NAJWYŻSZA IZBA KONTROLI
Delegatura w Zielonej Górze

LZG.410.002.02.2019

Pani
Wanda Szumna
Prezes Powiatowego Centrum Zdrowia Sp. z o.o.
Szpital w Drezdenku
ul. Piłsudskiego 8, 66-530 Drezdenko

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	Powiatowe Centrum Zdrowia Sp. z o.o., ul. Piłsudskiego 8, 66-530 Drezdenko (dalej: *Szpital* lub *Spółka*).
Kierownik jednostki kontrolowanej	Wanda Szumna, Prezes Zarządu Spółki od 31 grudnia 2015 r.
Zakres przedmiotowy kontroli	1. Opracowanie wymaganej dokumentacji oraz procedur związanych z ochroną przetwarzanych danych osobowych. 2. Zapewnienie prawidłowego przetwarzania i ochrony danych osobowych.
Okres objęty kontrolą	Od 25 maja 2018 r. (data wejścia w życie przepisów RODO[1]) do dnia zakończenia czynności kontrolnych[2].
Podstawa prawna podjęcia kontroli	Art. 2 ust. 2 ustawy z dnia 23 grudnia 1994 r. o Najwyższej Izbie Kontroli[3]
Jednostka przeprowadzająca kontrolę	Najwyższa Izba Kontroli Delegatura w Zielonej Górze
Kontroler	Tomasz Przybysz, inspektor kontroli państwowej, upoważnienie do kontroli nr LZG/5/2019 z dnia 7 stycznia 2019 r.

(akta kontroli str.1-2)

1 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*.

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

3 Dz. U. z z 2019 r. poz. 489., dalej: *ustawa o NIK*.

II. Ocena ogólna[4] kontrolowanej działalności

OCENA OGÓLNA

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

Uzasadnienie oceny ogólnej

Szpital terminowo opracował wymaganą dokumentację oraz procedury związane z ochroną przetwarzanych danych osobowych, a także powołano na stanowisko Inspektora Ochrony Danych (dalej: *IOD*) osobę posiadającą odpowiednie przygotowanie i kwalifikacje zawodowe oraz zgłoszono ten fakt Prezesowi Urzędu Ochrony Danych Osobowych (dalej: *PUODO*). Opracowany terminowo Rejestr czynności przetwarzania zawierał wszystkie wymagane elementy. Przeprowadzono także analizę procesów przetwarzania danych oraz ocenę skutków przetwarzania danych osobowych. Personel Szpitala uczestniczący w procesie przetwarzania danych osobowych został przeszkolony z zagadnień dotyczących bezpieczeństwa danych oraz obowiązywania przepisów RODO.

Wprowadzone rozwiązania organizacyjne, zmierzające do zapewnienia ochrony danych osobowych pacjentów, gwarantowały poszanowanie ich prywatności. Prawidłowo chroniono i przetwarzano dane osobowe w skontrolowanych trzech oddziałach szpitalnych, trzech poradniach specjalistycznych, a także w trzech rejestracjach, a stwierdzona w tym obszarze nieprawidłowość dotyczyła jedynie braku zamieszczenia klauzul informacyjnych RODO oraz stosowania znaków identyfikacyjnych pacjentów (opasek) zapisywanych w sposób umożliwiający ich identyfikację przez osoby nieuprawnione.

Personelowi Szpitala zapewniono odpowiedni dostęp do danych medycznych. Wystąpiło jednak pięć (na 30 badanych) przypadków nadania pielęgniarkom zbyt szerokich uprawnień[5], a także odbieranie ze znacznym opóźnieniem możliwości dostępu do tych systemów byłym pracownikom Szpitala[6].

Zastosowano fizyczne zabezpieczenia serwerowni Szpitala, w których przechowywano dane osobowe przetwarzane w formie elektronicznej, natomiast sposób użytkowania i zabezpieczenia wykorzystywanych w Szpitalu komputerów stacjonarnych (badaniami objęto 30 komputerów) nie gwarantował pełnej ochrony przetwarzanych na tych komputerach danych osobowych pacjentów wskutek możliwości instalowania oprogramowania przez użytkowników komputerów[7], praktyki logowania się do systemu operacyjnego z użyciem wspólnego loginu i hasła[8] i nieodbierania uprawnień byłym pracownikom.

Szpital zawierał umowy powierzenia przetwarzania danych w sytuacjach tego wymagających, a w pięciu analizowanych umowach zamieszczono postanowienia wymagane art. 28 RODO. Prawidłowo udostępniano również uprawnionym podmiotom dokumentację medyczną pacjentów.

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

---

4 Najwyższa Izba Kontroli formułuje ocenę ogólną jako ocenę pozytywną, ocenę negatywną albo ocenę w formie opisowej.

5 Pięć pielęgniarek, oprócz dostępu do danych medycznych pacjentów w komórkach organizacyjnych, na których świadczyły pracę, posiadały również dostęp do danych pacjentów z innych oddziałów.

6 W przypadku 8 z 9 byłych pracowników Szpitala dostęp do systemów informatycznych z danymi pacjentów zablokowano dopiero po upływie od 62 do 87 dni od zakończenia pracy (z tego w pięciu przypadkach w toku kontroli NIK).

7 Stwierdzono w 30 z 30 badanych przypadków.

8 Stwierdzono w 20 z 30 badanych przypadków.

III. Opis ustalonego stanu faktycznego oraz oceny cząstkowe[9] kontrolowanej działalności

OBSZAR

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

Opis stanu faktycznego

1.1. Stosownie do art. 8 ustawy z dnia 10 maja 2018 r. o ochronie danych osobowych (dalej: u.o.d.o.)[10], Zarząd Spółki powołał w Szpitalu z dniem 2 lipca 2018 r. Inspektora Ochrony Danych Osobowych (dalej: *IOD*)[11]. W zarządzeniu powołującym IOD wskazano m.in., że służbowo podlega on bezpośrednio Zarządowi Spółki, co było zgodne z przepisem art. 38 ust. 3 RODO[12]. Osoba wyznaczona na IOD nie pełniła przed wejściem w życie przepisów RODO funkcji Administratora Bezpieczeństawa Informacji Szpitala (dalej: *ABI*).

Prezes Zarządu wyjaśniła, iż powodem niepowołania IOD od dnia 25 maja 2018 r. było poszukiwanie odpowiedniego kandydata na powyższe stanowisko. Obowiązki te do dnia 1 lipca 2018 roku pełnił ABI.

Szpital terminowo zawiadomił Prezesa Urzędu Ochrony Danych Osobowych (dalej: *PUODO*) o wyznaczeniu na stanowisko IOD[13], a zawiadomienie zawierało wszystkie elementy wymagane przepisem art. 10 ust. 3 u.o.d.o.

Dane kontaktowe IOD (numer telefonu oraz adres email) zgodnie z treścią art. 37 ust. 7 RODO, udostępniono na stronie internetowej Szpitala[14].

(dowód: akta kontroli str. 5-6, 7, 248, 250-251, 254-255)

Zgodnie z wymogami art. 37 ust. 5 RODO osoba wyznaczona na IOD posiadała odpowiednie kwalifikacje, w szczególności ukończyła certyfikowany kurs Inspektora Ochrony Danych „Szkolenia i warsztaty, RODO w placówce medycznej".

(dowód: akta kontroli str. 249)

Do dnia zakończenia kontroli NIK, fakt wyodrębniania w strukturze Szpitala stanowiska IOD, nie został uwzględniony w obowiązującym Regulaminie Organizacyjnym[15] oraz Statucie[16] Spółki.

Prezes Zarządu wyjaśniła, iż (…) *Regulamin Organizacyjny Szpitala jest ściśle powiązany ze Statutem Powiatowego Centrum Zdrowia Sp. z o.o., którego zmiana wymaga podjęcia uchwały przez zgromadzenie wspólników. W związku z tym, że wszystkie udziały w spółce należą do Powiatu Strzelecko – Drezdeneckiego, prace związane z dostosowaniem w/w dokumentów do obowiązujących aktów prawnych, zostały zawieszone na czas ukonstytuowania się nowych władz samorządowych. Powiatowe Centrum Zdrowia Sp. z o.o. jest w trakcie opracowywania nowego Statutu, a także Regulaminu Organizacyjnego Szpitala Powiatowego, które będą uwzględniały wszystkie założenia dotyczące funkcjonowania Szpitala oraz nowe uwarunkowania prawne, w tym obejmujące między innymi IOD.*

(dowód: akta kontroli str. 145-161, 162-166, 233-234)

---

9 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.

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

11 Zarządzeniem nr 23/2018 z dnia 02.07.2018 r. w sprawie powołania Inspektora Ochrony Danych Osobowych (dalej: zarządzenie 23/2018).

12 Osoba pełniąca funkcję IOD wykonywała równolegle inne zadania i obowiązki wynikające z jej stanowiska pracy (Inspektor w Dziale Finansowo-Kadrowym), przy czym zadania te nie wyoływały konflktu interesów z zadaniamy przypisanymi IOD.

13 Zawiadomienia dokonano w dniu 16 lipca 2018 r. na formularzu elektronicznym.

14 Strona internetowa: szpital-drezdenko.pl/rodo/

15 Stanowiącym załącznik do Zarządzenia nr 39/2014 z dnia 30.10.2014 r.

16 Stanowiącym załącznik do uchwały Zgromadzenia Wspólników Powiatowego Centrum Zdrowia Sp. z o.o. w Drezdenku z dnia 18.07.2016 r.

Szpital do dnia 8 kwietnia 2019 r. nie został uznany (nie otrzymał decyzji administracyjnej od właściwego organu do spraw cyberpezpieczeństwa) za operatora usługi kluczowej, o którym mowa w art. 5 ust. 1 ustawy z dnia 5 lipca 2018 r. o krajowym systemie cyberbezpieczeństwa[17].

(dowód: akta kontroli str. 250-251)

1.2. Przed dniem wejścia w życie przepisów RODO w Szpitalu funcjonowała Instrukcja Zarządzania Systemem Informatycznym służącym do przetwarzania danych osobowych[18]. Opisywała ona m.in.: zasady przydziału haseł dla użytkowników, procedurę rozpoczęcia i zakończenia pracy przy komputerze, nadawanie, modyfikowanie i blokowanie uprawnień w systemach informatycznych, metody i częstotliwość tworzenia kopii awaryjnych oraz sposób i czas ich przechowywania, dokonywanie przeglądów systemu i zbioru danch osobowych.

Po wejściu w życie RODO w Szpitalu zaczął[19] obowiązywać Regulamin Ochrony Danych Osobowych, w którym wskazano wykaz obowiązków z zakresu przestrzegania zasad ochrony danych osobowych zgodnie z przepisami RODO. W dokumencie opisano m.in. zasady: użytkowania sprzętu IT, dotyczące nadawania uprawnień i polityki haseł, zabezpieczania dokumentacji, korzystania z poczty elektronicznej oraz sieci Internet, postępowania w przypadku naruszenia ochrony danych osobowych.

W Szpitalu w okresie od 30 kwietnia do 31 lipca 2018 r. przeprowadzony został audyt, którego celem było określenie stanu funkcjonowania całości systemu informatycznego i jego zarządzania.[20] W wyniku przeprowadzonego audytu, w celu dostosowania dokumentacji dotyczącej ochrony danych osobowych do przepisów RODO w Szpitalu opracowano i przyjęto[21] Politykę Ochrony Danych Osobowych (dalej: *Polityka*). W Polityce opisano m.in. zasady ochrony danych osobowych przetwarzanych w formie papierowej oraz w systemach elektronicznych w celu spełnienia wymagań RODO u.o.d.o., i zawarto m.in.: Regulamin ochrony danych osobowych, wykaz przetwarzanych zbiorów danych osobowych, rejestr lista zagrożeń podatności, rejestr powierzeń danych osobowych przez administratora, procedurę analizy ryzyka, analizę ryzyka przetwarzanych danych osobowych, ocenę skutków przetwarzania danych osobowych (dotyczy systemu monitoringu wizyjnego), rejestr naruszeń danych osobowych, raport z naruszenia ochrony danych osobowych, zgłoszenie naruszenia ochrony danych osobowych, rejestr czynności przetwarzania danych osobowych, procedurę audytów, plan ciągłości (dotyczący planów awaryjnych systemu informatycznego po awarii, w przypadku braku zasilania, na wypadek utraty dostępu do sieci Internet, a także zasad sporządznia kopii zapasowych). Szpital posiadał opracowany komplet dokumentów wskazanych w Polityce.

Opracowana dokumentacja obowiązująca w Szpitalu dotycząca ochrony danych osobowych nie była aktualizowana do zakończenia kontroli NIK, z uwagi na brak przesłanek uzasadniających taką zmianę.

(dowód: akta kontroli str. 79-127, 167-176, 209-213)

1.3. Szpital od 25 maja 2018 r. wprowadził rejestr czynności przetwarzania danych osobowych, który zgodnie z wymogami art. 30 ust. 3 RODO prowadzony był w formie pisemnej i elektronicznej (arkusz Excel). Rejestr zawierał wszystkie dane wymagane przepisem art. 30 ust. 1 RODO. Według stanu na dzień 15 lutego 2019 r. liczył on 18 pozycji.

(dowód: akta kontroli str. 217-221)

---

17 Dz. U. poz. 1560.

18 Instrukcja przyjęta zarządzeniem wewnętrznym nr 11/2010 z dnia 28 lipca 2010 r. Prezesa Powiatowego Centrum Zdrowia Sp. z o.o. w Drezdenku.

19 Tj. Od dnia 31 lipca 2019 r.

20 Ze sprawozdania z realizacji audytu sporządzonego 31 lipca 2018 r. wynika, iż analizie poddano m.in.: procedury, hasła dostępowe, autoryzacje, infrastrukturę, sprzęt oraz oprogramowanie. Badano dokumentację za okres 01.01.2016 r. – 31.10.2017 r.

21 W dniu 31 lipca 2018 r.

1.4. Stosownie do art. 32 RODO w Szpitalu dokonano analizy zachodzących procesów przetwarzania danych osobowych[22] poprzez oszacowanie poziomu ryzyka dla siedmiu zasobów[23] przeznacznych do przetwarzania danych osobowych. Nieakceptowalną wartość ryzyka wskazano na poziomie dziewięciu punktów. Jako opcjonalne (akceptowane lub obniżane) określono ryzyko w przedziale 3-6 pkt. Dla ww. zasobów jako poziom ryzyka wskazano: w jednym przypadku – 4 pkt. (outsourcing), w pięciu przypadkach – 6 pkt. (m.in. Personel, Pomieszczenia biurowe, Rejestracja, Składnica akt), w jednym przypadku dotyczącym punków dystrybucji (serwerownie, IDF, stacje robocze, drukarki, bazy danych, oprogramowanie) wskazano 9 pkt. W analizie wskazano wnioski z których wynika, iż należy podjąć działania w celu obniżenia potencjalnego ryzyka, które zostały wskazane w sprawozdaniu z przeprowadzonego audytu.

W przypadku punktów dystrybucji wskazano, iż w serwerowni należy: uporządkować pomieszczenia serwerowni poprzez usunięcie zbędnego sprzętu i rzeczy, właściwie umieścić wszystkie urządzeń, zakupić gaśnice CO2, podłączyć zasilacz UPC, zakupić oprogramowanie antywirusowe. Powyższe działania zostały zrealizowane. W przypadku stacji roboczych zalecono: wprowadzenie wymuszania zmiany haseł, zabezpiecyć wejścia USB, wykonywać kopie bezpieczeństwa, zabrać użytkownikom lokalnym prawa administracyjne. W przypadku stacji roboczych nie wykonano wszystkich zaleceń.

Zgodnie z zapisami art. 32 RODO Szpital w celu zapewnienia odpowiedniego stopnia bezpieczeństwa posiadał opracowane procedury dotyczące m.in.: tworzenia i przechowywania kopii baz danych, planów awaryjnych na wypadek awarii systemu informatycznego lub braku zasilania. Ponadto zgodnie z procedurą dotyczącą przeprowadzania audytów, IOD był odpowiedzialny za przeprowadzanie audytów z zakresu ochrony danych osobowych przynajmniej raz w roku. W szpitalu od 31 lipca 2018 r. prowadzono rejestr w którym ujęto wykaz stosowanych zabezpieczeń[24].

(dowód: akta kontroli str. 5, 177-204, 205-208)

1.5. W Szpitalu w trakcie przeprowadzonego audytu sporządzono ocenę skutków dla ochrony danych (dalej: *DPIA*), o której mowa w art. 35 RODO, dla funkcjonującego systemu monitoringu wizyjnego.

Wynika z niej, iż system monitoringu w Szpitalu wykazuje zgodność z przepisami RODO oraz zapewnia akceptowalny poziom ryzyka naruszenia praw lub wolności osób fizycznych, których dane osobowe objęte są jego procesem przetwarzania. Realizowane zadania przetwarzania w systemie monitoringu Szpitala są niezbędne i proporcjonalne w stosunku do realizowanych celów.

W Szpitalu nie wykonano oceny skutków ochrony danych dla innych operacji przetwarzania danych, o której mowa w art. 35 RODO – bowiem jej wykonanie w przypadku Szpitala jest fakultatywne. 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.

(dowód: akta kontroli str. 214-216)

1.6. Jednym z zadań IOD, w myśl art. 39 ust. 1 lit. b RODO jest prowadzenie szkoleń personelu uczestniczącego w operacjach przetwarzania danych. Kwestie przeprowadzania szkoleń zostały również określone w Zarządzeniu nr 23/2018 Prezesa Zarządu Spółki w sprawie powołania IOD, gdzie wskazano, że do zadań IOD należy m.in. szkolenie personelu uczestniczącego w operacjach przetwarzania danych osobowych.

---

[22] Na dokumencie brak jest daty jego sporządzenia. IOD wyjaśniła, iż został on sporządzony 31 lipca 2018 r.

[23] 1) Punkty dystrybucji (serwerownia, IDF, stacje robocze, drukarki, bazy danych, oprogramowanie); 2) Pomieszczenia biurowe (kadry, księgowość, rozliczania z NFZ, sekretariat – akta osobowe pracowników, stacje robocze, archiwum, oprogramowanie); 3) Personel; 4) Outsourcing; 5) Rejestracja (dokumentacja medyczna pacjentów w formie papierowej oraz stacje robocze z oprogramowaniem); 6) Dokumentacja medyczna pacjentów w formie papierowej oraz stacje robocze z oprogramowaniem; 7) Składnica akt (dokumentacja papierowa).

[24] Zabezpieczenia ujęto w podziale na fizyczne, techniczne, informatyczne, prawno-organizacyjne i zewnętrzne.

Ustalono, że po wejściu w życie przepisów RODO, w maju, wrześniu i listopadzie 2018 r. odbyły się szkolenia, które objęły wszystkie grupy zwodowe pracowników Szpitala. Tematyka szkoleń obejmowała m.in. zasady oraz zagrożenia związane z ochroną danych osobowych wskazane w RODO. W ww. szkoleniach udział wzięło i otrzymało stosowne certyfikaty – 327 pracowników Szpitala, co stanowiło 82,37% wszystkich pracowników Szpitala[25].

Prezes Zarządu wyjaśniła, że (…) *z pozostałych 70 osób (stanowiących 17,63% wszystkich pracowników) 66 osób odbyło szkolenia w swoich macierzystych jednostkach, które są ich podstawowym miejscem pracy lub zostało przeszkolonych przez IOD, a jedynie cztery osoby (co stanowi 1,01% wszystkich osob zatrudnionych) nie zostały przeszkolone w zakresie RODO.*

IOD wyjasniła, iż *osoby te poinformowały ją, iż nie otrzymały w swoich podstawowych miejscach pracy zaświadczeń o odbytym szkoleniu w zakresie RODO. Ponadto każdy pracownik zobowiązany był do zapoznania się z Regulaminem Ochrony Danych Osobowych oraz podpisania klauzul i oświadczeń o poufności. Proces ten trwał od sierpnia 2018 roku. Każdy nowo zatrudniony pracownik jest zapoznawany z Regulaminem o ochronie danych osobowych i zostaje przeszkolony z zakresu RODO niezbędnego na danym stanowisku. Otrzymuje również do podpisu klauzule zgody oraz oświadczenie o poufności*.

(dowód: akta kontroli str. 5, 59-61, 62-72, 243-244, 250-251)

1.7. Szpital nie zobowiązał się formalnie (np. poprzez deklarację stosowania) do przestrzegania regulacji zawartych w Kodeksie postępowania dla sektora ochrony zdrowia[26], 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*[27] i *Wytyczne dotyczące inspektorów ochrony danych*[28].

IOD wyjaśniła, iż (…) *z posiadanych informacji ze strony internetowej Ministerstwa Cyfryzacji wynika, iż kodeks branżowy znajduje się w fazie projektu. Szpital kieruje się wskazówkami zawartymi w „Przewodniku po RODO w służbie zdrowia"*[29]*, który jest opublikowany na stronie internetowej Szpitala*.

(dowód: akta kontroli str. 250-251)

Stwierdzone nieprawidłowości

W działalności kontrolowanej jednostki w przedstawionym wyżej zakresie nie stwierdzono nieprawidłowości.

OCENA CZĄSTKOWA

Szpital wywiązał się z obowiązku opracowania i wdrożenia dokumentacji oraz procedur dotyczących ochrony danych osobowych. Wywiązano się również z obowiązku powołania na stanowisko IOD osoby posiadającej odpowiednie przygotowanie i kwalifikacje zawodowe oraz zawiadomiono o tym fakcie PUODO.

Opracowany terminowo Rejestr czynności przetwarzania zawierał wszystkie wymagane elementy. Przeprowadzono także analizę procesów przetwarzania danych oraz ocenę skutków przetwarzania danych osobowych, a personel Szpitala uczestniczący w procesie przetwarzania danych osobowych został przeszkolony z zagadnień dotyczących bezpieczeństwa danych oraz obowiązywania przepisów RODO.

---

25 Wg stanu na 27 luty 2019 r.

26 Treść kodeksu została opublikowana na stronie internetowej: www.rodowzdrowiu.pl.

27 Przewodnik został 24 września 2018 r. opublikowany na stronie internetowej Ministerstwa Cyfryzacji.

28 Wytyczne zostały 10 maja 2018 r. opublikowane na stronie internetowej Urzędu Ochrony Danych Osobowych.

29 Poradnik opracowany przez Grupę Roboczą ds. Ochrony Danych Osobowych w Ministerstwie Cyfryzacji, opublikowany 24.09.2018 r. na stronie internetowej Ministerstwa https://www.gov.pl/web/cyfryzacja/rodo-w-sluzbie-zdrowia-po-pierwsze-pacjent.

Zapewnienie prawidłowego przetwarzania i ochrony danych osobowych.

Opis stanu faktycznego

2.1. Przeprowadzone oględziny trzech[30] z pięciu funkcjonujących w Szpitalu rejestracji[31] wykazały, że w celu właściwej ochrony danych osobowych pacjentów funkcjonowały poniższe rozwiązania:

- zapewniono, aby w obrębie wzroku pacjenta znajdującego się przy stanowisku rejestracji nie znajdowały się dokumenty zawierające dane osobowe innych pacjentów. Dokumenty pacjentów znajdowały się w zamykanych na klucz regałach lub szafach;
- pracownicy rejestracji nie wypowiadali na głos informacji zawierających dane osobowe;
- rejestracja pacjentów odbywała się na podstawie okazanych dowodów tożsamości, wg kolejności przyjścia do rejestracji (brak urządzeń elektronicznych wspomagających proces rejestracji);
- w przypadku rejestracji ogólnej: dwa stanowiska rejestracyjne usytuowane były obok siebie w odległości zapewniającej dyskrecję oraz uniemożliwiającej wgląd w dokumenty osoby z sąsiedniego okienka. Odległość usytuowanych przed stanowiskami miejsc siedzących dla osób oczekujących na rejestrację uniemożliwiała podsłuchanie informacji podawanych przez osoby rejestrujące się. Przed rejestracją znajdowała się pozioma linia zapewniająca odstęp pomiędzy osobami przy okienku, a kolejnymi osobami w kolejce. Ponadto wywieszona była informacja o treści „Do rejestracji prosimy podchodzić pojedynczo";
- dwie pozostałe rejestracje znajdowały się w osobnych pomieszczeniach w których przebywał tylko jeden pacjent. Pozostali pacjenci oczekiwali na korytarzu;
- ekrany komputerów znajdujących się w rejestracjach ustawiono w sposób uniemożliwiający wgląd w treści na nich wyświetlane osobom rejestrującym się;
- pacjenci po zarejestrowaniu otrzymywali specjalnie przygotowane karteczki, na których podawano datę i godzinę wizyty oraz numer w kolejce (w przypadku rejestracji w Poradni dla Kobiet oraz Zdrowia Psychicznego), natomiast w przypadku rejestracji ogólnej (na wizyty w poradniach chirurgicznej, kardiologicznej) pacjenci byli rejestrowani na konkretne dni bez wskazania godziny.

(akta kontroli str. 9-21)

We wszystkich trzech objętych oględzinami gabinetach poradni specjalistycznych Szpitala[32], 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. Pacjenci wywoływani byli po numerze (w przypadku Poradni Ginekologiczno-Położniczej) lub wchodzili bez wezwania lekarza po wyjściu z gabinetu poprzedniego pacjenta (poradnie Zdrowia Psychicznego oraz Gruźlicy i Chorób Płuc).

(akta kontroli str. 9-21)

Przeprowadzone oględziny dyżurek pielęgniarskich, sal chorych oraz gabinetów lekarskich na trzech oddziałach szpitalnych[33] wykazały m.in., że:

- na oddziałach znajdowało się łącznie: 20 sal chorych (61 łóżek), trzy gabinety lekarskie oraz pięć dyżurek pielęgniarskich;

---

30 Rejestracji: Ogólnej, Poradni Ginekologiczno-Położniczej (dalej: *Poradni dla kobiet*), Poradni zdrowia Psychicznego.

31 Dodatkowo w Szpitalu działają również rejestracja: Poradni Przeciwgruźliczej oraz Pracowni RTG endoskopowej, Laboratorium, USG.

32 Oględzinami objęto trzy poradnie: dla Kobiet, Zdrowia Psychicznego, Gruźlicy i Chorób Płuc.

33 Oględzinami objęto trzy oddziały szpitalne: Rehabilitacyjny, Chorób Wewnętrznych (dalej: *Wewnętrzny*), Anestezjologii i Intensywnej Terapi (dalej: *OIOM*).

- wszyscy zaobserwowani pacjenci oddziałów wewnętrznego oraz rehabilitacji posiadali na nadgarstku opaski informacyjne zawierające: imię, nazwisko, numer księgi głównej, nazwę oddziału. Opaski opisywano w sposób ręczny. Szczegółowy opis zawarto w dalszej części wystąpienia w sekcji „Stwierdzone nieprawidłowości". W przypadku OIOM pacjenci nie posiadali opasek, każde łóżko posiadało nadany numer, który odpowiadał numerowi z karty stanu pacjenta;
- ruch chorych[34] prowadzony był w dyżurkach pielęgniarskich w miejscu niewidocznym dla osób postronnych;
- we wszystkich dyżurkach pielęgniarskich oraz gabinetach lekarskich nie stwierdzono nieprawidłowości w zakresie sposobu użytkowania i zabezpieczenia komputerów (ekrany zwrócone były przodem do personelu w sposób uniemożliwiający odczytanie wyświetlanych danych, nie wystąpiły przypadki pozostawienia niezblokowanego komputera). Dokumentacja zawierające dane medyczne i osobowe pacjentów przechowywana była w zamykanych na klucz szafkach znajdujących się w dyżurkach pielęgniarskich (na oddziałach wewnętrznym i OIOM) oraz w gabinecie lekarskim – w przypadku Oddziału Rehabilitacji.

(akta kontroli str. 9-21)

W Szpitalu przy żadnej z rejestracji ani w ogólnodostępnym dla pacjentów miejscu nie umieszczono klauzul informacyjnych RODO (w formie wydruku). Powyższe szerzej opisano w dalszej części wystąpienia, w sekcji „Stwierdzone nieprawidłowości".

(akta kontroli str. 9-21)

W ramach przeprowadzonych oględzin stwierdzono ponadto, że funkcjonujący w Szpitalu monitoring wizyjny składał się z 22 kamer i obejmował swoim zasięgiem m.in. wejście główne do Szpitala, korytarze, parking, podjazd dla karetek, aptekę, szatnię, serwerownie (nie obejmował żadnego z oddziałów, rejestracji lub poradni). Nagrania z kamer przechowywane były przez okres od 14 do 20 dni. Szpital posiadał Regulamin monitoringu, a pracownicy byli informowani przez swoich przełożonych o jego wprowadzeniu[35].

(akta kontroli str. 26-27, 214-216, 239-240)

2.2. Według stanu na 14 lutego 2019 r. personel działów administracyjnych[36] Szpitala liczył 27 osób. Analiza danych w systemach InfoMedica oraz AMMS[37] wykazała, że uprawnienia jakie zostały nadane wszystkim ww. osobom z tej grupy odpowiadały zakresom zadań i obowiązków realizowanych przez tych pracowników. I tak:

- dziewięć osób z Działu Monitorowania Kosztów i Statystyki oraz dwie z Działu Logistyki[38]) posiadało dostęp do danych z systemu AMMS niezbędny z punktu widzenia realizowanych przez nich zadań, a także pisemne upoważnienia do przetwarzania danych osobowych;
- siedem osób z Działu Finansowo-Kadrowego posiadało dostęp do części administracyjnej systemu InfoMedica (dane księgowe, kadrowe);
- cztery osoby (trzy z Działu Monitorowania Kosztów i Statystyki, jedna osoba z Działu Logistyki) posiadały urpawnienia do systemu AMMS oraz do części administracyjnej systemu InfoMedica;
- siedmiu osobom nie nadano uprawnień do systemów informatycznych AMMS oraz IinfoMedica.

---

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

35 IOD wyjaśniła, że pracownicy byli informowani przez swoich przełożonych, iż w Szpitalu wprowadzany jest minitoring wizyjny.

36 Działy: Finansowo-Kadrowy, Monitorowania Kosztów i Statystyki, Logistyki, Kapelani Szpitalni, BHP.

37 System AMMS zawierający dane medyczne pacjentów funkcjonuje w Szpitalu od 7 marca 2019 r.

38 Jedna z osób (uprawnienia w AMMS dot. OIOM) weryfikuje poprawność procedur medycznych na OIOM, natomiast druga osoba (uprawnienia AMMS dot odziałów: Chirurgicznego, Wewnętrznego, Dziecięcego, OIOM, Izby Przyjęć Noworodków, Rehabilitacyjnego) oddelegowana jest do Działu Logistyki (pół etatu), a jej miejscem zatrudnienia jest Dział Monitorowania Kosztów i Statystyki.

(akta kontroli str. 54-56, 78)

2.3. Analiza przeprowadzona na próbie 30 (ze 156) pielęgniarek i położych zatrudnionych w Szpitalu[39] wykazała, m.in. że:

- wszystkie posiadały dostęp w systemie InfoMedica do danych medycznych pacjentów w komórkach organizacyjnych (oddziały, izba przyjęć), na których świadczyły pracę, a także pisemne upoważnienia do przetwarzania danych osobowych,
- pięć spośród nich (tj. 16,67%), oprócz ww. dostępu do danych medycznych pacjentów w komórkach organizacyjnych, na których świadczyły pracę, posiadało również dostęp do danych pacjentów z innych oddziałów, co szerzej opisano w dalszej części wystąpienia, w sekcji „Stwierdzone nieprawidłowości*"*.

W toku kontroli NIK, zablokowano ww. pielęgniarkom dostęp do danych osobowych pacjentów spoza ich oddziałów.

(akta kontroli str. 54-56)

Ustalono, że żadnej z osób zatrudnionych lub wykonujących na podstawie umów cywilnoprawnych[40] zadania salowej lub sprzątaczki nie nadano uprawnień w systemie do przetwarzania danych osobowych pacjentów, co było działaniem prawidłowym.

(akta kontroli str. 62-72)

2.4. W okresie od 25 maja 2018 r. do 14 lutego 2019 r. Szpital rozwiązał stosunek pracy/umowę cywilnoprawną z 25 osobami. Spośród nich, dziewięć osób w trakcie zatrudnienia miało przyznany dostęp do systemu InfoMedica, a 20 dostęp do systemu Windows. Przeprowadzona analiza terminu odebrania uprawnień ww. osobom wykazała, że:

- w przypadku czterech osób dostęp do systemu InfoMedica został zablokowany, przy czym w jednym przypadku 11 dni od zakończenia pracy, a w trzech przypadkach po 67 dniach od zakończenia pracy[41]; w pozostałych pięciu przypadkach dostęp do systemów został zablokowany w toku kontroli NIK (w dniu 28 marca 2019 r.), tj. po upływie od 62 do 87 dni od daty rozwiązania stosunku pracy/umowy cywilnoprawnej; co szerzej opisano w dalszej części wystąpienia, w sekcji *„Stwierdzone nieprawidłowości"*,
- w przypadku 20 osób, które miały dostęp do systemu Windows, uprawnienia nie zostały im odebrane z uwagi na to, iż nie był im przyznawany indywidualny login oraz hasło.

(akta kontroli str. 22-25)

2.5. W okresie objętym kontrolą Szpital zawarł następujące umowy dotyczące świadczenia usług serwisu oprogramowania oraz pomocy technicznej, tzw. helpdesk:

- z firmą Asseco Poland S.A.[42] na oprogramowanie „InfoMedica/AMMS",
- z firmą Pixel Technology Sp. z o.o.[43] na oprogramowanie RIS/PACS.

W myśl postanowień zawartych ww. umów serwisowych Szpital obowiązany był do zgłaszania błędów poprzez witrynę internetową help-desk'u wykonawcy lub w razie trudności z rejestracją na stronie internetowej, telefonicznie lub mailowo.

Przeprowadzone oględziny sposobu przekazania wszystkich zgłoszeń serwisowych związanych z błędami lub wadliwym działaniem systemów informatycznych z okresu od 25 maja 2018 do 1 marca 2019 r., tj. dwóch zgłoszeń InfoMedica oraz 12 zgłoszeń dotyczących RIS/PACS wykazały, że w każdym ze zgłoszeń nie przekazywano danych pacjenta.

---

39 Na umowę o pracę oraz umowy kontraktowe - stan na 14 lutego 2019 r.

40 Ogółem 20 osób - stan na 27 marca 2019 r.

41 W jednym przypadku 11 dni od zakończenia pracy, w trzech przypadkach 67 dni od zakończenia pracy.

42 Umowa nr PCZSZp/ZP/4.8/10/2018 z dnia 11.06.2018 r. dotyczaca objęcia nadzorem autorskim oprogramowania InfoMedica.

43 Umowa nr PCZSzp/ZP/ZO/4.8/14/2018 z dnia 02.07.2018 r. dotycząca objęcia nadzorem autorskim i opieką serwisową systemu RIS/PACS.

(akta kontroli str. 28)

2.6. Szpital w okresie objętym kontrolą zawarł 18 umów dotyczących powierzenia przetwarzania danych osobowych, w których wystąpił jako podmiot powierzający przetwarzanie danych. Nie wystąpił przypadek podpisania umowy w której Szpital byłby wskazany jako podmiot przetwarzający dane osobowe.

(akta kontroli str. 128-144, 239-240)

Ustalono, że umowy dotyczące powierzenia przetwarzania danych zawierano z podmiotami (wykonawcami) realizującymi na rzecz Szpitala zadania związane m.in. z: wykonywaniem badań histopatologicznych, badań SIMO, badań diagnostycznych oraz konsultacji specjalistycznych, badań tomografem komputerowym, badań laboratoryjnych, świadczeniem usług informatycznych oraz serwisu oprogramowania.

Analiza pięciu umów (porozumień)[44] 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.

Według stanu na 22 lutego 2019 r. usługi na rzecz Szpitala świadczyło na podstawie kontraktów 59 lekarzy (lekarze kontraktowi), przy czym każdy z nich posiadał odrębne imienne pisemne upoważnienie do przetwarzania danych osobowych oraz podpisywał oświadczenie o poufności – z ww. lekarzami nie zawierano umów (porozumień) dotyczących powierzenia przetwarzania danych osobowych.

(akta kontroli str. 59-61, 62-72, 128-144)

2.7. W Polityce Ochrony Danych Osobowych Szpitala zawarto Instrukcję postępowania z incydentami naruszenia ochrony danych osobowych, w której określono m.in. typowe incydenty naruszeń ochrony danych, zasady prowadzenia postępowania wyjaśniającego, procedury postępowania w przypadku naruszenia danych osobowych.

Ponadto analiza postanowień Polityki wykazała, że IOD zobowiązany był do prowadzenia rejestru naruszeń ochrony danych osobowych oraz sporządzania raportu z naruszenia ochrony danych osobowych, a także do zgłaszania organowi nadzoru każdego przypadku naruszenia ochrony danych osobowych skutkującego ryzykiem naruszenia praw lub wolności osób fizycznych bez zbędnej zwłoki – nie później niż w terminie 72 godzin po stwierdzeniu naruszenia (art. 33 ust. 1 RODO).

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

(akta kontroli str. 177-204, 250-251)

2.8. W okresie objętym kontrolą, Szpital nie posiadał wewnętrznych procedur dotyczących udostępniania danych osobowych. Szpital udostępniał dokumentację medyczną na podstawie przepisu art. 26 ust. 1 i 3 oraz art. 27 u.o.p.p., tj. dokumentację medyczną udostępniano pacjentowi lub jego przedstawicielowi ustawowemu, bądź osobie upoważnionej przez pacjenta oraz podmiotom określonym w ust. 3 ww. przepisu.

W okresie od 25 maja 2018 r. do 8 marca 2019 r. wpłynęło do Szpitala 818 wniosków o udostępnienie dokumentacji medycznej.

---

[44] Porozumienia zawarte z: Diagnostyka Sp. z o.o. z siedzibą w Krakowie w dniu 25.05.2018 r.; SP ZOZ w Międzychodzie z dnia 25.05.2018 r.; Wielospecjalistycznym Szpitalem Wojewódzkim w Gorzowie Wlkp w dniu 25.05.2018 r.; Diagnostyka Consillio Sp. z o.o. z siedzibą w Łodzi w dniu 22.05.2018 r.; Asseco Poland S.A. z siedzibą w Rzeszowie.

Informacje o udostępnieniu dokumentacji medycznej każdorazowo ujmowano w wykazie prowadzonym w formie elektronicznej, o którym mowa w art. 27 ust. 4 u.o.p.p.

(akta kontroli str. 237, 245)

Przeprowadzona analiza prawidłowości udostępnienia dokumentacji w odniesieniu do 30 przypadków, w których dokumentacja medyczna została udostępniona firmom ubezpieczeniowym oraz 30 przypadków udostępnienia dokumentacji innej osobie niż pacjent, którego ta dokumentacja dotyczyła wykazała, że:

- w każdym przypadku udostępniono kopię dokumentacji medycznej,
- we wszystkich przypadkach udostępniania dokumentacji osobie innej niż pacjent, dokumentacja medyczna została udostępniona osobom/instytucjom posiadającym pisemne upoważnienie pacjenta do dostępu do tej dokumentacji, na podstawie wniosków o jej udostępnienie.

(akta kontroli str. 222-225)

2.9. Regulacje dotyczące ochrony danych przed ich utratą w wyniku awarii, błędów lub nieuprawnionej modyfikacji zostały opisane w Regulaminie Ochrony Danych Osobowych (określono w nim m.in. zasady użytkowania sprzętu IT, Politykę haseł, Zasady wynoszenia nośników na zewnątrz, korzystania z sieci Internet, z poczty elektronicznej oraz ochronę antywirusową). Ponadto zgodnie z zapisami Polityki w Szpitalu opracowano Plan ciągłości zawierający m.in. plany awaryjne dotyczące: braku zasilania, systemu informatycznego po awarii, utraty dostępu do internetu, kopii zapasowych. W Szpitalu zarządzanie infrastrukturą informatyczną odbywało się z wykorzystaniem usługi ACTIVE Directory.

(akta kontroli str. 177-204, 209-213)

Przeprowadzone oględziny dwóch serwerowni Szpitala (tj. serwerowni głównej[45]/ serwerowni zastępczej[46]) wykazały, m.in. że:

- wyposażone były w drzwi antywłamaniowe zamykane kluczem oraz kratą – w przypadku serwerowni głównej, natomiast w przypadku serwerowni zastępczej sztabą magnetyczną otwieraną przy pomocy chipa dekodującego, dzięku któremu możliwa była kontrola dostępu,
- serwerownia główna posiadała okno które było zabezpieczone kratą oraz folią odblaskową,
- serwerownie wyposażone były w klimatyzację, wolnostojące gaśnice CO2, a serwerownia zastępcza w system monitoringu wizyjnego,
- serwery i urządzenia znajdowały się w specjalnie do tego przeznaczonych szafach oraz regałach, urządzenia posiadały układy podtrzymywania napięcia (tzw. UPS) na wypadek zaniku zasilania,
- w serwerowniach panował porządek, nie był w nich przechowywany niepotrzebny sprzęt,
- serwerownie nie posiadały systemu alarmowego, przeciwwłamaniowego ani przeciwpożarowego.

(akta kontroli str. 29-53)

Z wyjaśnień IOD wynika, iż planowana jest instalacja w serwerowniach czujek monitorujących poziom temperatury, dym w pomieszczeniu oraz sygnalizujących wejście do pomieszczenia. Obecnie Szpital jest na etapie wyceny powyższych prac (system p.poż. ma być zainstalowany również w innych częściach Szpitala).

(akta kontroli str. 250-251)

---

[45] Serwerownia główna umiejscowiona na 1 piętrze budynku, znajdują się w niej: serwery główne i pomocnicze, bazy danych medycznych, urządzenie zabezpieczające sieć.

[46] Serwerownia umiejscowiona na parterze budynku Szpitala, w której przechowywane są Urządzenia aktywne switch, urządzenie zapisujące dane z monitoringu wizyjnego, monitor z podglądem przekazu z kamer monitoringu wizyjnego.

W toku kontroli NIK, drzwi serwerowni głównej dodatkowo wyposażono w sztabę magnetyczną otwieraną chipem, dzięki czemu monitorowany był dostęp do serwerowni.

(akta kontroli str. 252-253)

W wyniku oględzin 30 losowo wybranych komputerów służących do przetwarzania danych osobowych[47] ustalono, że:

- na 20 komputerach użytkowanych wspólnie przez personel medyczny[48], użytkownicy logowali się do systemu operacyjnego z użyciem wspólnego loginu i hasła, co szerzej opisano w dalszej części wystąpienia, w sekcji „Stwierdzone nieprawidłowości",
- długość hasła odpowiadała wymaganiom określonym w dokumentacji wewnętrznej jednostki,
- wszystkie komputery posiadały zainstalowane programy antywirusowe z aktualną bazą sygnatur wirusów,
- na komputerach zainstalowany był Windows 7 (20 sztuk), Windows 10 (na 9 komputerach) oraz na jednym komputerze Windows XP. Dla systemu Windows XP brak wsparcia technicznego ze strony producenta oprogramowania wpływa na bezpieczeństwo infrastruktury informatycznej jednostki,
- we wszystkich komputerach porty USB były aktywne,
- na wszystkich 30 komputerach pracownicy byli w stanie zainstalować oprogramowanie, co szerzej opisano w dalszej części wystąpienia, w sekcji „Stwierdzone nieprawidłowości".

Prezes Zarządu wyjasniła iż *kopie zapasowe z danymi z serwera głównego znajdującego się w głównej serwerowni wykonywne są codziennie i zapisywane na serwerze znajdującym się w drugiej serwerowni. W Szpitalu jest 12 urządzeń przenośnych na których nie stosuje się ochrony kryptograficznej nośników pamięci. Urządzenia te są przypisane do miejsc stacjonowania i nie opuszczają budynków placówki. W Szpitalu wykorzystuje się pseudonimizację danych osobowych polegającą na ich przetwarzaniu*.

(akta kontroli str. 29-53, 236)

Stwierdzone nieprawidłowości

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

1. W Szpitalu przy żadnej z rejestracji, ani w ogólnodostępnym dla pacjentów miejscu nie umieszczono klauzul informacyjnych RODO. W przypadku zbierania danych bezpośrednio od pacjentów Szpital jest zobowiązany do przekazania im informacji o których mowa w art. 13 RODO.

Prezes Zarządu wyjaśniła, iż *klauzule informacyjne RODO zostały umieszczone na terenie Szpitala w miejscach ogólnodostępnych, zgodnie ze wzorem stanowiącym załącznik nr 9 do Polityki Ochrony Danych Osobowych Szpitala Powiatowego w Drezdenku dopiero w trakcie kontroli, z uwagi na wcześniejsze niedopatrzenie*.

W toku kontroli NIK, w budynku Szpitala (tablice informacyjne, główna rejestracja, Izba Przyjęć) zamieszczono klauzule informacyjne RODO.

(akta kontroli str. 9-21, 57, 243-244)

2. Pięć z 30 (tj. 16,67%) analizowanych pielęgniarek i położych zatrudnionych w Szpitalu[49], oprócz dostępu do danych medycznych pacjentów w komórkach organizacyjnych, na których świadczyły pracę, posiadało również dostęp do danych pacjentów z innych oddziałów.

---

[47] Po 10 komputerów użytkowanych przez lekarzy, pielęgniarki lub położne oraz przez pracowników administracyjnych.

[48] 20 komputerów znajdujących się na oddziałach Szpitala użytkowanych przez lekarzy i pielęgniarki.

[49] Na umowę o pracę oraz umowy kontraktowe - stan na 14 lutego 2019 r.

Stosownie do przepisu § 20 ust. 2 pkt 4 rozporządzenia Rady Ministrów z dnia 12 kwietnia 2012 r. w sprawie Krajowych Ram Interoperacyjności, minimalnych wymagań dla rejestrów publicznych i wymiany informacji w postaci elektronicznej oraz minimalnych wymagań dla systemów teleinformatycznych[50] (dalej: *KRI*), zarządzanie bezpieczeństwem informacji realizowane jest w szczególności przez zapewnienie przez kierownictwo podmiotu publicznego warunków umożliwiających realizację i egzekwowanie działań zapewniających, że osoby zaangażowane w proces przetwarzania informacji posiadają stosowne uprawnienia i uczestniczą w tym procesie w stopniu adekwatnym do realizowanych przez nie zadań oraz obowiązków mających na celu zapewnienie bezpieczeństwa informacji. Ponadto w przepisie art. 5 ust. 1 lit. c RODO wskazano zasadę adekwatności i minimalizacji danych, tj. wymóg ustalenia, kto i w jakim zakresie, powinien być uprawniony do przetwarzania danych.

W toku kontroli NIK zablokowano dostęp ww. pracowników do danych pacjentów z oddziałów, w których nie wykonywały pracy.

Prezes Zarządu wyjaśniła, iż *w ww. przypadkch nadano szersze uprawnienia w wyniku błędu.*

(akta kontroli str. 54-56, 243-244)

3. Ośmiu z 9 (88,9%) byłym pracownikom Szpitala dostęp do konta użytkownika w systemie AMMS zablokowano dopiero po upływie od 62 do 87 dni od zakończenia pracy (z tego w pięciu przypadkach w toku kontroli NIK).

Stanowiło to naruszenie § 20 ust. 2 pkt 5 KRI, zgodnie z którym należy podejmować działania polegające na bezzwłocznej zmianie uprawnień, w przypadku zmiany zadań osób zaangażowanych w proces przetwarzania informacji.

Prezes Zarządu wyjaśniła, że nieodebranie dostępu do systemów informatycznych dla byłych pracowników było niedopatrzeniem.

(akta kontroli str. 22-25, 243-244)

4. Na wszystkich 30 komputerach obętych badaniem pracownicy posiadali uprawnienia administratora systemu operacyjnego komputera.

Zgodnie z przepisem § 20 ust. 2 pkt 4 KRI, zarządzanie bezpieczeństwem informacji realizowane jest w szczególności przez podejmowania działań zapewniających, że osoby zaangażowane w proces przetwarzania informacji posiadają stosowne uprawnienia i uczestniczą w tym procesie w stopniu adekwatnym do realizowanych przez nie zadań oraz obowiązków, mających na celu zapewnienie bezpieczeństwa informacji.

Prezes Zarządu wyjaśniła, że *pobieranie i próba instalacji potencjalnie „złośliwego" oprogramowania nie jest możliwe, a możliwe jest tylko pobieranie oprogramowania i aktualizacji potrzebnych do funkcjonowania systemów. Szpitalna sieć informatyczna zabezpieczona jest m.in. poprzez urządzenie PaloAlto, które monitoruje i weryfikuje ruch sieciowy, oraz poprzez aktywne urządzenia sieciowe firmy Brocade, poprzez konfigurację których zapewnione jest wyeliminowanie możliwości podłączenia się zewnętrznych komputerów do sieci szpitalnej*.

NIK zauważa, iż pracownicy korzystający z ww. komputerów nie wykonywali zadań związanych z właściwym utrzymaniem sieci komputerowej Szpitala. Ponadto aktywne porty USB umożliwiały im instalowanie dowolnego oprogramowania.

(akta kontroli str. 29-53, 243-244)

5. Na 20 (z 30 zbadanych) komputerach użytkowanych wspólnie przez personel medyczny, użytkownicy logowali się do systemu operacyjnego z użyciem wspólnego loginu i hasła.

Działanie to było niezgodne 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 użytkowniokom, nie jest

[50] Dz. U. z 2017 r. poz. 2247.

możliwa prawidłowa rozliczalność sytemów. 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. Jednocześnie, zgodnie z motywem 39 preambuły 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.

Prezes Zarządu wyjaśniła, iż *logowanie się personelu na poszczególnych punktach szpitala za pomocą tego samego loginu i hasła do systemu Windows, ma na celu usprawnienie pracy personelu i mniejsze obciążanie pracy systemu operacyjnego. Takie logowanie się nie jest jednoznaczne z dostępem do bazy danych pacjentów. Aby mieć możliwość chociażby wglądu w dane pacjenta należy zalogować się do Szpitalnego Systemu Informatycznego AMMS, do którego każdy z pracowników ma osobne login i hasło.*

NIK zauważa, że z uwagi na fakt logowania się pracowników do systemu Windows z wykorzystaniem wspólnego loginu i hasła niemożliwe było odebranie uprawnień do logowania w systemie operacyjnym byłym pracownikom.

(akta kontroli str. 29-53, 243-244)

6. Pacjenci oddziałów wewnętrznego oraz rehabilitacji posiadali na nadgarstku znaki informacyjne (opaski) zawierające: imię, nazwisko, numer księgi głównej, nazwę oddziału. Opaski opisywano w sposób ręczny i możliwe było odczytanie ww. danych przez osoby postronne (nieuprawnione).

Zgodnie z treścią art. 36 ust 3 i 5 ustawy z dnia 15 kwietnia 2011 r. o działalności leczniczej[51] (dalej: *u.o.d.l.*) pacjentów szpitala zaopatruje się w znaki identyfikacyjne zapisane w sposób uniemożliwiający identyfikację pacjenta przez osoby nieuprawnione

IOD wyjaśniła, iż *na opaski nanoszono dane pacjenta w sposób tradycyjny, poprzez zapisywanie ich ręcznie. Z uwagi na wielkość nanoszonych liter odczytanie danych przez osoby postronne było utrudnione i możliwe tylko z bardzo bliskiej odległości. Obecnie po podpisaniu umowy z firmą Asseco Poland S.A. jest wdrażany system pozwalający na drukowanie opasek identyfikacyjnych zgodnie z wytycznymi wynikającymi z przepisów prawa.*

(akta kontroli str. 9-21, 243-244)

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.

Personelowi Szpitala zapewniono odpowiedni dostęp do danych medycznych. Wystąpiło jednak pięć (na 30 badanych) przypadków nadania pielęgniarkom zbyt szerokich uprawnień, a także odbieranie ze znacznym opóźnieniem możliwości dostępu do tych systemów byłym pracownikom Szpitala.

Dane identyfikujące pacjentów były nanoszone na opaski w sposób umożliwiający identyfikację pacjenta przez osoby nieuprawnione.

Zastosowano fizyczne zabezpieczenia serwerowni Szpitala, w których przechowywano dane osobowe przetwarzane w formie elektronicznej, natomiast sposób użytkowania i zabezpieczenia wykorzystywanych w Szpitalu komputerów stacjonarnych (badaniami objęto 30 komputerów) nie gwarantował pełnej ochrony przetwarzanych na tych komputerach danych osobowych pacjentów, wskutek możliwości instalowania oprogramowania przez użytkowników komputerów, praktyki logowania się do systemu operacyjnego z użyciem wspólnego loginu i hasła i nieodbierania uprawnień byłym pracownikom.

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

Szpital zawierał umowy powierzenia przetwarzania danych w sytuacjach tego wymagających, a w pięciu analizowanych umowach zamieszczono postanowienia wymagane art. 28 RODO. Prawidłowo udostępniano również uprawnionym podmiotom dokumentację medyczną pacjentów.

IV. Wnioski

Wnioski

W związku ze stwierdzonymi nieprawidłowościami, a także działaniami podjętymi w toku kontroli w celu ich wyeliminowania, Najwyższa Izba Kontroli, na podstawie art. 53 ust. 1 pkt 5 ustawy o NIK, przedstawia następujące wnioski:

1. Nadawanie pracownikom uprawnień w systemach informatycznych Szpitala w stopniu adekwatnym do realizowanych przez nich zadań.
2. Bezzwłoczne odbieranie uprawnień w systemach informatycznych byłym pracownikom Szpitala.
3. Cofnięcie nadanych pracownikom uprawnień administratora, tak, aby nie mieli możliwości samodzielnego instalowania na komputerach oprogramowania.
4. Nadanie wszystkim użytkownikom komputerów indywidualnych danych do autoryzacji w systemach operacyjnych oraz wprowadzenie rozwiązań uniemożliwiających pracę kilku osób na jednym koncie użytkownika.
5. Opisywanie opasek identyfikujących pacjentów w sposób uniemożliwiający ich identyfikację przez osoby nieuprawnione.

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 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, 17 kwietnia 2019 r.

Kontroler
Tomasz Przybysz
Inspektor kontroli państwowej

.....
podpis

Najwyższa Izba Kontroli
Delegatura w Zielonej Górze
p.o. Dyrektora
Włodzimierz Stobrawa

.....
podpis