szpitalu Polityką Bezpieczeństwa. Docelowo problemy zostaną rozwiązane po wdrożeniu zarządzania domenowego.

(akta kontroli str. 410-412)

Ad c) Administrator systemów informatycznych w Szpitalu wyjaśnił, że jednym z powodów pozostawienia użytkownikom komputerów kadry medycznej uprawnień administratora, była konieczność dostępu do dysku C:/ na potrzeby aktualizacji programu ESKULAP.

(akta kontroli str. 642-652)

Ad d) Administrator systemów informatycznych w Szpitalu wyjaśnił, że przetwarzanie danych osobowych pacjentów poza systemem ESKULAP wynikało z braku pełnej funkcjonalności programu ESKULAP na komputerach użytkowanych przez lekarzy, co spowodowane było zbyt małą liczbą licencji posiadanych przez Szpital.

(akta kontroli str. 411, 642-652)

4. W dziesięciu przypadkach Szpital zawarł i realizuje umowy główne w zakresie zlecania lub realizacji świadczeń zdrowotnych na rzecz pacjentów (własnych lub kontrahenta) lub usług serwisowych programów informatycznych, w których przetwarzane są dane osobowe, a tylko sześć z nich ujęto w prowadzonym wykazie umów powierzenia przetwarzania danych. Ponadto stwierdzono cztery przypadki, w których Szpital do czasu kontroli NIK nie podjął działań w celu zawarcia umowy powierzenia przetwarzania danych[67] mimo faktycznego powierzania podmiotom zewnętrznym, co stanowiło naruszenie przepisu art. 28 RODO.

   W myśl przepisu § 20 ust. 2 pkt 7 i 9 rozporządzenia KRI, kierownictwo podmiotu publicznego jest obowiązane do podejmowania działań zapewniających ochronę przetwarzanych informacji przed ich kradzieżą, nieuprawnionym dostępem, uszkodzeniami lub zakłóceniami, a także zabezpieczenia przetwarzanych informacji w sposób uniemożliwiający nieuprawnionemu jej ujawnienie, modyfikację, usunięcie lub zniszczenie. Dodatkowo, zgodnie z przepisem § 20 ust. 2 pkt 12 ww. rozporządzenia, zapewnienie odpowiedniego poziomu bezpieczeństwa w systemach teleinformatycznych polega w szczególności na dbałości o aktualizację oprogramowania, minimalizowaniu ryzyka utraty informacji w wyniku awarii oraz ochronie przed błędami, utratą, nieuprawnioną modyfikacją. W myśl art. 5 ust. 1 lit. f RODO, dane osobowe muszą być przetwarzane w sposób zapewniający odpowiednie bezpieczeństwo danych osobowych, w tym ochronę przed niedozwolonym lub niezgodnym z prawem przetwarzaniem oraz przypadkową utratą, zniszczeniem lub uszkodzeniem, za pomocą odpowiednich środków technicznych lub organizacyjnych („integralność i poufność").

   (akta kontroli str. 291-366, 393-396)

Osoba odpowiedzialna w Szpitalu za prowadzenie wykazu umów powierzenia przetwarzania danych osobowych wyjaśniła, że wobec natłoku licznych obowiązków związanych z bieżącą obsługą Zarządu Szpitala i nadzorem nad realizacją zadań przez podległe komórki organizacyjne przez przeoczenie nie uzupełniała na bieżąco prowadzonego wykazu. Dodała, że na niektóre przypadki zlecania badań (np. w Laboratorium firmy Roche) lub wysyłania wyników badań (Terminal WOŚP)

[67] Dotyczyło to zlecanych usług zdrowotnych lub przekazywanych wyników badań pacjentów na Terminalu WOŚP, Laboratorium Roche Diagnostics, Medycznego Centrum Laboratoryjnego Diagnostyka z Gorzowa Wlkp., Nowego Szpitala w Kostrzynie n/Odrą.

nie zwrócono uwagi, stąd Szpital dopiero w trakcie kontroli NIK podjął starania o zawarcie umów powierzenia przetwarzania danych z tymi podmiotami.

(akta kontroli str. 404-405)

5. W jednym przypadku Szpital naruszył art.5 ust.1 lit.c) i 32 RODO oraz art. 24 ust.2 ustawy o prawach pacjenta i rzeczniku Praw Pacjenta[68] poprzez wysłanie w jednym zgłoszeniu serwisowym danych osobowych pacjenta (imię i nazwisko) bez pisemnego polecenia i upoważnienia ADO.

(akta kontroli str. 681-683)

ASI wyjaśnił, że przesłanie imienia i nazwiska pacjenta w opisie zgłoszenia serwisowego nastąpiło przez jego przeoczenie, dostrzeżono ten błąd dopiero w trakcie badań kontrolnych NIK.

(akta kontroli str. 410-412)

OCENA CZĄSTKOWA

W Szpitalu wdrożono rozwiązania organizacyjne i techniczne zmierzające do zapewnienia prawidłowej ochrony i przetwarzania danych osobowych. Nie były one jednak w pełni przestrzegane.

Prawidłowo chroniono i przetwarzano dane osobowe w skontrolowanych trzech Oddziałach szpitalnych, trzech poradniach specjalistycznych, a także w punktach rejestracji do poradni szpitalnych oraz szpitalnej Izbie Przyjęć.

Personelowi Szpitala nie zapewniono jednakże odpowiedniego dostępu do danych medycznych. Stwierdzono w toku kontroli przypadki pisemnych upoważnień, wydanych w oparciu o nieaktualne przepisy, braku wymaganej precyzji i adekwatności poprzez pozostawienie zbyt szerokich uprawnień, nadawania upoważnień personelowi, który nie realizował zadań związanych z przetwarzaniem danych osobowych, a także odbierania ze znacznym opóźnieniem możliwości dostępu do tych systemów byłym pracownikom Szpitala.

Szpital nie we wszystkich wymaganych przypadkach zawierał także umowy powierzenia przetwarzania danych a prowadzony wykaz podmiotów z którymi zawarto takie umowy był niekompletny. Natomiast w pięciu analizowanych umowach powierzenia przetwarzania zamieszczono postanowienia wymagane art. 28 RODO.

Szpital prawidłowo udostępniał uprawnionym podmiotom dokumentację medyczną pacjentów, a funkcjonujący w Szpitalu wykaz udostępniania tych danych był zgodny z obowiązującymi wymogami.

W administrowanych przez Szpital komputerach poddanych badaniom nie zapewniono pełnej zgodności z Polityką Bezpieczeństwa. Należy zauważyć, że sposób użytkowania i zabezpieczenia wykorzystywanych w Szpitalu komputerów nie gwarantował – wskutek m.in. nieprzestrzegania wymogów dotyczących obowiązujących haseł oraz możliwości instalowania dowolnego oprogramowania – pełnej ochrony przetwarzanych na tych komputerach danych osobowych pacjentów.

Stan użytkowanej serwerowni i pomieszczenia, w którym Szpital przechowuje kopie danych nie zapewnia maksymalnej ochrony przed skutkami zdarzeń losowych, jednak w Szpital jest w trakcie wdrażania nowych rozwiązań w zakresie infrastruktury informatycznej, co powinno wpłynąć na poprawę stanu zabezpieczenia danych przetwarzanych w Szpitalu.

IV. Uwagi i wnioski

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

Wnioski pokontrolne

1/ Objęcie szkoleniami z zakresu ochrony danych osobowych wszystkich pracowników Szpitala uczestniczących w przetwarzaniu tych danych.

2/ Zaktualizowanie wydanej na potrzeby RODO dokumentacji i procedur a także pisemnych upoważnień ADO oraz nadanych uprawnień ASI do przetwarzania

[68] Dz. U. 2017 r. poz.1318, ze zm.

danych osobowych przez personel Szpitala, w sposób zapewniający adekwatność nadanych uprawnień do zajmowanych stanowisk i realizowanych obowiązków;

3/ Dostosowanie infrastruktury informatycznej Szpitala do wymogów art.56 ust.1 ustawy z dnia 28 kwietnia 2011 r. o systemie informatyzacji w ochronie zdrowia oraz zapewnienie zgodności z przyjętą w Szpitalu Polityką Bezpieczeństwa i Instrukcją Zarządzania Systemem Informatycznym służącym do przetwarzania danych osobowych (sprzęt, oprogramowanie, organizacja ochrony i zabezpieczeń).

4/ Nadawanie pracownikom upoważnień ADO i nadawanych przez ASI uprawnień w systemach informatycznych oraz w systemach operacyjnych komputerów Szpitala w stopniu adekwatnym do realizowanych przez nich zadań, a także bezzwłoczne odbieranie uprawnień w systemach informatycznych byłym pracownikom Szpitala.

5/ Podjęcie skutecznych działań w celu zawarcia z wszystkimi kontrahentami Szpitala umów powierzenia przetwarzania danych osobowych w sytuacji, kiedy występuje przetwarzanie tych danych przez Szpital lub kontrahenta Szpitala.

6/ Zapewnienie przestrzegania obowiązujących w Szpitalu i wynikających z przyjętej Polityki Bezpieczeństwa - zasad logowania do programów operacyjnych oraz wymogów dotyczących jakości stosowanych haseł.

7/ Wyeliminowanie sytuacji, w których przetwarzanie danych osobowych odbywałoby się poza dedykowanym i należycie zabezpieczonym programem medycznym.

8/ Zaktualizowanie rejestru przetwarzania danych osobowych o obszary związane z przetwarzaniem dokumentacji w formie papierowej (zlecenia transportu medycznego) oraz przetwarzanie danych na terminalu WOŚP.

9/ Podjęcie działań zapewniających brak nieuzasadnionego udostępnienia danych osobowych pacjentów w przypadkach zgłaszania tzw. help desk, dotyczących pomocy serwisowej udzielanej przez podmioty zewnętrzne w zakresie użytkowanych przez szpital programów informatycznych zawierających dane osobowe, w szczególności dane medyczne pacjentów pochodzące z programu ESKULAP.

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 Zielonej Górze. Prawo zgłaszania zastrzeżeń, zgodnie z art. 61b ust. 2 ustawy o NIK, nie przysługuje do wystąpienia pokontrolnego zmienionego zgodnie z treścią uchwały w sprawie zastrzeżeń.

Obowiązek poinformowania NIK o sposobie wykonania wniosków

Zgodnie z art. 62 ustawy o NIK należy poinformować Najwyższą Izbę Kontroli, w terminie 30 dni 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.

Zielona Góra, 19 kwietnia 2019 r.

Najwyższa Izba Kontroli
Delegatura w Zielonej Górze
Dyrektor
Włodzimierz Stobrawa

.....
podpis

Kontroler
Krzysztof Hofman
Specjalista k.p.

.....
podpis