NAJWYŻSZA IZBA KONTROLI

Delegatura w Poznaniu

LPO.410.002.03.2019

Pan
Prof. dr hab. Julian Malicki
Dyrektor Wielkopolskiego Centrum
Onkologii im. Marii Skłodowskiej-Curie
w Poznaniu
ul. Garbary 15, 61-866 Poznań

WYSTĄPIENIE POKONTROLNE

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

NAJWYŻSZA IZBA KONTROLI
Delegatura w Poznaniu
ul. Dożynkowa 9H, 61-662 Poznań
T +48 61 655 62 00, F +48 61 655 62 01
lpo@nik.gov.pl

I. Dane identyfikacyjne

Jednostka kontrolowana	Wielkopolskie Centrum Onkologii im. Marii Skłodowskiej-Curie, ul. Garbary 15, 61-866 Poznań (dalej: WCO albo Szpital)
Kierownik jednostki kontrolowanej	Prof. dr hab. Julian Malicki, Dyrektor Szpitala, od 1995 r. (dalej: Dyrektor)
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. do 1 marca 2019 r.[1].
Podstawa prawna podjęcia kontroli	Art. 2 ust. 2 ustawy z dnia 23 grudnia 1994 r. o Najwyższej Izbie Kontroli[2]
Jednostka przeprowadzająca kontrolę	Najwyższa Izba Kontroli Delegatura w Poznaniu
Kontroler	Daniel Braciszewski, inspektor kontroli państwowej, upoważnienie do kontroli nr LPO/5/2019 z 9 stycznia 2019 r.

(akta kontroli str. 1)

[1] Badania kontrolne objęły także działania sprzed tego okresu, które miały związek z zagadnieniami będącymi przedmiotem kontroli.
[2] Dz. U. z 2019 r. poz. 489, dalej: ustawa o NIK.

II. Ocena ogólna[3] kontrolowanej działalności

OCENA OGÓLNA

Najwyższa Izba Kontroli ocenia pozytywnie wdrożenie i stosowanie w Szpitalu regulacji, które zapewniały prawidłową ochronę i przetwarzanie danych osobowych.

Uzasadnienie oceny ogólnej

Regulacje wewnętrzne WCO związane z ochroną i przetwarzaniem danych osobowych były sporządzone profesjonalnie, kompleksowo i na wysokim poziomie szczegółowości. Rzetelnie przeprowadzono analizę procesów przetwarzania danych osobowych oraz ocenę skutków ich przetwarzania, jak również prawidłowo prowadzono dotyczące tych kwestii rejestry.

Personelowi Szpitala zapewniono odpowiedni, zgodny z zakresem wykonywanych przez poszczególne osoby czynności, dostęp do danych pacjentów oraz właściwie udostępniano ich dokumentację medyczną. Pracowników WCO zapoznano z przepisami rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r.[4] oraz zagadnieniami dotyczącymi bezpieczeństwa danych. Zastosowane środki organizacyjne i techniczne skutecznie przeciwdziałały ujawnieniu danych pacjentów osobom nieuprawnionym oraz ich utracie w wyniku awarii, błędów lub nieuprawnionej modyfikacji. Środki te zapewniały stopień bezpieczeństwa adekwatny do ryzyk związanych m.in. ze skalą i rodzajem przetwarzanych danych osobowych.

Nieprawidłowością było łączenie stanowisk Inspektora Ochrony Danych i Kierownika Działu Informatyki przez jedną osobę, która była jednocześnie zaangażowana w proces określania sposobów i celów przetwarzania danych osobowych. Pomimo istnienia potencjalnego konfliktu interesów, nie stwierdzono jednak by wpłynęło to negatywnie na bezpieczeństwo przetwarzania oraz ochronę danych osobowych w Szpitalu.

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

OBSZAR

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

Opis stanu faktycznego

1.1 Zarządzeniem wewnętrznym Dyrektora z 31 sierpnia 2018 r.[6] w Szpitalu wyznaczono Inspektora Ochrony Danych (dalej: IOD), który podlegał bezpośrednio kierownikowi kontrolowanej jednostki. Wcześniej (do 24 maja 2018 r.) ta sama osoba pełniła obowiązki Administratora Bezpieczeństwa Informacji (dalej: ABI), a następnie zajmowała stanowisko IOD do dnia wprowadzenia ww. zarządzenia. IOD zajmował jednocześnie stanowisko Kierownika Działu Informatyki, a od 9 kwietnia 2018 r. był także przewodniczącym Zespołu ds. zapewnienia bezpieczeństwa i ochrony danych osobowych w WCO. Celem tego Zespołu był organizacyjny i merytoryczny nadzór nad przygotowaniem Szpitala do wdrożenia i stosowania przepisów RODO. Ponadto na mocy ww. zarządzenia wyznaczono Administratora Bezpieczeństwa Systemów Informatycznych (dalej: ABSI), którego zadaniem była ścisła współpraca z IOD w zakresie ochrony danych osobowych

[3] Najwyższa Izba Kontroli formułuje ocenę ogólną jako ocenę pozytywną, ocenę negatywną albo ocenę w formie opisowej.
[4] 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., weszło w życie 24 maja 2016 r., znajduje zastosowanie od 25 maja 2018 r., dalej: RODO.
[5] Oceny cząstkowe to oceny działalności w poszczególnych obszarach badań kontrolnych. Ocena cząstkowa może być sformułowana jako ocena pozytywna, ocena negatywna albo ocena w formie opisowej.
[6] Nr 41 (znak DI6396/2018) w sprawie wyznaczenia Inspektora Ochrony Danych w Wielkopolskim Centrum Onkologii.

przetwarzanych w WCO[7]. W przywołanym dokumencie określono i rozgraniczono zadania Administratora Danych Osobowych (dalej: ADO), IOD oraz ABSI. Powyższe stanowiska ujęto w strukturze organizacyjnej Szpitala określonej w regulaminie organizacyjnym WCO, którego ostatnią wersję wprowadzono 31 grudnia 2018 r.[8]

Szpital wywiązał się z obowiązku zawiadomienia Prezesa Urzędu Ochrony Danych Osobowych (dalej: Prezes UODO) o wyznaczeniu IOD[9] w terminie o którym mowa w art. 158 ust. 1 i 2 ustawy z dnia 10 maja 2018 r. o ochronie danych osobowych[10]. Nastąpiło to w dniu wyznaczenia IOD, tj. 31 sierpnia 2018 r. poprzez przekazanie Prezesowi UODO formularza elektronicznego. Przekazane zawiadomienie zawierało wszystkie elementy określone w art. 10 ust. 1 i 3 ww. ustawy. Dane IOD oraz sposób i formę kontaktu udostępniono na stronie internetowej Szpitala, zgodnie z wymogami art. 37 ust. 7 RODO i art. 11 ustawy o ochronie danych osobowych.

(akta kontroli str. 6-49, 659-676, 696-746)

W zakresie czynności IOD podpisanym 4 stycznia 2019 r.[11] zawarto m.in. postanowienia o odpowiedzialności pracownika za sumienne i terminowe wykonywanie powierzonych zadań oraz prawidłową współpracę ze współpracownikami oraz instytucjami współpracującymi w zakresie powierzonych zadań[12], a także o wykonywaniu bezpośrednich poleceń przełożonego, czyli Dyrektora WCO i jednocześnie Reprezentanta ADO. Z formalnoprawnego punktu widzenia treść ww. elementów zakresu czynności IOD mogła być postrzegana jako ograniczenie wykonywania przez niego obowiązków w sposób całkowicie niezależny, wymagany przez art. 38 ust. 3 i motyw 97 RODO[13].

Zgodnie z wyjaśnieniami Dyrektora, podległość służbowa, jak i wynikające z tego wykonywanie poleceń należy rozumieć w kategoriach porządkowych i organizacji pracy, a nie w zakresie ingerencji w przedmiot i decyzje merytoryczne wynikające z wykonywanych zadań. Zdaniem Dyrektora, zapisy w zakresie czynności wynikały wyłącznie z zastosowania standardowych zapisów formularza zakresu czynności pracownika, stanowiącego dokument Polityki Zintegrowanego Systemu Zarządzania WCO, stosowanego przy opracowywaniu wszystkich zakresów czynności pracowników WCO.

W trakcie kontroli NIK powyższe elementy zostały usunięte z zakresu czynności IOD[14].

(akta kontroli str. 88-89, 94-95, 214-220, 232-234, 661-665, 677-682)

W WCO IOD zajmowała również stanowisko Kierownika Działu Informatyki i należały do niej obowiązki związane z zaangażowaniem w proces określania sposobów i celów przetwarzania danych osobowych[15].

(akta kontroli str. 659-665, 677-695, 778-786)

Zgodnie z wymogami art. 37 ust. 5 RODO, IOD posiadała należyte przygotowanie i kwalifikacje zawodowe do pełnienia swojej funkcji. Pełniła wcześniej funkcje ABSI oraz ABI w kontrolowanym Szpitalu a także ukończyła studia podyplomowe w zakresie ochrony informacji niejawnych i danych osobowych. IOD była członkiem

[7] Funkcję ABSI pełnił Zastępca Kierownika Działu Informatyki.
[8] Zarządzeniem wewnętrznym Dyrektora nr 68 (znak D.012/1-2-9865/2018)
[9] Pełnił funkcję Kierownika Działu Informatyki.
[10] Dz. U. poz. 1000, ze zm., dalej: ustawa o ochronie danych osobowych.
[11] Zakres czynności pracownika na stanowisku IOD, zał. I-2-01-01/1, edycja 6 z dnia 4 stycznia 2019 r.
[12] Punkt nr 15.
[13] Art. 38 ust. 3 - Administrator oraz podmiot przetwarzający zapewniają, by inspektor ochrony danych nie otrzymywał instrukcji dotyczących wykonywania tych zadań. Nie jest on odwoływany ani karany przez administratora ani podmiot przetwarzający za wypełnianie swoich zadań […]. Motyw 97 – […] inspektorzy ochrony danych - bez względu na to, czy są pracownikami administratora - powinni być w stanie wykonywać swoje obowiązki i zadania w sposób niezależny.
[14] Zakres czynności pracownika na stanowisku IOD, zał. I-2-01-01/1, edycja 6 z dnia 6 lutego 2019 r.
[15] Szerzej tę kwestię opisano w sekcji „Stwierdzone nieprawidłowości".

Grupy Roboczej ds. Ochrony Danych Osobowych w Zespole ds. Systemu Ochrony Zdrowia przy Ministerstwie Cyfryzacji, a także członkiem rzeczywistym Stowarzyszenia Inspektorów Ochrony Danych SABI[16]. W okresie od 2006 do 2018 r. uczestniczyła w wielu szkoleniach z zakresu ochrony danych osobowych, cyberbezpieczeństwa i elektronicznej dokumentacji medycznej.

WCO nie zostało uznane za operatora usługi kluczowej, o którym mowa w art. 5 ust. 1 w zw. z art. 2 pkt 16 ustawy z dnia 5 lipca 2018 r. o krajowym systemie cyberbezpieczeństwa[17].

(akta kontroli str. 666-670, 673-676, 696-746)

1.2 Przed rozpoczęciem stosowania RODO w Szpitalu funkcjonowały dokumenty związane z ochroną danych osobowych w postaci polityki bezpieczeństwa, na którą składały się m.in. polityki: Bezpieczeństwa Danych Osobowych (dalej: PBDO), Bezpieczeństwa Informacji[18] (dalej: PBI), Ochrony Prywatności (dalej: POP). Dokumenty te zostały zaktualizowane[19]. Zgodnie z motywem 78 i art. 24 RODO, w WCO wdrożono odpowiednie środki techniczne i organizacyjne, które zapewniły zgodność przetwarzania danych osobowych z RODO.

PBDO[20] odnosiła się do zabezpieczenia danych osobowych przetwarzanych tradycyjnie oraz w systemach informatycznych. Wprowadzone w związku z RODO regulacje zostały zatwierdzone przez ADO. Dotyczyły one m.in. procedur przetwarzania danych osobowych i oceny ich skutków, wypełnienia obowiązku informacyjnego, zapewnienia poufności, rozliczalności i spójności danych, czynności pracowników w zakresie przetwarzania danych osobowych, prowadzenia rejestrów czynności i kategorii czynności przetwarzania tych danych[21].

Ponadto wewnętrzne procedury, obowiązujące w WCO przed rozpoczęciem stosowania RODO, zostały dostosowane do wymogów tego rozporządzenia. Dotyczyły one m.in.: przetwarzania danych osobowych i zaznajamiania osób upoważnionych do ich przetwarzania z przepisami o ochronie danych osobowych, zarządzania upoważnieniami i poleceniami do przetwarzania tych danych, pracy użytkowników w systemie informatycznym, zgłaszania naruszeń ochrony danych osobowych, zapewnienia bezpieczeństwa sieci komputerowej, zasad udostępniania ww. danych[22].

---

[16] Statut tego stowarzyszenia zakładał członkostwo rzeczywiste lub wspierające (http://sabi.org.pl/czlonkostwo.php).

[17] Dz. U. poz. 1560.

[18] Zgodnie z § 2 pkt 15 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 (Dz. U. z 2017 r. poz. 2247) - dalej: rozporządzenie KRI - jest to zestaw efektywnych, udokumentowanych zasad i procedur bezpieczeństwa wraz z ich planem wdrożenia i egzekwowania.

[19] Aktualizacje odbywały się systematycznie od kwietnia do września 2018 r. i polegały na zmianie podstawy prawnej umieszczonej w obowiązujących przed wejściem w życie RODO procedurach.

[20] Dokument opracowany na podstawie RODO, pełniący rolę konstytutywną w stosunku do wydanych w tym zakresie wewnętrznych zarządzeń oraz instrukcji, zawiera opracowanie szczegółowych wytycznych w zakresie obowiązków nałożonych na ADO, m. in. obowiązek ochrony interesów osób, których dane dotyczą, obowiązek informacyjny.

[21] Np.: „Analiza poufności, rozliczalności i spójności w aspekcie potencjalnych zagrożeń i ryzyka w WCO", „Procedura oceny skutków operacji przetwarzania danych osobowych w WCO", „Procedura zasady przetwarzania danych osobowych w WCO", „Procedura klauzula obowiązku informacyjnego w WCO", „Procedura zgody na przetwarzanie danych osobowych w WCO", „Wytyczne w zakresie ochrony danych osobowych – zakres czynności pracownika/umowa cywilnoprawna w WCO", „Procedura realizacji praw osób, których dane dotyczą w WCO", „Procedura prowadzenia rejestrów czynności i kategorii czynności przetwarzania danych osobowych w WCO".

[22] Np.: „Program zaznajomienia osób upoważnionych do przetwarzania danych z przepisami o ochronie danych osobowych oraz w zakresie regulaminu środowiska informatycznego służącego do przetwarzania danych osobowych w WCO", „Przetwarzanie danych osobowych w imieniu Administratora", „Procedura zarządzania upoważnieniami i poleceniami do przetwarzania danych osobowych w WCO", „Procedura rozpoczęcia, zawieszenia i zakończenia pracy użytkownika w systemie informatycznym WCO", „Procedura zgłaszania naruszeń ochrony danych osobowych w WCO", „Procedura zapewnienia bezpieczeństwa techniczno-organizacyjnego Szpitalnej Sieci Komputerowej w WCO", „Procedura dostępu do obszaru przetwarzania danych osobowych w WCO – strefa bezpieczeństwa podstawowego", „Procedura udostępniania danych osobowych przetwarzanych w WCO", „Procedura dostępu do obszaru przetwarzania danych osobowych w WCO – strefa bezpieczeństwa podwyższonego i wysokiego" , „Procedura sprawdzania zgodności przetwarzania danych osobowych (audyt) z przepisami o ochronie danych osobowych w WCO oraz opracowania sprawozdania w tym zakresie".

W WCO dostosowano także do wymogów RODO wzory dokumentów będące integralną częścią ww. procedur, jak m.in.: ewidencja osób upoważnionych do przetwarzania danych osobowych, upoważnienie i polecenie do przetwarzania tych danych, zobowiązanie do zachowania w tajemnicy danych osobowych i sposoby ich zabezpieczenia, klauzula obowiązku informacyjnego dla pracownika i osobno dla pacjenta, obszar przetwarzania danych osobowych, wniosek kierownika komórki organizacyjnej o przyznanie dostępu do domeny i osobny o dostęp do systemu informatycznego do obsługi WCO. Wejście w życie RODO było czynnikiem determinującym stworzenie wzorów nowych dokumentów, m.in. takich jak: klauzula zgody na przetwarzanie danych osobowych w procesie rekrutacji, klauzula obowiązku informacyjnego dla osoby ubiegającej się o pracę, a także dla użytkownika systemów informatycznych, rejestr naruszeń danych osobowych, formularz zgłoszenia incydentu bezpieczeństwa i naruszenia ochrony danych osobowych organowi nadzorczemu.

(akta kontroli str. 245-265, 577-658, 863-887, 1052-1308, 1543-1735)

W ramach funkcjonującego w WCO Zintegrowanego Systemu Zarządzania[23], opracowano procedurę „Nadzór nad udokumentowanymi informacjami", której celem było zapewnienie prawidłowego zarządzania dokumentami w zakresie opracowania, wdrażania, dystrybucji (także w tzw. bazie dokumentacji ZSZ w Intranecie) i aktualizacji dokumentacji oraz efektywnego zarządzania informacją w postaci gromadzenia danych, sposobów ich przetwarzania, zarządzania, udostępniania, przechowywania i mechanizmów zapewniających bezpieczeństwo informacji. Integralną część ZSZ stanowiła procedura „Komunikacja", która regulowała przebieg procesu komunikacji wewnętrznej i zewnętrznej, w tym w sprawach dotyczących ochrony danych osobowych. W ramach ZSZ opracowano również procedurę „Udostępnianie dokumentacji medycznej" określającą zasady udostępniania dokumentacji medycznej pacjentom oraz organy mające do niej dostęp, wraz ze sposobem udostępniania tej dokumentacji.

(akta kontroli str. 508-511, 810-837)

W WCO, zgodnie z § 20 ust. 1 rozporządzenia KRI, została opracowana Polityka Bezpieczeństwa Informacji w ramach której, w związku z wejściem w życie RODO wprowadzono nową Politykę Ochrony Prywatności. Określała ona zasady przetwarzania danych[24] wszystkich osób odwiedzających strony internetowe WCO, w tym osób rejestrujących się na wydarzenia naukowe, na świadczenia zdrowotne, osób kontaktujących się z WCO lub wypełniających ankiety. W dokumencie tym opisano też zasady automatycznego zbierania danych podczas wizyty użytkownika na stronach WCO, a także omówiono strategię ochrony danych osobowych, opcje wyboru sposobu zbierania danych i ich wykorzystywania. Ponadto Dyrektor w „Deklaracji Wsparcia Kierownictwa Dla Polityki Bezpieczeństwa Informacji WCO" zadeklarował pełną odpowiedzialność i wsparcie za realizację przyjętej PBI, a w szczególności dla PBDO oraz zapewnienie odpowiednich środków i zasobów do jej wdrożenia. PBI tworzyły m.in. procedury funkcjonujące w kontrolowanej jednostce, które zostały zmodyfikowane w związku z RODO. Dotyczyły one m.in. ciągłości działania środowiska informatycznego, wykonywania kopii bezpieczeństwa

[23] System zarządzania funkcjonujący w WCO obejmujący System Zarządzania Jakością wg ISO 9001:2015, System Zarządzania Środowiskowego wg ISO 14001:2015, System Zarządzania Bezpieczeństwem i Higieną Pracy wg PN-N-18001:2014, dalej: ZSZ .

[24] Gromadzenia, modyfikacji, usuwania, udostępniania.

danych, zabezpieczania komputerów, szyfrowania danych i uzyskiwania do nich dostępu, uwierzytelniania użytkowników systemów informatycznych[25].

(akta kontroli str. 245-265, 1331-1539)

W WCO od 2015 r. stosowano także procedurę dotyczącą sprawdzania[26] zgodności przetwarzania danych osobowych z przepisami o ochronie danych osobowych, dokonywanego dla ADO[27]. W ramach ww. procedury przeprowadzono audyt, zgodnie z planem sprawdzeń i zaplanowano kolejny audyt na 2019 rok[28]. IOD tym samym spełniła obowiązek zawarty w art. 24 ust. 1 i art. 39 ust. 1 pkt b RODO.

Ponadto pracownicy i kierownicy wszystkich komórek organizacyjnych Szpitala zostali zobowiązani przez Dyrektora do współpracy z Zespołem ds. zapewnienia bezpieczeństwa i ochrony danych osobowych w WCO i wdrożenia zasad przetwarzania danych osobowych. Kierownik Działu Informatyki i ABSI zostali także zobowiązani do realizacji obowiązku zabezpieczenia danych osobowych i medycznych podlegających ochronie prawnej w Szpitalnej Sieci Komputerowej WCO (dalej: SSK WCO) przed zagrożeniami z sieci publicznej.

(akta kontroli str. 659-665, 778-786, 1282-1330)

W dwóch zarządzeniach wewnętrznych Dyrektora[29], które w trakcie trwania kontroli NIK były modyfikowane, przywołano m.in. ustawę z dnia 29 sierpnia 1997 r. o ochronie danych osobowych[30], a nie przywołano ustawy o tej samej nazwie, która weszła w życie 25 maja 2018 r. Zagadnienia dotyczące danych osobowych zawarte w ww. zarządzeniach znalazły się jednak w aktualnych i dostosowanych do RODO procedurach tworzących PBDO oraz ZSZ, które to zostały zatwierdzone przez ADO i były stosowane przez personel Szpitala.

(akta kontroli str. 761-777)

Postanowienia polityki ochrony danych osobowych obejmowały zarówno ochronę danych osobowych pracowników WCO, jak i pacjentów oraz określały sposoby zapewnienia bezpieczeństwa tych danych, przetwarzanych w formie papierowej oraz w systemach elektronicznych. Akty prawne przywołane w opracowanej dokumentacji, z wyjątkiem dwóch ww. zarządzeń wewnętrznych, zostały zaktualizowane. Bez zbędnej zwłoki i w odpowiedniej formie opracowano kompletną dokumentację wymaganą regulacjami wewnętrznymi, każdorazowo zatwierdzaną przez Dyrektora. Wewnętrzne akty prawne związane z RODO zostały udostępnione personelowi WCO zgodnie z jego kompetencjami. Na każdym dokumencie umieszczono informację o jego wykonawcach wraz z podaniem stanowisk lub grupy osób, dla których dokumentacja ta była przeznaczona do stosowania. W WCO

[25] Np.: „Procedura zachowania ciągłości działania środowiska informatycznego WCO" „Procedura wykonywania kopii bezpieczeństwa i archiwizacji w WCO", „Procedura zarządzania dostępem użytkownika do systemów informatycznych w WCO", „Procedura zarządzania identyfikatorem użytkownika w systemach informatycznych w WCO", „Procedura zarządzania hasłem użytkownika w systemie informatycznym w WCO", „Procedura ewidencji i analizy dzienników zdarzeń systemowych zasobów informatycznych w WCO", „Procedura nadzoru nad dokumentacją i zapisami Polityki Bezpieczeństwa Informacji w WCO", „Procedura Szyfrowania Danych w WCO", „Procedura zarządzania nośnikami zawierającymi dane (w tym osobowe) w WCO", „Procedura przydziału haseł administracyjnych w WCO", „Wytyczne do zawarcia umowy zdalnego dostępu do środowiska informatycznego WCO", „Instrukcja szyfrowania nośników zewnętrznych w systemie MS Windows". W związku z rozpoczęciem stosowania RODO opracowano także „Instrukcję zabezpieczenia plików hasłem w WCO". W WCO stosowane były także procedury w oparciu o dokumenty związane z Polityką Zarządzania Oprogramowaniem i Polityką Certyfikacji.

[26] Sprawdzenia planowe albo doraźne.

[27] W ramach procedury wprowadzono szereg wzorów dokumentów, jak np. wzór sprawozdania ze sprawdzenia zgodności przetwarzania danych osobowych, plan audytów, zawiadomienie ADO o rozpoczęciu audytu, zawiadomienie kierownika komórki organizacyjnej objętej audytem o zakresie planowanych czynności w audycie.

[28] Plan sprawdzeń zgodności przetwarzania danych osobowych z przepisami o ochronie danych osobowych – 2018 r. zatwierdzony przez ADO 10 stycznia 2018 r. Natomiast 7 maja 2018 r. ADO zatwierdził korektę ww. planu wyznaczając okres sprawdzenia od 26 maja do 31 grudnia 2019 r. w celu weryfikacji czy w rok po wprowadzeniu nowych regulacji prawnych osoby przetwarzające dane wdrożyły je w życie.

[29] Nr 52 z 23 października 2017 r. (znak D/6518/2017), nr 53 z 8 listopada 2016 r. (znak WCO/D/6467/2016).

[30] Dz. U z 2016 r. poz. 922, ze zm. uchylona z dniem 6 lutego 2019 r.

funkcjonowała też baza dokumentacji ZSZ w sieci Intranet, do której dostęp posiadali wszyscy pracownicy.

(akta kontroli str. 245-265, 747-760, 1001-1804)

1.3 Od 25 maja 2018 r. IOD prowadziła rejestr czynności przetwarzania danych i rejestr kategorii czynności przetwarzania danych, o których mowa w art. 30 ust. 1 i 2 RODO. Rejestry te prowadzone były jako jeden dokument w formie elektronicznej w Systemie Wspomagania Pracy Działu Informatyki (dalej: SWPDI) z możliwością ich wygenerowania w formie papierowej jako skonsolidowanego dokumentu. Według stanu na 17 stycznia 2019 r. rejestr ten liczył 154 pozycje i zawierał wszystkie dane wymagane ww. przepisami.

(akta kontroli str. 888-938, 1169-1175)

1.4 Stosownie do wymogów określonych w art. 24 ust. 1 i art. 32 ust. 1 i 2 RODO, w WCO przeprowadzono analizę procesów przetwarzania danych osobowych pacjentów Szpitala oraz określono ryzyka dla każdego z nich[…][31]

(akta kontroli str. 596-597, 1061-1076)

1.5 W WCO, podczas kontroli NIK została wykonana ocena skutków dla ochronnych danych, o której mowa w art. 35 RODO, chociaż była ona fakultatywna. Grupa Robocza Art. 29 ds. Ochrony Danych[32] (dalej: Grupa Robocza Art. 29) zalecała dokonanie DPIA[33] dla operacji przetwarzania trwających przed 25 maja 2018 r. oraz w przypadkach, gdy nie było jasne, czy jest ona wymagana[34]. Uznano bowiem, że jest ona „przydatnym narzędziem, które może pomóc administratorom danych w zapewnieniu zgodności z prawem ochrony danych", pomimo że Prezes UODO w komunikacie wydanym na podstawie art. 35 ust. 4 RODO[35] wśród rodzajów operacji przetwarzania danych osobowych wymagających oceny skutków przetwarzania dla ich ochrony, nie zawarł danych medycznych przetwarzanych w szpitalach. W okresie objętym kontrolą nie doszło do przetwarzania nowych kategorii danych (np. w związku z wprowadzeniem dodatkowych usług medycznych), co powinno determinować wykonanie DPIA. Zgodnie z zarządzeniem wewnętrznym Dyrektora[36], jednym z zadań Zespołu ds. zapewnienia bezpieczeństwa i ochrony danych osobowych w WCO była m.in. ocena skutków planowanych operacji przetwarzania danych osobowych, jeżeli dany rodzaj przetwarzania mógł powodować wysokie ryzyko naruszenia praw lub wolności osób fizycznych. Ponadto w WCO opracowano procedurę dotyczącą przygotowania DPIA[37], w której zawarto zapis nakładający na ADO obowiązek konsultowania się z IOD w zakresie przygotowania ww. dokumentu. Konsultacje ADO z organem nadzorczym były przewidziane, np. w celu uzyskania pisemnych zaleceń, jeśli DPIA wskazałaby, że przetwarzanie danych osobowych powodowałoby wysokie ryzyko

[31] Na podstawie art. 5 ust. 2 ustawy z dnia 6 września 2001 r. o dostępie do informacji publicznej (Dz. U. z 2018 r. poz. 1330 ze zm.) i art. 11 ust. 4 ustawy z dnia 16 kwietnia 1993 r. o zwalczaniu nieuczciwej konkurencji (Dz. U. z 2019 r. poz. 1010) NIK wyłączyła jawność informacji w zakresie stwierdzonych ryzyk i procedur zabezpieczających dane osobowe. Wyłączenia tego dokonano w interesie przedsiębiorcy.

[32] Tj. Grupa Robocza ds. Ochrony Osób Fizycznych w Zakresie Przetwarzania Danych Osobowych Grupa Robocza została powołana na podstawie art. 29 dyrektywy 95/46/WE Parlamentu Europejskiego i Rady z dnia 24 października 1995 r. w sprawie ochrony osób fizycznych w zakresie przetwarzania danych osobowych i swobodnego przepływu tych danych (Dz. Urz. UE L 281 z 24 października 1995 r., str. 31). Jest ona niezależnym organem doradczym w zakresie ochrony danych i prywatności. Zadania grupy określone są w art. 30 dyrektywy 95/46/WE oraz art. 15 dyrektywy 2002/58/WE Parlamentu Europejskiego i Rady z dnia 12 lipca 2002 r. dotyczącej przetwarzania danych osobowych i ochrony prywatności w sektorze łączności elektronicznej (Dz. Urz. UE L 201 z 12 lipca 2002 r., str. 37).

[33] DPIA (ang. Data Protection Impact Assessment) - ocena skutków dla ochrony danych osobowych.

[34] Wytyczne dotyczące oceny skutków dla ochrony danych oraz pomagające ustalić, czy przetwarzanie „może powodować wysokie ryzyko" do celów rozporządzenia 2016/679, WP 248/01 (przyjęte 4 kwietnia 2017 r., zmienione i przyjęte 4 października 2017 r.).

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

[36] Nr 16 z 9 kwietnia 2018 r. (WCO.D/2601/2018).

[37] Załącznik nr PBDO.P012 do PBDO z 28 maja 2018 r.

w przypadku niezastosowania środków w celu jego zminimalizowania. W ww. procedurze zaznaczono, że wymóg dokonania oceny skutków dotyczy operacji przetwarzania, spełniających kryteria wskazane w art. 35 RODO i rozpoczętych po tym jak RODO zacznie mieć zastosowanie w dniu 25 maja 2018 r.

Ocena skutków dla ochrony danych osobowych w WCO została zatwierdzona przez ADO w lutym 2019 r. w postaci trzech dokumentów[38], w których wysokie ryzyko oszacowano w związku z: systematycznym monitorowaniem wizyjnym pacjentów i pracowników, systemem monitorowania pracowników oraz wykorzystywania przez nich narzędzi (poczty elektronicznej, Internetu, systemów branżowych), systematycznym monitorowaniem danych dotyczących zdrowia pacjentów. Analizy zawierały wszystkie elementy określone w art. 35 ust. 7 RODO, a wyodrębnione procesy wynikały ze specyfiki działania i struktury WCO.

Dyrektor wyjaśnił, że wykonał ocenę skutków dla ochrony danych jako wynik szczególnej staranności ADO, mimo iż zgodnie z art. 35 ust. 1 i 10 oraz motywem 90 i 93 RODO, DPIA powinna być przeprowadzona przed rozpoczęciem przetwarzania, a w WCO nie podjęto nowych operacji przetwarzania po 25 maja 2018 r. Dodał, że w toku konsultacji nie było sytuacji, aby nie zgadzał się z zaleceniami IOD, które zostały udzielone na podstawie art. 39 ust. 1 RODO.

(akta kontroli str. 88-91, 220-223, 652-653, 659-660, 1001-1051, 1139-1144)

1.6 Jednym z zadań IOD, zgodnie z art. 39 ust. 1 lit. b RODO, było prowadzenie szkoleń personelu uczestniczącego w operacjach przetwarzania danych. Kwestia szkoleń dotyczących bezpieczeństwa danych została także uregulowana w § 20 ust. 2 pkt 6 rozporządzenia KRI[39]. W myśl ww. przepisów, a także wewnętrznych procedur[40], w WCO każda osoba mająca przetwarzać dane osobowe była zobowiązana do zaznajomienia się z przepisami dotyczącymi ochrony danych osobowych oraz politykami bezpieczeństwa ADO, a także z regulaminem środowiska informatycznego WCO. Spełnienie tego wymogu było konieczne do uzyskania upoważnienia do przetwarzania danych osobowych. Zgodnie z obowiązującą w Szpitalu praktyką oraz ww. procedurami, przez szkolenie rozumiano także zapoznanie z wyciągiem ze szkolenia oraz z informacjami zamieszczonymi w serwisie Intranet, w zakładce Polityka Bezpieczeństwa Informacji[41]. Ponadto ADO zobowiązał IOD do prowadzenia szkoleń przypominających. Tematyka szkolenia w WCO obejmowała m.in.: przesłanki legalizujące przetwarzanie danych osobowych, zabezpieczenia organizacyjne, zabezpieczenia techniczne środowiska informatycznego, kontrolę i monitoring pracy pracowników, prawa osób, których dane są przetwarzane, powierzanie przetwarzania danych osobowych i ich udostępnianie, naruszenia bezpieczeństwa systemu, odpowiedzialność osób przetwarzających dane. W wydawanych upoważnieniach do przetwarzania danych osobowych umieszczana była informacja o zaznajomieniu pracownika z przepisami, zgodnie z programem szkolenia oraz o zrozumieniu treści przepisów o ochronie danych osobowych. Szkolenia w formie

[38] Załącznik PBI.PBDO.E006/01 do PBDO z 12 lutego 2019 r., Załącznik PBI.PBDO.E006/02 do PBDO z 8 lutego 2019 r., Załącznik PBI.PBDO.E006/03 do PBDO z 18 lutego 2019 r.

[39] Szkolenia osób zaangażowanych w proces przetwarzania informacji powinny uwzględniać następujące zagadnienia: zagrożenia bezpieczeństwa informacji, skutki naruszenia zasad bezpieczeństwa informacji, w tym odpowiedzialność prawną, stosowanie środków zapewniających bezpieczeństwo informacji (np. szyfrowanie dysków, szyfrowanie kluczy USB, dostęp do systemów IT po podaniu hasła).

[40] Program zaznajomienia osób upoważnionych do przetwarzania danych z przepisami o ochronie danych osobowych oraz w zakresie regulaminu środowiska informatycznego służącego do przetwarzania danych osobowych w WCO, załącznik nr PBDO.P007 do PBDO, wersja 03.01, zatwierdzenie przez ADO 3 stycznia 2019. Program w wersji 01.00 obowiązywał w WCO od 1 grudnia 2008 r., Zarządzenie wewnętrzne nr 41 Dyrektora WCO z dn. 31.08.2018 r., znak D/6396/2018. Procedura „Szkolenia" P-2-01-B, edycja 7 z 18 lutego 2019 r.

[41] Dnia 14 lutego 2019 r. dokonano zmiany w dokumencie Zintegrowanego Systemu Zarządzania - Procedura „Szkolenia" P-2-01-B poprzez dodanie pkt I dotyczącego szkoleń z zakresu ochrony danych osobowych i bezpieczeństwa informacji, które prowadzone są za pośrednictwem serwisu Intranet poprzez umieszczenie komunikatów, informacji, przypomnień.

osobistych spotkań z IOD odbywały się w WCO tylko w przypadku zatrudnienia nowego pracownika, który był zaangażowany w proces przetwarzania danych osobowych. Dotyczyło to pracowników niezależnie od zajmowanych przez nich stanowisk, tj. m.in. osób pracujących w rejestracji, udzielających świadczeń zdrowotnych, farmaceutów, analityków medycznych, techników, osób z działów administracyjnych. Ponadto szkoleniami obejmowano osoby przetwarzające dane osobowe w przypadku zmiany formy zatrudnienia, ich danych osobowych, miejsca wykonywania zadań lub świadczenia usług[42]. Powyższe odnotowywane było w prowadzonej ewidencji osób upoważnionych do przetwarzania danych osobowych w WCO. W Szpitalu, w związku z rozpoczęciem obowiązywania RODO, nie przeprowadzono szkoleń w formie spotkań wszystkich pracowników z IOD. Stosowne informacje znajdowały się natomiast w serwisie Intranet i były aktualizowane. Po rozpoczęciu stosowania RODO, pomiędzy 25 maja 2018 r. a 15 stycznia 2019 r., IOD indywidualnie przeszkoliła 133 osoby (w tym pracowników Szpitala i inne osoby np. uczestników wydarzeń naukowych i kontrahentów) oraz dodatkowo 64 nowych pracowników (upoważnionych do przetwarzania danych osobowych)[43]. Trzy nowo zatrudnione osoby nie zostały przeszkolone w formie spotkania z IOD, gdyż uprzednio odbywały w WCO praktyki lub wolontariat. Tego rodzaju osoby były traktowane w Szpitalu jako pracownicy i podlegały zasadom PBI, zgodnie z którymi były zobowiązane do stałego zapoznawania się z treściami szkoleniowymi umieszczanymi w serwisie Intranet. Szkolenia w formie indywidualnego spotkania z IOD lub samokształcenia objęły wszystkich pracowników WCO.

(akta kontroli str. 96-97, 235-244, 560, 564, 661-665, 847-850, 854-887)

IOD wyjaśniła, że z uwagi na specyfikę podmiotu, gdzie zadaniem statutowym jest obowiązek diagnozowania i leczenia chorych, stosuje się różne metody szkoleniowe, które mają zapewnić przetwarzanie danych osobowych zgodnie z obowiązującymi przepisami prawa, nie powodując zakłócenia procesu udzielania świadczeń zdrowotnych. Wobec powyższego metody te, to nie tylko osobiste spotkania z IOD, ale również: okresowe zamieszczanie aktualności w serwisie Intranet, przygotowanie materiałów szkoleniowych i ich przekazywanie do komórek organizacyjnych, przekazywanie informacji na odprawach i zebraniach, zamieszczanie treści w zakładce PBI w sieci Intranet. IOD zaznaczyła, że w WCO szkolenia z zakresu ochrony danych osobowych prowadzi się od wielu lat, praktycznie od początku obowiązywania przepisów krajowych, a od 2005 r. rozszerzone są o wymogi regulowane wprowadzeniem ustawy z dnia 17 lutego 2005 r. o informatyzacji działalności podmiotów realizujących zadania publiczne[44] i rozporządzeń wykonawczych do tej ustawy. Ponadto IOD wyjaśniła, że przepisy nie narzucają formy przeprowadzenia szkolenia, dlatego wybrano w WCO formę najbardziej adekwatną, która jest praktykowana również do innych szkoleń, jak w szczególności w zakresie Zintegrowanego Systemu Zarządzania Jakością i Akredytacji Centrum Monitorowania Jakością. Podkreśliła, że wprowadzenie RODO nie było dla WCO zagadnieniem całkowicie nowym, a jedynie zmieniającym wdrożone od lat zasad i reguły postępowania w tym zakresie. IOD zwróciła uwagę, że program szkolenia stale ulega zmianom w celu dostosowania jego treści do zmieniających się przepisów. Wskazała, że szkolenia, których treści są udostępnione w wewnętrznym serwisie Intranet, uznawanym za podstawowe narzędzie przekazywania informacji, są dostępne dla osób przetwarzającym dane

[42] M.in. zmiany: komórki organizacyjnej, uprawnień, zbioru przetwarzania danych osobowych np. z pracowniczych na dane pacjenta.
[43] Na podstawie umowy o pracę wg stanu na 15 stycznia 2019 r. zatrudnione były 1 052 osoby.
[44] Dz. U. z 2017 r. poz. 570, ze zm.

osobowe w każdym momencie, co gwarantuje, iż pracownicy będą sięgać do zamieszczonych treści, przyswajać je i kontaktować się z IOD w sytuacji ich niezrozumienia. Powodowało to jej zdaniem, że szkolenie nie było traktowane tylko jako obowiązek służbowy, ale realnie podnosiło świadomość pracowników w zakresie ochrony danych osobowych.

(akta kontroli str. 235-241)

1.7 W WCO nie został sporządzony oddzielny dla Szpitala kodeks dobrych praktyk lub medyczny kodeks branżowy. W szpitalu stosowano rozwiązania przewidziane w „Przewodniku po RODO w Służbie Zdrowia" Ministerstwa Cyfryzacji[45], które współtworzyła IOD poprzez udział w pracach Grupy Roboczej ds. Ochrony Danych Osobowych w Sekcji Ochrony Zdrowia. Pracownicy WCO byli zaznajamiani z treścią tego opracowania w wewnętrznym serwisie Intranet oraz zostali zobowiązani do jego stosowania w praktyce.

Zastępca Dyrektora ds. Klinicznych wyjaśnił, że WCO w pełni popiera inicjatywę stworzenia kodeksu postępowania dla sektora ochrony zdrowia[46], który jest mechanizmem pozwalającym na zdefiniowanie przez instytucje zajmujące się ochroną zdrowia list dobrych praktyk, referencji, poradników, zaleceń w zakresie „dobrych praktyk" mówiących o tym, jak w najlepszy sposób w danym środowisku wykonywać zadania związane z ochroną danych osobowych. Ponadto podkreślił, że w momencie zatwierdzenia kodeksu przez organ nadzorczy, WCO rozpocznie jego implementację mając świadomość, że może on wpłynąć na podwyższenie jakości i skuteczności działań podejmowanych w zakresie ochrony danych.

(akta kontroli str. 100-102, 673-676)

Stwierdzone nieprawidłowości

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

IOD zajmowała również stanowisko Kierownika Działu Informatyki WCO i należały do niej obowiązki związane z zaangażowaniem w proces określania sposobów i celów przetwarzania danych osobowych, co mogło powodować konflikt interesów, o którym mowa w art. 38 ust. 6 RODO. Zgodnie z tym przepisem IOD może wykonywać inne zadania i obowiązki, ale administrator lub podmiot przetwarzający mają obowiązek zapewnić, by takie zadania i obowiązki nie powodowały konfliktu interesów. W wytycznych Grupy Roboczej Art. 29 zawartych w dokumencie „Wytyczne dotyczące inspektorów ochrony danych ('DPO')[47], wskazuje się, że za powodujące konflikt interesów uważa się stanowiska kierownicze, w tym stanowisko Kierownika IT (tu: Kierownika Działu Informatyki), a ponadto IOD nie może zajmować w organizacji innego stanowiska pociągającego za sobą określania sposobów i celów przetwarzania danych (pkt 3.5, str. 17 oraz pkt 10 załącznika nr 5 do wytycznych, str. 25).

Z zakresu czynności pracownika zatrudnionego na stanowisku Kierownika Działu Informatyki[48] wynikało natomiast, że do czynności tych należało m.in. określanie sposobów i celów przetwarzania danych osobowych poprzez:

1) wykonywanie obowiązków w zakresie: administrowania siecią komputerową, serwerami i macierzami dyskowymi, przedstawiania opinii w zakresie procesu

[45] Opracowany przez Grupę Roboczą ds. Ochrony Danych Osobowych, utworzoną w Ministerstwie Cyfryzacji https://www.gov.pl/web/cyfryzacja/rodo-w-sluzbie-zdrowia-po-pierwsze-pacjent - opublikowany 24 września 2018 r. na stronie Ministerstwa Cyfryzacji – dostęp z 15 stycznia 2019 r.

[46] Dokument przekazany do akceptacji do Prezesa UODO w listopadzie 2018 r., który wydaje opinię o zgodności projektu z RODO i go zatwierdza jeśli uzna, że stanowi on odpowiednie zabezpieczenie. Po zarejestrowaniu zostanie opublikowany w BIP (art. 40 ust. 5 RODO), przy czym do 1 marca 2019 r. Kodeks Branżowy w Ochronie Zdrowia nie został zatwierdzony przez Prezesa UODO: (http://www.rodowzdrowiu.pl/wp-content/uploads/2018/11/2018-11-13-KODEKS-BRAN%C5%BBOWY-Wniosek-o-zatwierdzenie-kodeksu-postepowania.pdf)

[47] https://www.giodo.gov.pl/pl/1520344/10390, przyjęte 13 grudnia 2016 r., ostatnio zmienione i przyjęte 5 kwietnia 2017 r.

[48] Zakres czynności pracownika z 4 stycznia 2019 r., Zał. I-2-01-01/1, edycja 6. – pkt 12 i 13.

informatyzacji WCO, współtworzenie dokumentacji PBI, w tym m.in. zarządzanie dostępem do sieci, zasobów, systemów, usług informatycznych, a także administrowanie uprawnieniami oraz opracowanie procedur polityki bezpieczeństwa w zakresie systemów i usług informatycznych.

2) współtworzenie dokumentacji PBDO w WCO, która obejmowała m.in. program zaznajomienia osób upoważnionych do przetwarzania danych z przepisami o ochronie danych osobowych oraz w zakresie regulaminu środowiska informatycznego służącego do przetwarzania danych osobowych, procedurę oceny skutków operacji przetwarzania danych osobowych, procedurę dotyczącą zasad przetwarzania danych osobowych w WCO.

3) zapewnienie bezpieczeństwa informacji, w tym danych osobowych przetwarzanych w WCO oraz opracowanie i wdrażanie nowych rozwiązań i technologii informatycznych przy zapewnieniu bezpieczeństwa przetwarzanych danych.

Ponadto Dział Informatyki WCO, na podstawie zarządzenia wewnętrznego w sprawie SSK WCO[49], odpowiadał za informatyczne dostosowanie wymagań związanych z wdrożeniem RODO, czyli realizację ustawowego obowiązku zabezpieczenia danych osobowych i medycznych oraz innych danych, które podlegają ochronie prawnej. Dyrektor WCO powierzył wykonanie zarządzenia ABSI Kierownikowi Działu Informatyki, którego to dział zarządzał SSK w WCO. […][50].

NIK wskazuje, że nawet w przypadku gdy zabezpieczenia były nadzorowane przez ABSI, to za zarządzanie SSK WCO i wdrożenie w systemie informatycznym wymagań wynikających z RODO, odpowiadał Kierownik Działu Informatyki wraz z ABSI, który był jednocześnie jego zastępcą[51].

(akta kontroli str. 659-695, 778-786, 872-873, 1773-1804)

Dyrektor wyjaśnił, że pełnienie przez IOD jednocześnie funkcji Kierownika Działu Informatyki wynikało z przesłanek pragmatycznych. Według niego, IOD jest pracownikiem posiadającym szerokie kompetencje i aby jego zalecenia były wykonywane przez kadrę wysokiej klasy specjalistów w dziedzinach medycznych musi mieć odpowiednią pozycję i autorytet, a taką osobą jest Kierownik Działu Informatyki i informatyk z wykształcenia. W opinii Dyrektora należy stosować interpretację celową przepisów, a więc dokonać takiego ułożenia rozdziału obowiązków, aby postanowienia RODO, które nakładają na personel wiele uciążliwych obowiązków i niejednokrotnie są kwestionowane przez pacjentów jako nieżyciowe, były wykonywane, a ewentualnie zagrożenia konfliktu interesów były rzadkie, jedynie potencjalne i nie miały możliwości zaistnienia. Wskazał on, że zajmowanie tych dwóch stanowisk przez IOD jest merytorycznie zasadne, a decyzję podjęto wiedząc, że jakość wykonywanej przez pracownika pracy przełoży się na zmniejszenie ryzyka poniesienia odpowiedzialności przez ADO w przypadku powstania naruszeń przepisów dotyczących ochrony danych osobowych. Powyższe powoduje, iż wykonywanie funkcji IOD nie jest iluzoryczne, ale daje mu faktyczną możliwość pracy. Ponadto Dyrektor WCO zaznaczył, że Kierownik Działu

[49] Zarządzenie wewnętrzne Dyrektora WCO nr 17 z 11 kwietnia 2018 r., znak: WCO.D/2700/2018, wydane m.in. w celu realizacji ustawowego obowiązku zabezpieczenia danych osobowych i medycznych oraz innych danych, które podlegają ochronie prawnej.

[50] Na podstawie art. 5 ust. 2 ustawy z dnia 6 września 2001 r. o dostępie do informacji publicznej (Dz. U. z 2018 r. poz. 1330 ze zm.) i art. 11 ust. 4 ustawy z dnia 16 kwietnia 1993 r. o zwalczaniu nieuczciwej konkurencji (Dz. U. z 2019 r. poz. 1010) NIK wyłączyła jawność informacji w zakresie metod zabezpieczenia sieci komputerowej. Wyłączenia tego dokonano w interesie przedsiębiorcy.

[51] Zakres czynności pracownika z 4 stycznia 2019 r., Zał. I-2-01-01/1, edycja 6. Zastępca Kierownika Działu Informatyki bierze udział w określania sposobów i celów przetwarzania danych osobowych i odpowiada za wykonywanie obowiązków przez Kierownikiem.

Informatyki nie jest odpowiedzialny za określanie środków i celów przetwarzania danych w WCO, gdyż jest to zadanie reprezentanta ADO, tj. jego.

(akta kontroli str. 214-220)

Podczas kontroli zakres obowiązków IOD został zmieniony w taki sposób, aby w pełni zapewnić niezależność w sprawowaniu jego funkcji[52]. Ponadto zmianie uległ też zakres obowiązków Kierownika Działu Informatyki[53], z którego usunięto ww. zapisy wprost odwołujące się do brania udziału w określaniu celów i sposobów przetwarzania danych osobowych przez osobę zatrudnioną na tym stanowisku.

(akta kontroli str. 214-220, 677-695)

OCENA CZĄSTKOWA

NIK ocenia pozytywnie opracowanie i wdrożenie przez Szpital dokumentacji oraz procedur dotyczących ochrony danych osobowych. Przyjęty system zarządzania bezpieczeństwem informacji co do zasady odpowiadał wymogom § 20 ust. 1 rozporządzenia KRI. Regulacje wewnętrzne WCO związane z ochroną i przetwarzaniem danych osobowych były sporządzone profesjonalnie, kompleksowo i na wysokim poziomie szczegółowości. Rzetelnie przeprowadzono analizę procesów przetwarzania danych osobowych oraz ocenę skutków ich przetwarzania, jak również prawidłowo prowadzono rejestr czynności i kategorii czynności przetwarzania tych danych. Z przepisami RODO oraz zagadnieniami dotyczącymi bezpieczeństwa danych zapoznano cały personel Szpitala. Nie stwierdzono by fakt łączenia stanowisk IOD i Kierownika Działu Informatyki przez jedną osobę oraz jej zaangażowanie w proces określania sposobów i celów przetwarzania danych osobowych – co zmieniono w toku kontroli – wpłynęły negatywnie na realizację zadań w badanym obszarze.

OBSZAR

2. Zapewnienie prawidłowego przetwarzania i ochrony danych osobowych.

Opis stanu faktycznego

2.1 W celu właściwej ochrony danych osobowych w WCO[54] stosowano reguły wynikające z „Przewodnika po RODO w Służbie Zdrowia" opracowanego przez Ministerstwo Cyfryzacji. Podczas przeprowadzonych oględzin oddziałów i sposobu rejestrowania pacjentów do poradni szpitalnych oraz procesu wywoływania i przyjmowania tych osób przez lekarzy w gabinetach[55] ustalono, że w WCO stosowano następujące rozwiązania:

- Na łóżkach szpitalnych nie umieszczano kart pacjentów z ich nazwiskami i informacjami o stanie zdrowia. Informacje o wynikach badań i leczeniu były ewidencjonowane w systemie informatycznym i dostępne do wglądu po wczytaniu kodu kreskowego z opaski umieszczonej na nadgarstku pacjenta.

- Każdego z pacjentów wyposażono w opaskę zawierającą znak identyfikacyjny w postaci kodu kresowego, na podstawie którego możliwe było ustalenie danych osobowych i medycznych.

- […][56] Ponadto, na oddziałach szpitalnych zainstalowany był monitoring wizyjny, rejestrujący ruch osobowy na korytarzach prowadzących do sal chorych oraz

[52] Patrz punkt 1.1 niniejszego wystąpienia pokontrolnego.
[53] Zakres czynności pracownika z 6 lutego 2019 r.
[54] Oddziały szpitalne, rejestracje do poradni, gabinety lekarskie.
[55] Oddział Radioterapii Onkologicznej III, Oddział Chirurgii Onkologicznej Chorób Przewodu Pokarmowego oraz Oddział Radioterapii i Onkologii Ginekologicznej, Rejestracja Główna, Rejestracja Tomografii Komputerowej, Rejestracja na Oddziale Chemioterapii, gabinety lekarskie na terenie Poradni Chirurgii Onkologicznej, Poradni Ginekologii Onkologicznej i Poradni Chemioterapii.
[56] Na podstawie art. 5 ust. 2 ustawy z dnia 6 września 2001 r. o dostępie do informacji publicznej (Dz. U. z 2018 r. poz. 1330 ze zm.) i art. 11 ust. 4 ustawy z dnia 16 kwietnia 1993 r. o zwalczaniu nieuczciwej konkurencji (Dz. U. z 2019 r. poz. 1010) NIK wyłączyła jawność informacji w zakresie stosowanych metod zabezpieczenia fizycznego pomieszczeń. Wyłączenia tego dokonano w interesie przedsiębiorcy.

pomieszczeń, w których mogą przebywać tylko pracownicy szpitala lub personel medyczny razem z pacjentami, a także w salach intensywnego nadzoru i w sekretariatach.

- Na oddziałach nie była przechowywana dokumentacja medyczna, gdyż znajdowała się ona wyłącznie w systemie informatycznym, w którym prowadzony był także ruch chorych[57]. W niektórych dyżurkach stosowano karty zleceń badań lekarskich, oddzielne dla każdego pacjenta, w formie papierowej ułożone według numerów sal chorych i przechowywane w zamykanych szafach. Pacjenci nie posiadali dostępu do tych pomieszczeń, gdyż wejście do nich było ograniczone […][58].

Jedynymi dokumentami przechowywanymi w sekretariatach dyżurek lekarskich były zgody pacjentów na leczenie i wykonanie zabiegów, które po opuszczeniu przez pacjenta oddziału były przekazywane do archiwum. Dostęp do nich, oprócz lekarzy, miały także sekretarki medyczne, posiadające upoważnienie do przetwarzania danych osobowych. Według informacji Pełnomocnika Dyrektora Ds. Klinicznych obecnie obowiązujące przepisy nie pozwalają na zeskanowanie podpisów pacjentów, a szpital chętnie przechowywałby ww. zgody w systemie informatycznym, gdyby było to dopuszczone prawnie[59].

- […][60]

- Rejestracja pacjentów odbywała się w rejestracji ogólnej i osobnej rejestracji do poradni chorób piersi, w której kolejność ustalana była za pośrednictwem stanowiska samoobsługowego. Rejestracja do poradni chorób piersi znajdowała się w wydzielonym dla niej oddzielnym pomieszczeniu.

- Rejestracja prowadzona była w pięciu okienkach, usytuowanych w taki sposób aby uniemożliwić usłyszenie danych osobowych lub wgląd w dokumenty osoby obsługiwanej na sąsiednim stanowisku. Dodatkowo przestrzeń między okienkami rejestracji oddzielona była barierkami. Pacjenci byli obsługiwani przy poszczególnych okienkach po wyświetleniu odpowiedniego numeru.

- Na terenie rejestracji znajdowały się dwa ekrany informacyjne wyświetlające m.in. slajdy z klauzulą informacyjną o przetwarzaniu danych osobowych wraz z danymi kontaktowymi IOD, a także oddzielny slajd dotyczący funkcjonowania monitoringu wizyjnego. Stosowne klauzule w czasie trwania kontroli NIK umieszczono dodatkowo na tablicach informacyjnych znajdujących się w pomieszczeniach rejestracji.

- W widocznych miejscach umieszczone były komunikaty informujące o funkcjonowaniu monitoringu wizyjnego. Na drzwiach pomieszczeń zajmowanych przez personel rejestrujący pacjentów umieszczono informacje zabraniające wstępu osobom nieupoważnionym.

- Po zarejestrowaniu się w poradni pacjenci otrzymywali jeden dokument w formie wydruku potwierdzający fakt rejestracji i zawierający: dane osobowe, nazwę

[57] Lista pacjentów danego oddziału wraz z numerem sali, w których przebywają.

[58] Na podstawie art. 5 ust. 2 ustawy z dnia 6 września 2001 r. o dostępie do informacji publicznej (Dz. U. z 2018 r. poz. 1330 ze zm.) i art. 11 ust. 4 ustawy z dnia 16 kwietnia 1993 r. o zwalczaniu nieuczciwej konkurencji (Dz. U. z 2019 r. poz. 1010) NIK wyłączyła jawność informacji w zakresie stosowanych metod zabezpieczenia fizycznego i technicznego. Wyłączenia tego dokonano w interesie przedsiębiorcy.

[59] Art. 17 i 18 ustawy z dnia 6 listopada 2008 r. o prawach pacjenta i Rzeczniku Praw Pacjenta (Dz. U. z 2017 r. poz. 1318, ze zm., dalej: ustawa o prawach pacjenta), art. 32 i 34 ustawy z dnia 5 grudnia 1996 r. o zawodach lekarza i lekarza dentysty (Dz.U. z 2018 r. poz. 617, ze zm.), art. 74 ustawy z dnia 23 kwietnia 1964 r. - Kodeks cywilny (Dz. U. z 2018 r. poz. 1025, ze zm.)

[60] Na podstawie art. 5 ust. 2 ustawy z dnia 6 września 2001 r. o dostępie do informacji publicznej (Dz. U. z 2018 r. poz. 1330 ze zm.) i art. 11 ust. 4 ustawy z dnia 16 kwietnia 1993 r. o zwalczaniu nieuczciwej konkurencji (Dz. U. z 2019 r. poz. 1010) NIK wyłączyła jawność informacji w zakresie stosowanych metod zabezpieczenia fizycznego i technicznego. Wyłączenia tego dokonano w interesie przedsiębiorcy.

poradni, nazwę płatnika, numer pokoju, datę przyjęcia w poradni, przewidywaną godzinę przyjęcia i numer skierowania[61].

- Osoby dokonujące rejestracji pacjentów na swoich stanowiskach nie posiadały dokumentacji medycznej gdyż, jak to wyżej wskazano, dane przetwarzano wyłącznie w systemie informatycznym. Identyfikacja pacjentów odbywała się na podstawie dowodu osobistego. Monitory komputerów ustawiono w sposób uniemożliwiający wgląd do danych osobom postronnym. W trakcie kontroli NIK nie ujawniono przypadków posługiwania się danymi wrażliwymi przez pracowników Szpitala.

- We wszystkich gabinetach lekarskich na terenie WCO pacjenci oczekujący na wizytę przyjmowani byli według kolejności wynikającej z numeru przydzielonego podczas rejestracji. Pacjenci wchodzili do gabinetów po wywołaniu ich imienia przez pielęgniarki lub sekretarki medyczne.

- W gabinetach lekarskich personel dysponował w systemie komputerowym listą osób zapisanych na dany dzień i godzinę, nie korzystając przy tym z dokumentacji medycznej w formie papierowej, albowiem była ona sporządzana w formie elektronicznej. Stanowisko komputerowe było obsługiwane przez towarzyszącego lekarzowi pracownika posiadającego upoważnienie do przetwarzania danych osobowych, tj. sekretarkę medyczną lub pielęgniarkę.

- […][62]

(akta kontroli str. 281-321)

W WCO jeszcze przed wejściem w życie przepisów RODO stosowano monitoring wizyjny w pomieszczeniach ogólnodostępnych dla pacjentów i personelu, który rejestrował obraz obejmujący ciągi piesze, pomieszczenie rejestracji głównej oraz sale intensywnej opieki medycznej. System ten wykorzystywany był zgodnie z art. 111 ustawy o ochronie danych osobowych i art. 22² Kodeksu pracy[63]. Informację o stosowaniu monitoringu wizyjnego umieszczono w układzie zbiorowym pracy dla pracowników WCO dnia 28 listopada 2018 r. z mocą obowiązującą od 1 stycznia 2019 r.[64]. W Szpitalu obowiązywała wewnętrzna procedura w zakresie monitoringu wizyjnego[65], zgodnie z którą system ten nadzorował główny energetyk WCO. Nagrania obrazu przechowywano przez okres nieprzekraczający trzech miesięcy albo do czasu prawomocnego zakończenia postępowania, jeśli stanowiły one dowód w prowadzonych sprawach. Klauzula obowiązku informacyjnego dla pracowników zawierająca wpis na temat monitoringu wizyjnego od 1 stycznia 2019 r. przekazywana była przez Dział Spraw Pracowniczych nowemu pracownikowi przed dopuszczeniem go do pracy. Pracownik potwierdzał zapoznanie się z zasadami tego monitoringu. Wcześniej, także przez RODO, informacja o monitoringu była przekazywana nowo zatrudnianym pracownikom podczas podpisywania dokumentów związanych z zatrudnieniem. Ponadto była udostępniona w serwisie Intranet, na stronie internetowej WCO oraz wyświetlana

[61] Wydruk zawierał też kod QR, za pomocą którego pacjent mógł wyznaczyć trasę w kiosku nawigacyjnym WCO.

[62] Na podstawie art. 5 ust. 2 ustawy z dnia 6 września 2001 r. o dostępie do informacji publicznej (Dz. U. z 2018 r. poz. 1330 ze zm.) i art. 11 ust. 4 ustawy z dnia 16 kwietnia 1993 r. o zwalczaniu nieuczciwej konkurencji (Dz. U. z 2019 r. poz. 1010) NIK wyłączyła jawność informacji w zakresie stosowanych metod zabezpieczenia fizycznego i technicznego. Wyłączenia tego dokonano w interesie przedsiębiorcy.

[63] Ustawa z dnia 26 czerwca 1974 r., Dz. U. z 2018 r. poz. 917, ze zm.

[64] Protokół dodatkowy nr 1 do zuzp nr U-CMI/1017/12 zawarty w dniu 15 listopada 2018 r. został wpisany do rejestru Państwowej Inspekcji Pracy w dniu 28 listopada 2018 r. (Rozdział XIII – Monitoring Wizyjny, Rozdział XIV – Monitoring Poczty Elektronicznej i Monitoring Aktywności w Sieci).

[65] Procedura monitoringu w WCO, Załącznik nr WCO.PBI.P022 do PBI, wersja 01.00, zatwierdzenie przez ADO 2 grudnia 2018 r.

na ekranach dotykowych w pomieszczeniu rejestracji[66]. W widocznych miejscach, w czytelny sposób oznaczono pomieszczenia i teren monitorowany.

Dyrektor wyjaśnił m.in, że procedura regulująca monitoring została wprowadzona do układu zbiorowego najszybciej jak to było możliwe, biorąc pod uwagę zasady wprowadzenia zmian, które wymagają zgody wszystkich stron oraz akceptację Państwowej Inspekcji Pracy. Prace nad wprowadzeniem nowych regulacji formalnych rozpoczęły się po 25 maja 2018 r. w drodze negocjacji z pięcioma funkcjonującymi w WCO związkami zawodowymi, podczas których w międzyczasie powstały dwa kolejne związki, które wstąpiły w prawa i obowiązki stron układu zbiorowego w dniu 13 listopada 2018 r. Dopiero po tym terminie można było skierować do Państwowej Inspekcji Pracy wniosek o rejestrację regulaminu monitoringu w układzie zbiorowym. Dyrektor podkreślił, że stworzenie wewnętrznej procedury monitoringu jest przejawem szczególnej staranności administratora danych osobowych, gdyż nie jest to wymagane przepisami prawa.

(akta kontroli str. 61-71, 92-93, 224-227, 1037-1060)

2.2 W WCO, zgodnie z art. 24 ust. 2 pkt 2 ustawy o prawach pacjenta, a także art. 5 ust. 1 lit. c RODO i art. 20 ust. 2 pkt 7 lit. c rozporządzenia KRI, personel administracyjny szpitala posiadał dostęp do danych medycznych wyłącznie w zakresie niezbędnym do wykonywanych zadań.

Nowym pracownikom dostęp do danych medycznych w systemie informatycznym WCO[67] przydzielany był przez ASI, na wniosek kierownika komórki organizacyjnej, w której wykonywali pracę. IOD weryfikował poziom wymaganych uprawnień względem zadań, jakie użytkownik miał realizować na danym stanowisku pracy. Użytkownik otrzymywał dostęp do systemu informatycznego po odebraniu upoważnienia i polecenia do przetwarzania danych osobowych w WCO wydawanego przez IOD, działającego z upoważnienia ADO. Obejmowało ono tylko zakres niezbędny do wykonywania zadań na zajmowanym stanowisku. Poziom dostępu do określonych danych osobowych i uprawnień w systemie informatycznym WCO był zindywidualizowany i podlegał modyfikacjom na wniosek kierownika komórki organizacyjnej, po akceptacji IOD i ASI. Osoba posiadająca aktywny profil w systemie informatycznym WCO nie miała automatycznie nadawanego dostępu do danych medycznych pacjentów[68]. Upoważnienie do przetwarzania danych osobowych nie było też tożsame z automatycznym dostępem do tych danych medycznych pacjentów w systemie informatycznym WCO.

W związku z rozpoczęciem stosowania RODO nie uległy zmianie zasady przydzielania uprawnień w systemie informatycznym i wydawania upoważnień do dostępu do danych osobowych i danych medycznych.

Na dzień 15 tycznia 2019 r. w WCO zatrudnionych było 128 osób wchodzących w skład personelu niemedycznego. Osoby te zatrudniono w działach administracyjnych Szpitala[69] oraz innych jego komórkach organizacyjnych[70]. W toku

---

[66] Klauzula Obowiązku Informacyjnego – osoby objęte monitoringiem wizyjnym w WCO, wersja 01.00, Załącznik nr E011m. do PBDO.P006, zatwierdzenie przez ADO 23 lipca 2018 r.; Klauzula Obowiązku Informacyjnego – pracownik WCO, wersja 03.01., Załącznik nr E011 do PBDO, zatwierdzenie przez ADO 2 listopada 2018 r.

[67] System Klasy HIS (Hospital Information System) – rodzaj oprogramowania do obsługi ruchu pacjentów wewnątrz podmiotu leczniczego.

[68] Procedura zarządzania dostępem użytkownika do systemów informatycznych, Załącznik nt P004 do PBDO, wersja: 02.00 z 11 lipca 2018 r.; Procedura zarządzania upoważnieniami i poleceniami do przetwarzania danych osobowych, Załącznik nr P002 do PBDO, wersja 02.01 z 25 kwietnia 2018 r.; Wniosek kierownika komórki organizacyjnej o przyznanie dostępu do systemu informatycznego, wersja 03.00 z 28 grudnia 2018 r.; Wniosek kierownika komórki organizacyjnej o przyznanie dostępu do domeny, wersja 03.00 z 28 grudnia 2018 r.

[69] Dyrekcja, Dział Administracji, Dział Ewidencji Świadczeń Medycznych, Dział Inwestycji i Remontów, Dział Zamówień Publicznych i Zaopatrzenia, Dział Obsługi Porządkowo – Transportowej, Dział Żywienia, Dział Szkoleń i Współpracy Naukowej, Dział Informatyki, Dział Spraw Pracowniczych, Kancelaria, Księgowość, Apteka, Punkt Informacyjny, Sekcja Rejestracji i Dokumentacji Chorych, Sekcja ds. Badań Klinicznych, Sekcja Rozliczeń Kosztów, Wielkopolskie Biuro Rejestracji Nowotworów, Zespół Magazynów.

oględzin zweryfikowano zakres uprawnień w systemie informatycznym dla 30 pracowników niemedycznych WCO, stwierdzając że 13 osób posiadało ten dostęp w zakresie niezbędnym do wykonywania zadań i miejsca zatrudnienia (np. moduł magazyn, apteczka, rozliczenia). Pozostałe 17 osób nie posiadało takiego dostępu, co wynikało z ich zakresów obowiązków.

Osoby, które nie posiadały upoważnienia do przetwarzania danych osobowych podpisywały zobowiązania do zachowania tajemnicy w tym zakresie (podobnie jak osoby upoważnione do przetwarzania tych danych). Dotyczyło to głównie personelu sprzątającego[71].

(akta kontroli str. 80-84, 102-105, 118-120, 128-213, 370-377, 947-991, 1077-1093, 1356-1376, 1549-1567)

2.3 Na próbie 30 pielęgniarek i położnych spośród z 335 zatrudnionych w WCO[72] stwierdzono, że we wszystkich przypadkach dostęp do szpitalnego systemu informatycznego był adekwatny do realizowanych zadań. W 11 przypadkach uprawnienia te wykraczały poza komórki organizacyjne Szpitala, do których te osoby były przypisane w systemie finansowo-kadrowym. W dziewięciu przypadkach dostęp poszerzono o jeszcze inne jednostki organizacyjne WCO, a w dwóch pielęgniarki posiadały dostęp wyłącznie do innego oddziału, niż ten do którego były przypisane. Dostęp ten był jednak zgodny z wykonywanymi czynnościami i faktycznym miejscem świadczenia pracy, co zostało odzwierciedlone w upoważnieniach do przetwarzania danych osobowych oraz wnioskach złożonych przez kierowników komórek organizacyjnych o przyznanie odpowiedniego dostępu w systemie informatycznym.

W WCO nie były wydawane upoważnienia do przetwarzania danych osobowych i medycznych pacjentów dla salowych i sanitariuszy. Osoby te nie posiadały też możliwości wglądu do danych medycznych pacjentów w systemach informatycznych Szpitala. Wybrany personel sprzątający oraz obsługujący punkt informatyczny posiadał ww. upoważnienia, które były wydawane wyłącznie w zakresie niezbędnym do wykonania zadań na zajmowanym stanowisku lub zadań koniecznych do realizacji umowy.

(akta kontroli str. 80-84, 112-118, 128-149, 152-172, 350-365, 838-846, 1176-1201, 1543-1567, 1773-1804)

2.4. Spośród 23 osób, z którymi rozwiązano umowy o pracę w okresie od 25 maja 2018 r. do 15 stycznia 2019 r., 20 osobom zablokowano konta w systemie Windows i systemie informatycznym WCO w dniu wygaśnięcia stosunku pracy. Dwóch pracowników nadal posiadało dostęp do ww. systemów, gdyż osoby te zmieniły formę zatrudnienia w Szpitalu i zawarły umowy cywilno-prawne w trybie art. 26 i 27 ustawy z dnia 15 kwietnia 2011 r. o działalności leczniczej[73].

W przypadku jednego z pozostałych pracowników konto w domenie Windows nie zostało zablokowane w dniu rozwiązania stosunku pracy tj. 31 grudnia 2018 r., gdyż nie zgłosił się on z kartą obiegową do Działu Informatyki. Zgodnie z procedurami wewnętrznymi, w zakresie dostępu do systemów informatycznych w WCO, pracownik był zobowiązany do rozliczenia się z pracodawcą, o czym został powiadomiony przez Dział Spraw Pracowniczych. Wraz z wygaśnięciem stosunku pracy anulowano mu upoważnienie do przetwarzania danych osobowych.

[70] Klinika Chirurgii Głowy, Szyi i Onkologii Laryngologicznej, Oddział Chemioterapii, Zakład Radioterapii III, Zakład Radioterapii IV, Pracownia Psychologii Klinicznej, Zakład Epidemiologii i Profilaktyki Nowotworów.
[71] Wykaz 111 osób objętych zobowiązaniem do zachowania w tajemnicy danych osobowych z 22 stycznia 2018 r., załącznik nr 2 do pisma DL.08/2-2-511/2019.
[72] Na dzień 15 stycznia 2019 r.
[73] Dz. U. z 2018 r. poz. 2190.

Jakkolwiek pracownikowi temu zablokowano dostęp do systemu informatycznego WCO zawierającego dane medyczne i dane osobowe pacjentów w dniu 7 stycznia 2019 r., a zablokowanie jego konta do systemu operacyjnego nastąpiło 1 lutego 2019 r. (tj. odpowiednio po siedmiu i 31 dniach), to od dnia zakończenia pracy nie posiadał on dostępu do domeny Windows, gdyż dostęp taki nie był możliwy z zewnętrznego środowiska informatycznego, tj. wymagał użycia szpitalnego stanowiska komputerowego. Ponadto logowanie do domeny Windows wymagało uwierzytelnienia przy użyciu imiennej karty inteligentnej zabezpieczonej numerem PIN[74], która to została przez pracownika zwrócona w dniu zakończenia pracy.

Dostrzegając, że ww. pracownik nie miał realnej możliwości uzyskania dostępu do danych osobowych pacjentów po 31 grudnia 2018 r., NIK wskazuje, że w świetle § 20 ust. 2 pkt 5 rozporządzenia KRI, kierownictwo podmiotu publicznego jest obowiązane do podejmowania działań zapewniających bezzwłoczną zmianę uprawnień w przypadku zmiany zadań osób zaangażowanych w proces przetwarzania informacji (w tym do odbierania uprawnień w systemach po zakończeniu zatrudnienia).

Dyrektor wyjaśnił, że na pracowniku ciążył obowiązek rozliczenia się z zakładem pracy i był on informowany o tym przez Dział Spraw Pracowniczych. Podał, że w sytuacji braku rozliczenia ww. komórka organizacyjna przesyła do byłego pracownika pismo z informacją o konieczności dokonania rozliczenia lub powiadamia o takiej konieczności drogą telefoniczną - co miało miejsce w tym przypadku. Dyrektor wskazał, że sytuacja ta zainicjowała potrzebę wprowadzenia zmiany do procedur wewnętrznych.

Od 22 lutego br. w WCO wprowadzono zasadę informowania administratora właściwego systemu informatycznego przez Dział Spraw Pracowniczych, o zakończeniu stosunku pracy z użytkownikiem tego systemu.

(akta kontroli str. 80-84, 112-120, 366-369, 838-846, 1176-1201, 1356-1376, 1543-1567, 1773-1804)

2.5 […][75]

(akta kontroli str. 344-349, 1805-1876)

2.6 W okresie od 25 maja 2018 r. do 15 stycznia 2019 r. WCO zawarło 34 umowy powierzenia przetwarzania danych osobowych z 26 podmiotami, które wykonywały na rzecz Szpitala strategiczne usługi związane z: świadczeniem opieki serwisowej w zakresie użytkowanych systemów informatycznych i specjalistycznego sprzętu medycznego, ochroną mienia i osób, archiwizacją oraz realizacją świadczeń zdrowotnych dla pacjentów WCO. We wszystkich ww. umowach Szpital był podmiotem powierzającym przetwarzanie danych. Zgodnie z wewnętrzną procedurą, umowa powierzenia mogła stanowić załącznik lub aneks do umowy zawartej na określoną usługę lub też część umowy głównej i podlegała zaewidencjonowaniu w Kancelarii Szpitala[76]. Analiza wybranych pięciu umów zawartych przez ADO z podmiotem zewnętrznym w zakresie powierzenia

[74] Dostęp do systemów regulują wewnętrzne procedury: WCO.PBI.P004 (Procedura zarządzania dostępem użytkownika do systemów informatycznych), WCO.PBI.PBDO.P005 (Program zgłaszania naruszeń ochrony danych osobowych), WCO.PBI.IZSI.P007 (Procedura zarządzania identyfikatorem użytkownika w systemach), WCO.IN.PC-PZKI (Procedura zarządzania kartami inteligentnymi użytkownika systemu informatycznego).

[75] Na podstawie art. 5 ust. 2 ustawy z dnia 6 września 2001 r. o dostępie do informacji publicznej (Dz. U. z 2018 r. poz. 1330 ze zm.) i art. 11 ust. 4 ustawy z dnia 16 kwietnia 1993 r. o zwalczaniu nieuczciwej konkurencji (Dz. U. z 2019 r. poz. 1010) NIK wyłączyła jawność informacji w zakresie zabezpieczeń i parametrów zdalnego dostępu do środowiska informatycznego WCO. Wyłączenia tego dokonano w interesie przedsiębiorcy.

[76] Powierzenie danych osobowych w imieniu ADO, Załącznik PBDO.P09 do PBDO, wersja 03.00 z 26 marca 2018 r., procedura jest stosowana w WCO od 6 lipca 2010 r.

przetwarzania danych wykazała, że spełniły one wymagania określone w art. 28 ust. 3 RODO.

NIK wskazuje, że w przypadku 12 umów powierzenia przetwarzania danych osobowych, zawartych w okresie od stycznia do kwietnia 2018 r., aneksy w których jako podstawę prawną przywołano przepisy RODO zawarto dopiero w listopadzie i grudniu 2018 r., tj. po upływie ponad sześciu miesięcy od rozpoczęcia stosowania tych przepisów. W przypadku dwóch innych umów zawartych w czerwcu i sierpniu 2018 r. wskazano nieaktualną podstawę prawną, a aneksy zawierające aktualną podstawę prawną (RODO) zawarto dopiero w grudniu 2018 r. NIK dostrzega przy tym, że wynikało to z konieczności stosowania wzorów umów przygotowanych przez Ministerstwo Zdrowia, w ramach realizacji projektu dofinansowanego z UE pt. „Realizacja Programu Profilaktyki Nowotworów Głowy i Szyi w województwie lubuskim, wielkopolskim i zachodniopomorskim”[77].

(akta kontroli str. 85-87, 106-111, 838-846, 1109-1120, 1701-1711, 1877-2036)

2.7 Prowadzony w WCO rejestr stwierdzonych przypadków naruszenia bezpieczeństwa danych osobowych nie zawierał wpisów o przypadkowym lub niezgodnym z prawem zniszczeniu, utraceniu, zmodyfikowaniu, nieuprawnionym ujawnieniu lub nieuprawnionym dostępie do danych osobowych. Po rozpoczęciu stosowania RODO nie odnotowano też skarg zgłoszonych do Dyrekcji i Pełnomocnika ds. Praw Pacjenta w zakresie naruszenia ochrony danych osobowych. W kontrolowanym okresie wpłynął jeden wniosek o usunięcie konta z systemu internetowego wco.pl, co odnotowano w rejestrze żądań osób, których dane przetwarzano[78].

(akta kontroli str. 939-946, 1094-1102, 1712-1724)

2.8 Sposób udostępniania kopii dokumentacji medycznej został uregulowany w procedurze[79] stanowiącej element ZSZ. Do 15 stycznia 2019 r. do WCO wpłynęło 230 wniosków o udostępnienie kserokopii dokumentacji medycznej od instytucji oraz 2.160 wniosków od osób fizycznych[80]. Natomiast w 53 przypadkach kserokopię dokumentacji medycznej udostępniono zakładom ubezpieczeń[81], a w 108 – Zakładowi Ubezpieczeń Społecznych[82]. Spośród spraw zakończonych udostępnieniem dokumentacji medycznej, szczegółowym badaniem objęto po 30 przypadków, w których została ona udostępniona zakładom ubezpieczeń oraz osobie fizycznej innej niż pacjent, którego dokumentacja ta dotyczyła.

W aktach spraw znajdowały się upoważnienia do udostępnienia kopii dokumentacji medycznej, złożone w oparciu o szablon WCO lub w dowolnej formie przygotowanej i podpisanej przez pacjenta. W przypadku wniosków złożonych przez zakłady ubezpieczeń dokumentów nie udostępniano, gdy dana osoba nie figurowała w bazie danych pacjentów WCO.

(akta kontroli str. 378-551)

---

[77] Umowa z 19 czerwca 2017 r. nr POWR.05.01.00-00-0002/16 między WCO i Ministerstwem Zdrowia. Projekt profilaktyczny w zakresie wczesnego wykrywania nowotworów głowy i szyi realizowany w ramach programu operacyjnego Wiedza Edukacja Rozwój 2014-2020, współfinasowanego ze środków Europejskiego Funduszu Społecznego.

[78] Założenie konta na stronie eRejestracja (https://erejestracja.wco.pl/) umożliwiało wielokrotne rejestrowanie pacjenta do poradni bez potrzeby ponownego podawania danych oraz podgląd historii zapisów.

[79] Procedura P-0-02-01 „Udostępnianie dokumentacji medycznej”, określa m.in. wzór wniosku, wzór rejestru dotyczącego udostępniania dokumentacji, kartę udostępnienia dokumentacji medycznej z archiwum zakładu oraz sposób postępowania w zależności do rodzaju podmiotu (pacjent albo zakład ubezpieczeń) występującego z takim wnioskiem.

[80] W tym w sprawie: udostępnienia kserokopii kartotek pacjentów (749), przekazania kopii dokumentacji medycznej pacjentom lub osobom upoważnionym (1 160), wydania oryginałów oraz kopii kart onkologicznych (odpowiednio 135 i 47), a także wysłania kserokopii kartotek za pośrednictwem poczty (191).

[81] W rozumieniu ustawy z dnia 11 września 2015 r. o działalności ubezpieczeniowej i reasekuracyjnej (Dz. U. z 2019 r. poz. 381).

[82] O którym mowa w ustawie z dnia 13 października 1998 r. o systemie ubezpieczeń społecznych (Dz. U. z 2019 r. poz. 300, ze zm.).

2.9 W WCO podejmowano odpowiednie działania mające na celu minimalizację ryzyka utraty danych osobowych pacjentów w wyniku awarii, błędów lub nieuprawnionej modyfikacji:

[…][83]

Stwierdzone nieprawidłowości

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

OCENA CZĄSTKOWA

NIK ocenia pozytywnie wprowadzone w Szpitalu rozwiązania organizacyjne i techniczne zmierzające do zapewnienia ochrony danych osobowych pacjentów oraz poszanowania ich prywatności. Zastosowane środki skutecznie przeciwdziałały ujawnieniu danych pacjentów osobom nieuprawnionym oraz ich utracie w wyniku awarii, błędów lub nieuprawnionej modyfikacji. Personelowi Szpitala zapewniono odpowiedni, zgodny z zakresem wykonywanych czynności dostęp do danych pacjentów, właściwie też udostępniano ich dokumentację medyczną. Stosowane środki techniczne i organizacyjne zapewniały stopień bezpieczeństwa adekwatny do ryzyk związanych m.in. ze skalą i rodzajem przetwarzanych danych osobowych.

IV. Uwagi i wnioski

Uwzględniając działania podjęte w trakcie kontroli w celu usunięcia stwierdzonej nieprawidłowości, Najwyższa Izba Kontroli nie formułuje uwag ani wniosków.

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 Poznaniu. 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.

Poznań, 16 kwietnia 2019 r.

Najwyższa Izba Kontroli
Delegatura w Poznaniu

Kontroler	Dyrektor
Daniel Braciszewski	z up. Tomasz Nowiński
inspektor kontroli państwowej	p.o. Wicedyrektora
.....	.....
podpis	*podpis*

[83] Na podstawie art. 5 ust. 2 ustawy z dnia 6 września 2001 r. o dostępie do informacji publicznej (Dz. U. z 2018 r. poz. 1330 ze zm.) i art. 11 ust. 4 ustawy z dnia 16 kwietnia 1993 r. o zwalczaniu nieuczciwej konkurencji (Dz. U. z 2019 r. poz. 1010) NIK wyłączyła jawność informacji w zakresie stosowanych metod zabezpieczenia środowiska informatycznego WCO. Wyłączenia tego dokonano w interesie przedsiębiorcy.