NAJWYŻSZA IZBA KONTROLI
Delegatura w Szczecinie

LSZ.410.002.04.2019

Krzysztof Kowalczyk
Dyrektor Samodzielnego Publicznego
Wielospecjalistycznego Zakładu Opieki Zdrowotnej
w Stargardzie
ul. Wojska Polskiego 27
73-110 Stargard

WYSTĄPIENIE POKONTROLNE

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

NAJWYŻSZA IZBA KONTROLI
Delegatura w Szczecinie
ul. Jacka Odrowąża 1, 71-420 Szczecin
T +48 91 831 39 00, F +48 91 831 39 66
lsz@nik.gov.pl

I. Dane identyfikacyjne

Jednostka kontrolowana	Samodzielny Publiczny Wielospecjalistyczny Zakład Opieki Zdrowotnej w Stargardzie ul. Wojska Polskiego 27, 73-110 Stargard[1].
Kierownik jednostki kontrolowanej	Krzysztof Kowalczyk Dyrektor Szpitala[2], od 15 stycznia 2018 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. do dnia zakończenia czynności kontrolnych.
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 Szczecinie.
Kontroler	Jarosław Pułka, główny specjalista kontroli państwowej, upoważnienie do kontroli nr LSZ/20/2019 z dnia 11 stycznia 2019 r. (akta kontroli str.1-2)

[1] Dalej: Szpital.

[2] Dalej: Dyrektor lub ADO.

[3] Dz. U. z 2019 r. poz. 489; dalej: ustawa o NIK.

II. Ocena ogólna[4] kontrolowanej działalności

OCENA OGÓLNA

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

Szpital wywiązał się z obowiązku powołania Inspektora Ochrony Danych i zgłoszenia tego faktu Prezesowi Urzędu Ochrony Danych Osobowych[5]. Przeprowadzono wymaganą analizę ryzyka procesów przetwarzania danych osobowych oraz opracowano rejestr czynności przetwarzania tych danych. Pracowników Szpitala zapoznano z regulacjami dotyczącymi ochrony danych osobowych. W Szpitalu prawidłowo chroniono i przetwarzano dane osobowe w skontrolowanych trzech oddziałach szpitalnych, trzech poradniach specjalistycznych oraz w rejestracji ogólnej do poradni specjalistycznych. Objęty kontrolą personel administracyjny Szpitala oraz pielęgniarki i położne przetwarzali dane osobowe w systemie HIS[6] adekwatnie do realizowanych zadań i obowiązków. W pięciu analizowanych umowach powierzenia przetwarzania danych osobowych zamieszczono postanowienia wymagane art. 28 rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (ogólne rozporządzenie o ochronie danych)[7]. Dokumentację medyczną pacjentów we wszystkich skontrolowanych sprawach udostępniono wyłącznie uprawnionym podmiotom. W trakcie kontroli zainstalowano monitoring serwerowni Szpitala, w której przechowywano dane osobowe przetwarzane w formie elektronicznej.

Stwierdzone nieprawidłowości polegały na:
- nieodbieraniu uprawnień do systemu HIS pracownikom, z którymi Szpital rozwiązał stosunek pracy,
- nadaniu personelowi medycznemu i lekarzom pełnych uprawnień administracyjnych w systemach operacyjnych,
- niestosowaniu indywidualnych identyfikatorów i haseł dostępu do systemów operacyjnych na oddziałach Szpitala,
- przechowywaniu kopii zapasowych elektronicznych baz danych Szpitala w tym samym pomieszczeniu, w którym przechowywano dane produkcyjne.

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

[5] Dalej: Prezes UODO.

[6] Hospital Information System – rodzaj oprogramowania przeznaczony do prowadzenia w wersji elektronicznej dokumentacji medycznej zbiorczej i indywidualnej oraz zarządzania ruchem chorych na oddziałach i w poradniach podmiotu leczniczego.

[7] Dz. Urz. UE L 119 z 4.05.2016 r., str. 1, ze zm. Rozporządzenie zwane dalej: RODO.

III. Opis ustalonego stanu faktycznego oraz oceny cząstkowe[8] kontrolowanej działalności

OBSZAR

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

Opis stanu faktycznego

1.1. Szpital z dniem 25.05.2018 r. wyznaczył Inspektora Ochrony Danych (dalej: *IOD*), wywiązując się tym samym z obowiązku określonego w art. 8 ustawy z dnia 10 maja 2018 r. o ochronie danych osobowych[9] w związku z art. 37 RODO. Pełnienie funkcji i wykonywanie zadań IOD powierzone zostało zewnętrznej osobie prowadzącej działalność gospodarczą pod nazwą iCentrum w Stargardzie[10]. W okresie od 1 maja 2018 r. do 24 maja 2018 r. ten sam podmiot wykonywał w Szpitalu funkcję Administratora Bezpieczeństwa Informacji (dalej: *ABI*). Szpital terminowo, tj. zgodnie z art. 8 i 10 u.o.d.o.[11], (za pośrednictwem formularzy elektronicznych) wywiązał się z obowiązku zawiadomienia Prezesa UODO o powołaniu IOD. Przekazane Prezesowi UODO zawiadomienie zawierało wszystkie elementy określone art. 10 ust. 1 i 3 u.o.d.o., tj. m.in.: imię, nazwisko oraz adres poczty elektronicznej i numer telefonu IOD, nazwę oraz adres siedziby i numer identyfikacyjny REGON administratora danych osobowych. Zgodnie z wymogiem określonym w art. 37 ust. 7 RODO oraz art. 11 w związku z art. 10 ust. 1 u.o.d.o., dane IOD oraz sposób i formę kontaktu udostępniono na stronie internetowej Szpitala[12].
W umowie z osobą wykonującą na rzecz Szpitala funkcję IOD, wskazano wszystkie zadania określone w art. 39 RODO, m.in. informowanie administratora danych osobowych oraz pracowników, którzy przetwarzają dane osobowe, o obowiązkach spoczywających na nich na mocy RODO, w tym działania zwiększające świadomość, szkolenia personelu. Osobie tej umożliwiono wykonywanie obowiązków w sposób niezależny, stosownie do art. 38 ust. 3 RODO. Samodzielne stanowisko IOD, podległe bezpośrednio Dyrektorowi Szpitala, zostało wyodrębnione w strukturze organizacyjnej Szpitala. W umowie IOD miał zagwarantowaną niezależność i nieusuwalność w związku z realizacją powierzonych zadań.

Zgodnie z wymogami art. 37 ust. 5 RODO, osoba realizująca zadania IOD miała należyte przygotowanie i kwalifikacje zawodowe do pełnienia swojej funkcji, tj. m.in.: posiadała wyższe wykształcenie prawnicze, tytuł doktora nauk ekonomicznych, certyfikat Kompetencji Inspektora Ochrony Danych – ekspert stosowania zabezpieczeń zgodnie z przepisami RODO, Certyfikat Pełnomocnika i Audytora Wewnętrznego ISO/IEC 27001:2013, Certyfikat Pełnomocnika Systemu Zarządzania Bezpieczeństwem Informacji oraz była wykładowcą na uczelniach wyższych w zakresie ochrony danych osobowych i bezpieczeństwa w cyberprzestrzeni.

(dowód: akta kontroli str. 36, 74-86, 140-144)

Pismem z 12.10.2018 r. Ministerstwo Zdrowia poinformowało Szpital o wszczęciu z urzędu postępowania administracyjnego w sprawie uznania Szpitala za operatora usługi kluczowej, o której mowa w art. 5 ust. 1 ustawy z dnia 5 lipca 2018 r. o

[8] 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.

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

[10] Umowa z 10.04.2018 r.

[11] W związku z art. 158 ust. 2 u.o.d.o., tj. w terminie do 1 września 2018 r.

[12] www.bip-zozstargard.pl/ochrona-danych-osobowych; www.zozstargard.pl

krajowym systemie cyberbezpieczeństwa[13]. Następnie pismem z 03.12.2018 r. Ministerstwo powiadomiło Szpital o zakończeniu postępowania w tej sprawie informując, że w sprawie zostanie wydana decyzja. Do dnia zakończenia kontroli (05.04.2019 r.) Szpital nie otrzymał decyzji Ministra Zdrowia w powyższej sprawie.

(dowód: akta kontroli str. 95-98)

Szpital rozpoczął budowę wewnętrznych struktur bezpieczeństwa informacji, w tym odpowiedzialnych za cyberbezpieczeństwo. Zarządzeniem Nr 126/2018 Dyrektora Szpitala z 27.11.2018 r. IDO, został powołany do pełnienia funkcji Pełnomocnika ds. Zarządzania Systemami Bezpieczeństwa i Informacji, jako osoba odpowiedzialna za kontakty z podmiotami krajowego systemu cyberbezpieczeństwa. W związku z tym Szpital 6.12.2018 r. dokonał zgłoszenia osoby wyznaczonej do kontaktów z CSRiT GOV[14].

(dowód: akta kontroli str. 89-94)

1.2. IOD po objęciu swojej funkcji, w okresie od 07.05. do 30.06.2018 r., przeprowadził audyt zgodności przetwarzania danych osobowych z przepisami RODO. Celem audytu była weryfikacja spełniania przez Szpital obowiązków wynikających z RODO. W wyniku audytu stwierdzono m.in., że:

- spełniono obowiązek informacyjny, jednak z dniem wejścia przepisów RODO koniecznym było opracowanie nowego wzoru klauzul;
- obowiązek opracowania i wdrożenia procedur był spełniony, jednak wdrożone w lutym 2018 r. dokumenty nie spełniały wszystkich wymogów przewidzianych dla Polityki Przetwarzania Danych Osobowych m.in. Szpital nie posiadał ustrukturyzowanych zbiorów danych osobowych, co stanowiło utrudnienie dla przeprowadzenia analizy i oceny ryzyka oraz rejestru operacji przetwarzania danych, a w dokumentacji brak było rozwiązań przewidzianych przepisami RODO;
- obowiązująca od lutego 2018 r. w Szpitalu Polityka Bezpieczeństwa Danych Osobowych, Instrukcja Zarządzania Systemami Informatycznymi służącymi do Przetwarzania Danych Osobowych oraz Zasady Przygotowywania, obiegu oraz prowadzenia Rejestru Umów Powierzenia Przetwarzania Danych Osobowych wymagały uaktualnienia i dostosowania ich do wymagań RODO;
- nie wszystkie osoby przetwarzające dane osobowe posiadały upoważnienia wystawione przez administratora danych; Szpital nie posiadał ewidencji osób upoważnionych do przetwarzania danych osobowych;
- nie prowadzono rejestru czynności przetwarzania danych osobowych;
- nie prowadzono analizy ryzyka oraz oceny skutków ryzyka;
- nie przeprowadzano audytów bezpieczeństwa informacji ani sprawdzeń przetwarzania danych w systemach informatycznych;
- nie opracowano i nie wdrożono wewnętrznych procedur naruszeń ochrony danych osobowych;
- nie sprawowano kontroli nad umowami powierzenia, w tym nie prowadzono w Szpitalu rejestru tych umów;
- nie prowadzono szkoleń osób dopuszczonych do operacji na danych;
- nie opracowano i nie wdrożono zasad ochrony prywatności pacjenta, w szczególności dotyczących sposobów potwierdzania tożsamości i identyfikacji pacjentów, zapewnienia anonimowości pacjentom podczas wzywania do gabinetów lekarskich oraz na salach chorych, oznaczania produktów leczniczych, stosowania kart przyłóżkowych na salach chorych, telefonicznego udostępniania informacji o pacjencie - by ułatwić personelowi przetwarzanie danych pacjenta podczas udzielania świadczeń medycznych;

[13] Dz. U. poz. 1560, dalej: ustawa o cyberbezpieczeństwie.

[14] CSRiT GOV - Zespół Reagowania na Incydenty Bezpieczeństwa Komputerowego.

- nie wprowadzono zasad korzystania z systemów informatycznych Szpitala podczas przetwarzania danych, by ułatwić personelowi wykonywanie operacji na danych pacjentów - co stwarzało ryzyko wystąpienia naruszeń podczas wykonywania przez personel Szpitala operacji na danych w systemie informatycznym z powodu nieznajomości zasad przetwarzania danych w formacie elektronicznym.

Wśród zaleceń przedstawionych w swoim audycie IOD rekomendował, by w Szpitalu podjąć następujące działania:
- weryfikacja dokumentacji/przepisów wewnętrznych Szpitala w zakresie ochrony danych osobowych i uzupełnienie ich o regulacje, które powinny zapewniać bezpieczeństwo ochrony danych osobowych oraz umożliwiać wykazanie zasady rozliczalności przez administratora danych - należy uzupełnić istniejące dokumenty w zakresie ochrony danych o rozwiązania, na które wskazują zapisy RODO;
- przygotowanie i wdrożenie Rejestru czynności przetwarzania zgodnie z postanowieniami art. 30 RODO;
- rejestrowanie i wdrożenie postępowania w przypadku naruszeń oraz ich raportowania zgodnie z art. 33-34 RODO;
- realizację obowiązku informacyjnego wobec osób, których dane są przetwarzane przez Szpital zgodnie z art. 12-14 RODO;
- szacowanie ryzyka przetwarzania danych, w tym jego analiza;
- analiza procesów powierzania danych;
- weryfikacja oraz doskonalenie systemów informatycznych w Szpitalu w oparciu o określone w RODO zasady zapewnienia podczas przetwarzania danych prywatności oraz domyślnej ochrony danych;
- usprawnienie i doskonalenie systemu przetwarzanych informacji zgodnie z wytycznymi zawartymi w rozporządzeniu Rady Ministrów z dnia 12 kwietnia 2012 r. w sprawie Krajowych Ram Interoperacyjności, minimalnych wymogów dla rejestrów publicznych i wymiany informacji w postaci elektronicznej oraz minimalnych wymagań dla systemów teleinformatycznych[15] ;
- przeprowadzenie procesu kompleksowego upoważniania do przetwarzania danych, w tym przygotowanie Rejestru upoważnień;
- przeszkolenie personelu Szpitala z zasad ochrony danych osobowych zgodnych z RODO;
- wdrożenie zasad poszanowania intymności i godności pacjenta;
- informowanie o przetwarzaniu danych pozyskiwanych podczas stosowania monitoringu wizyjnego.

(dowód: akta kontroli str. 99-139)

Realizując powyżej określone zadania w Szpitalu dostosowano dokumentację do przepisów RODO. W dniu 2.07.2018 r. zatwierdzono i podano do wiadomości personelowi Politykę Ochrony Danych (dalej: *Polityka*), obejmującą :
- Politykę Bezpieczeństwa Danych Osobowych (wraz ze wzorem Rejestru czynności przetwarzania danych);
- Instrukcję Zarządzania Systemami Informatycznymi (dalej: *IZSI*) służącymi do Przetwarzania Danych Osobowych;
- Zasady Przygotowywania, obiegu oraz prowadzenia Rejestru Umów Powierzenia Przetwarzania Danych Osobowych.

W Polityce uregulowano ewidencjonowanie osób upoważnionych do przetwarzania danych osobowych. Określono wzory upoważnień do przetwarzania danych oraz wzór Rejestru Osób upoważnionych do przetwarzania danych. Uregulowano również procedury realizacji obowiązku informacyjnego wobec osób, których dane

[15] Dz. U. z 2017 r., poz. 2247; dalej: rozporządzenie KRI.

Szpital przetwarzał. Wprowadzono wzór klauzul informacyjnych wraz z wykazem elementów koniecznych, które taka klauzula musi posiadać oraz sposoby realizacji tego obowiązku. W dokumencie zawarto również informacje dotyczące obsługi zgłoszeń dotyczących realizacji praw osób, których dane Szpital przetwarza, uregulowano zasady dotyczące umów powierzenia (uszczegółowione i zaktualizowane 31.12.2018 r.). Opracowano rejestr czynności przetwarzania danych, który stanowił formę dokumentowania czynności przetwarzania danych, pełnił rolę mapy przetwarzania danych i był jednym z kluczowych elementów umożliwiających realizację zasady rozliczalności (inwentaryzowanie i monitorowanie sposobu wykorzystywania danych osobowych).

(dowód: akta kontroli str. 233-245)

W IZSI opisano m.in. cele i zasady bezpieczeństwa systemów informatycznych oraz sposoby zabezpieczenia i użytkowania systemów informatycznych. Dokument określał aspekty zabezpieczeń (procedura nadawania uprawnień do przetwarzania danych osobowych, procedura rozpoczęcia, zawieszenia i zakończenia dla użytkowników systemu, długość i złożoność haseł dostępowych serwerów, strukturę sieci informatycznej oraz częstotliwość sporządzania kopii bezpieczeństwa, procedury wykonywania przeglądu i konserwacji systemów oraz nośników informacji do przetwarzania danych osobowych). Dokument był udostępniany tylko służbom informatycznym Szpitala, odpowiedzialnym za wdrożenie i stosowanie tych regulacji. W dokumentacji tej były przywołane przepisy RODO.

(dowód: akta kontroli str. 246-265)

Oprócz wyżej wymienionych dokumentów, w Szpitalu 17.01.2019 r. wdrożono dodatkowe dokumenty wewnętrzne, w których uszczegółowiono zasady opisane we wdrożonej 2.07.2018 r. Polityce, tj. dokument pn.: „Ochrona Prywatności Pacjenta - Procedury Postępowania Podczas Przetwarzania Danych Osobowych Pacjenta" oraz „Vademecum w zakresie ochrony danych podczas korzystania z systemów informatycznych Szpitala". W procedurze Ochrony Prywatności Pacjenta uregulowano zasady zapewnienia anonimowości oraz potwierdzania tożsamości pacjenta podczas rejestracji, na salach chorych oraz w gabinetach lekarskich, zasady oznaczania materiałów medycznych oraz udzielania informacji o pacjencie. W Vademecum (wyciąg z IZSI) zaprezentowano personelowi Szpitala, który przetwarza dane osobowe w systemach informatycznych, w sposób uproszczony zasady korzystania z HIS podczas przetwarzania danych.

(dowód: akta kontroli str. 293-307)

W sprawie zaktualizowania dokumentacji Szpitala 37 dni po terminie wejścia w życie przepisów RODO, Dyrektor Krzysztof Kowalczyk wyjaśnił, że dnia 25 maja 2018 r., zgodnie z art. 30 RODO zrealizowany był obowiązek prowadzenia rejestru czynności przetwarzania. W szpitalu obowiązywała polityka ochrony danych, a zapisy w dokumentacji nie były niezgodne z RODO, w związku z czym nie istniała potrzeba ich uchylenia. Na dzień 25 maja 2018 r. w Szpitalu trwał audyt, którego celem było m.in. *dostosowanie Administratora Danych do reformy danych osobowych*. RODO nie określa szczegółowo zakresu i formy dokumentacji wewnętrznej w zakresie ochrony danych, a Administrator ma dowolność w ich określaniu. Jedynym wymaganym dokumentem jest Rejestr czynności przetwarzania, który został przygotowany na 25.05.2018 r. W wyjaśnieniach Dyrektor wskazał, że *w Szpitalu ostatecznie funkcjonuje zarówno obligatoryjny Rejestr czynności (od 25.05.2018 r.), jak i fakultatywne procedury rejestrowania czynności (od 2.07.2018 r.).*

(dowód: akta kontroli str. 392-395)

1.3. Rejestr czynności przetwarzania danych osobowych (dalej: *Rejestr*), o którym mowa w art. 30 RODO, został sporządzony 25.05.2018 r.
Zgodnie z wymogami art. 30 ust. 3 RODO, rejestr prowadzony był w formie pisemnej i elektronicznej oraz zawierał wymagane elementy, określone w ust. 1 tego przepisu, w tym: dane kontaktowe ADO i IOD; cele przetwarzania; opis kategorii osób, których dane dotyczą; kategorie odbiorców, którym dane osobowe zostały lub zostaną ujawnione; ogólny opis technicznych i organizacyjnych środków bezpieczeństwa, o których mowa w art. 32 ust. 1 RODO; planowane terminy usunięcia poszczególnych kategorii danych oraz informację dotyczącą ewentualnego przekazania danych osobowych do państwa trzeciego lub organizacji międzynarodowej. W Rejestrze zamieszczono dla każdej z 9 wykazanych kategorii osób, których dane dotyczą m.in.: zakres, charakter i kontekst przetwarzanych danych; podstawę prawną przetwarzania; sposób realizacji praw osób, których dane są przetwarzane.

(dowód: akta kontroli str. 396-397)

1.4. W Szpitalu 02.05.2018 r. przeprowadzono analizę procesów przetwarzania danych osobowych. Dokonano analizy zagrożeń i zabezpieczeń w kontekście ochrony przed utratą poufności, integralności i dostępności. Dokonano oceny prawdopodobieństwa wystąpienia strat, analizy podatności i oceny ryzyka. Szacowania ryzyka dokonano w oparciu o takie zagrożenia jak: całkowita bądź częściowa utrata danych w skutek awarii dysków (działania zaradcze określone w procedurach: tworzenie kopii), nieuprawniony dostęp do danych (wdrożone działania zaradcze: firewall, polityka haseł), utrata zasilania (wdrożone działania: zasilanie awaryjne UPS), brak dostępu do internetu w skutek awarii (wdrożone działania: niezależne łącze zapasowe), uszkodzenie w czasie prac remontowych czy konserwacyjnych (wdrożone działania: okablowanie zabezpieczone w korytkach, pełna dokumentacja techniczna). Wszystkie działania zaradcze zostały wdrożone.

(dowód: akta kontroli str. 383-385)

1.5. Szpital nie przeprowadzał oceny skutków dla operacji przetwarzania danych osobowych. IOD wyjaśnił, że zgodnie z art. 35 ust. 1 RODO ocena skutków ryzyka (tzw. DPIA) powinna być przeprowadzana, jeżeli dane przetwarzane są w szczególności z użyciem nowych technologii i może powodować wysokie ryzyko naruszenia praw lub wolności osób fizycznych. Ocena taka jest wymagana w szczególności w przypadku przetwarzania na dużą skalę szczególnych kategorii danych osobowych, o których mowa w art. 9 ust. 1 RODO. Aktualnie trwają prace nad zatwierdzeniem przez Prezesa UODO kodeksu branżowego dla placówek medycznych w zakresie stosowania RODO, który wskaże konieczność przeprowadzenia DPIA. Kodeks Postępowania dla Sektora Ochrony Zdrowia z dnia 13 listopada 2018 r.[16] w pkt. 5.3. stanowi, że podmioty, które nie przetwarzają na dużą skalę danych nie muszą przeprowadzać oceny skutków dla ochrony danych, wymaganych na podstawie art. 35 ust. 3 RODO.

(dowód: akta kontroli str. 398-399)

1.6. W Szpitalu przeprowadzono w okresie objętym badaniem szkolenia z zakresu RODO. Szkolenia grupowe prowadzone były przez IOD w okresie 28.05. – 10.07.2018 r. Ponadto prowadzone były szkolenia osób przyjmowanych do pracy oraz osób powracających do pracy z urlopów i zwolnień. Łącznie, wg stanu na 04.04.2019 r., przeszkolono 307 osób przy ogólnym zatrudnieniu 320 osób posiadających dostęp do danych osobowych (personel medyczny i administracja z wyłączeniem pracowników obsługi gospodarczej, którzy nie posiadali dostępu do

[16] Wersja: 22 przygotowana w celu przedłożenia do Prezesa Urzędu Ochrony Danych Osobowych (załącznik nr 1 do wniosku).

zbiorów danych, tj. pomoc kuchenna, konserwator, pracownik gospodarczy itp.) co stanowiło 96 % - przy czym z 13 nieprzeszkolonych osób, 12 przebywało na długotrwałych zwolnieniach lub urlopach (macierzyńskie, wychowawcze, urlop bezpłatny itp.).

(dowód: akta kontroli str. 403-426, 567-574)

1.7. W sprawie stosowania w Szpitalu kodeksu branżowego, IOD wyjaśnił, że Szpital zamierza stosować regulacje określone w projekcie kodeksu branżowego, jak tylko zostanie przyjęty i zatwierdzony przez organ nadzorczy. Posiłkując się zapisami kodeksu w Szpitalu opracowano tzw. Podręcznik dobrych praktyk pn. „Ochrona Prywatności Pacjenta. Procedury Postępowania podczas Przetwarzania Danych Osobowych Pacjenta." Dokument został wdrożony w Szpitalu zarządzeniem nr 2/2019 z 17.01.2019 r. IOD uczestniczył jako ekspert w pracach nad projektem kodeksu podczas konferencji pn. „RODO w sektorze medycznym – gdzie jesteśmy, dokąd zmierzamy?", która odbyła się 27.02.2019 r. Ponadto Szpital przystąpił do kampanii promującej wdrażanie zasad opisanych w przygotowywanym kodeksie branżowym - rododlapacjenta.pl[17].

(dowód: akta kontroli str. 88-91)

Ustalone nieprawidłowości

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

OCENA CZĄSTKOWA

Najwyższa Izba Kontroli pozytywnie ocenia działalność jednostki w kontrolowanym zakresie. Szpital opracował i wdrożył dokumentację oraz procedury dotyczące ochrony danych osobowych uwzględniając przepisy RODO. Ich aktualizacja i dostosowanie nastąpiło po miesiącu od wejścia w życie rozporządzenia. Wywiązano się z obowiązku powołania IOD i terminowego zgłoszenia tego faktu Prezesowi UODO. Pracowników Szpitala przeszkolono w zakresie ochrony danych osobowych i zagadnień dotyczących bezpieczeństwa. Prowadzony rejestr czynności przetwarzania został wdrożony 25 maja 2018 r. i zawierał wszystkie wymagane elementy, zgodnie z art. 30 RODO.

OBSZAR

2. Zapewnienie prawidłowego przetwarzania i ochrony danych osobowych.

Opis stanu faktycznego

2.1. W celu właściwej ochrony danych osobowych w Szpitalu wprowadzono następujące rozwiązania:

- w trzech badanych oddziałach Szpitala[18] na łóżkach szpitalnych nie było kart pacjentów z ich nazwiskiem i innymi danymi o stanie zdrowia pacjenta;
- pacjenci badanych oddziałów posiadali na nadgarstkach opaski z numerem tzw. księgi głównej oraz nr PESEL[19] . Szpital nie posiadał specjalistycznej drukarki do wydruków opasek, sporządzano je ręcznie;
- w dyżurkach pielęgniarskich na trzech objętych oględzinami oddziałach szpitalnych ruch chorych[20] prowadzony był w miejscu niewidocznym dla osób postronnych. W dyżurkach oraz w gabinetach lekarskich znajdowały się szafki na dokumentację medyczną zamykane na klucz. W salach chorych łóżka oznaczono numerem zawierającym numer sali i numer łóżka;

[17] Szczegóły na stronie: http://zozstargard.pl/pacjencie-znaj-swoje-prawa-z-rodo/

[18] Oddział Ginekologiczno-Położniczy, Oddział Chorób Wewnętrznych, Oddział Chirurgii Ogólnej.

[19] Dane na opasce były od strony ciała.

[20] Ruch chorych to lista pacjentów danego oddziału wraz z numerem sali, w których przebywają pacjenci.

- Personel pielęgniarski we wszystkich objętych oględzinami oddziałach szpitalnych, opuszczając dyżurkę pielęgniarek, blokował dostęp do systemu komputerowego;

(dowód: akta kontroli str. 428-444)

Na terenie Szpitala funkcjonowała jedna ogólna rejestracja. Punkt rejestracyjny był odrębnym zespołem pomieszczeń (trzech), w tym jednego, w którym odbywała się rejestracja pacjentów. Pozostałe dwa pomieszczenia, to pomieszczenie z kartoteką (szafy metalowe zabezpieczone na klucz) oraz pomieszczenie ze stanowiskami rejestracji telefonicznej (trzy stanowiska). Dostęp pacjentów do stanowisk rejestracyjnych odbywał się z korytarza/poczekalni przez przeszkolone drzwi. Na drzwiach umieszczona był informacja, że w pomieszczeniu może znajdować jedna osoba – przy każdym stanowisku. Taka sama informacja umieszczona była przy każdym stanowisku rejestracyjnym. Ponadto wyznaczone zostały obszary (poprzez wyklejenie jaskrawą żółtą taśmą na podłodze) każdego stanowiska. Klauzule informacyjne w formie wydruku umieszczone były na tablicy informacyjnej znajdującej się bezpośrednio przy wejściu do rejestracji oraz na tablicy w pomieszczeniu ze stanowiskami rejestracyjnymi. Treść klauzuli była zgodna z treścią klauzuli stanowiącej załącznik do obowiązującej Polityki Bezpieczeństwa Danych Osobowych. Przy rejestracji i wewnątrz zamieszczona był informacja o konieczności okazania dowodu osobistego w rejestracji (lub innego dokumentu, jak również określono i zapewniono możliwość spisania danych na kartkach papieru – w przypadku braku dokumentów). Wszystkie trzy komputery znajdujące się w rejestracji były ustawione w sposób uniemożliwiający wgląd w treści na nich wyświetlane osobom rejestrującym się. W obrębie wzroku pacjenta znajdującego się przy stanowisku rejestracji nie było dokumentów zawierających dane osobowe innych pacjentów.

Pacjenci oczekujący na wizytę w poradniach wywoływani byli według kolejności rejestracji bez podawania imienia i nazwiska i innych danych osobowych pacjenta[21].

We wszystkich trzech objętych oględzinami gabinetach poradni specjalistycznych[22] Szpitala dokumentację pacjentów przechowywano we właściwy sposób. Pacjent wchodzący do gabinetu nie miał możliwości zapoznania się z danymi osobowymi innych osób oczekujących w kolejce lub tych, którzy odbyli już wizytę. W trakcie oględzin żaden gabinet nie został pozostawiony bez opieki, a w drzwiach do gabinetów nie zostały pozostawione klucze.

Na poddanych oględzinom oddziałach, poradniach i rejestracji nie stwierdzono niewłaściwego zabezpieczenia danych medycznych oraz osobowych pacjentów. Rozwiązania techniczne i organizacyjne nie stwarzały możliwości ujawnienia danych medycznych pacjentów.

(dowód: akta kontroli str. 445-448)

Na terenie Szpitala funkcjonował monitoring w miejscach wskazanych w Regulaminie Monitoringu, który był dostępny na stronie internetowej Szpitala. Zgodnie z zapisami tego regulaminu, dane z monitoringu przechowywane są nie dłużej niż 30 dni od ich zapisu, a dostęp do danych posiada dwóch pracowników Szpitala. W regulaminie, jako osobę do kontaktu wskazano IOD.

(dowód: akta kontroli str. 398-402)

[21] Pacjenci wchodzili do gabinetu poradni wzywani przez pielęgniarkę, po podaniu nr/godziny wyznaczonej wizyty bez podawania danych osobowych pacjenta.

[22] Poradnia kardiologiczna, gastroenterologiczna, chirurgii ogólnej.

2.2. Według stanu na 04.03.2019 r. personel działów administracyjnych szpitala liczył 45 osób. Analiza uprawnień w systemie AMMS/Infomedica[23], jakie zostały nadane 30 osobom z tej grupy wykazała, że odpowiadały one zakresom zadań i obowiązków realizowanych przez tych pracowników. I tak:

- dziewięć osób nie posiadało dostępu do systemu AMMS/Infomedica, co wynikało z ich zakresów obowiązków (nie realizowali oni zadań wymagających dostępu do danych z ww. systemów),
- sześć osób posiadało nadane im uprawnienia w tym systemie, które pozwalały na dostęp do danych medycznych niezbędnych do wykonywania zadań przypisanych tym pracownikom (byli oni zatrudnieni w Dziale Organizacji i Rozliczeń Świadczeń Medycznych, Dziale Organizacyjno-Prawnym na stanowisku statystyka medycznego oraz w Sekcji Informatyki),
- 15 osób posiadało ograniczony dostęp do danych w systemie AMMS/Infomedica w części administracyjnej (np. tylko do danych statystycznych lub księgowych apteki bądź wyłącznie do informacji o sprzęcie wykorzystywanym w Szpitalu).

(dowód: akta kontroli str. 452-456)

2.3. Analiza przeprowadzona na próbie 30 (z 229) pielęgniarek i położnych zatrudnionych w Szpitalu[24] wykazała, że wszystkie posiadały dostęp w systemie AMMS/Infomedica do danych medycznych pacjentów tylko na oddziałach szpitalnych, na których świadczyły pracę. Wszystkie osoby posiadały w aktach osobowych potwierdzenia nadania im przez ADO pisemnych upoważnień do przetwarzania danych osobowych. Na podstawie prowadzonych rejestrów osób upoważnionych nie stwierdzono przypadków nadania upoważnień do przetwarzania danych osobowych lub uprawnień do AMMS/Infomadica personelowi gospodarczemu i pomocniczemu Szpitala.

(dowód: akta kontroli str. 457-467)

2.4. Od 25.05.2018 r. do 15.03.2019 r. Szpital rozwiązał stosunek pracy ze 105 osobami. Spośród nich, 47 w trakcie zatrudnienia miało przyznany dostęp do systemów informatycznych, w tym do systemu AMMS/Infomedica. Analiza terminu odebrania uprawnień przeprowadzona na próbie 30 osób wykazała, że do 18.03.2019 r. żadnej osobie nie został odebrany dostęp do ww. systemów, co szerzej opisano w dalszej części wystąpienia, w sekcji *Stwierdzone nieprawidłowości*. W przypadku ww. 30 osób nie stwierdzono logowania się do systemu AMMS/Infomedica po dniu rozwiązania stosunku pracy.

(dowód: akta kontroli str. 470-475)

2.5. W umowie serwisowej z 15.04.2018 r. zawartej pomiędzy Szpitalem a RAVEN Sp. z o.o. określono, że usługi serwisowe systemu Infomedica/AMMS będą świadczone w siedzibie zamawiającego lub zdalnie, a zgłoszenia będą dokonywane pod adresem: helpdesk@raven-it.pl lub alternatywnie telefonicznie.
Główny specjalista z Sekcji Informatycznej, wyjaśnił, że w okresie od 25.05.2018 r. do 27.03.2019 r. wszelkich zgłoszeń awarii systemu dokonywał telefonicznie lub osobiście, w kontakcie bezpośrednim z pracownikiem firmy RAVEN, który co tydzień w czwartki jest na terenie Szpitala. W powyższym okresie nie dokonywał żadnych zgłoszeń w formie elektronicznej.

W okresie od 25.05.2018 r. do 27.03.2019 r. nie stwierdzono korespondencji wysyłanej na adres: helpdesk@raven-it.pl.

(dowód: akta kontroli str. 478)

---

23 System typu HIS.

24 Dane wg stanu na 04 marca 2019 r.

2.6. Szpital w okresie objętym kontrolą posiadał 15 umów dotyczących powierzenia przetwarzania danych osobowych, w których wystąpił jako podmiot powierzający przetwarzanie danych (Administrator) oraz 9 umów, gdzie wskazano go jako podmiot przetwarzający (Procesor). Dyrektor Szpitala wyjaśnił, że: *Przesłanką zawierania umów powierzenia była konieczność uregulowania zasad przetwarzania powierzanych przez Szpital innym podmiotom danych osobowych, co było niezbędne do realizacji umowy głównej – zgodnie z art. 28 RODO.*

(dowód: akta kontroli str. 479-483)

Analiza pięciu umów dotyczących powierzenia przez Szpital przetwarzania danych osobowych (dwóch z podmiotami świadczącymi usługi prawne, dwóch – w zakresie usług informatycznych oraz jednej z IOD) wykazała, że zawierały one postanowienia wymagane art. 28 ust. 3 RODO i stanowiły integralną część umowy na świadczenie usług, zawartej z danym podmiotem zewnętrznym.

(dowód: akta kontroli str. 458-533)

W kontrolowanym okresie Szpital nie zawierał umów dotyczących powierzenia przetwarzania danych osobowych. Dyrektor (z up. Z-ca Dyrektora) wyjaśnił, że: *z lekarzem zatrudnionym na podstawie kontraktu nie trzeba zawierać umowy powierzenia przetwarzania danych osobowych. Zgodnie z projektem kodeksu branżowego dla podmiotów medycznych w zakresie ochrony danych osobowych (www.rodowzdrowiu.pl, wersja z 28 maja 2018 r.) w poniższych przypadkach nie jest zasadne podpisywanie umowy powierzenia, ponieważ taki lekarz (lub pielęgniarka) nie jest zobowiązany do samodzielnego prowadzenia dokumentacji - lekarz prowadzi dokumentację w imieniu placówki medyczne*j.

(dowód: akta kontroli str. 565-566)

2.7. Zgodnie z zapisami Rejestru Naruszeń (stanowiącego element określony w § 19 Polityki) w Szpitalu nie wystąpiły przypadki naruszenia zasad ochrony danych osobowych pacjentów.

(dowód: akta kontroli str. 484)

2.8. W zakresie udostępniania dokumentacji medycznej w Szpitalu obowiązywała Procedura Udostępniania Dokumentacji Medycznej Na Zewnątrz SP WZOZ z 01.03.2013 r. Tryb udostępniania dokumentacji został również określony w Regulaminie organizacyjnym z 15.02.2019 r. W 2018 r. do Szpitala wpłynęło 1388 wniosków o udostępnienie dokumentacji medycznej. Dokumentację udostępniono w 1372 przypadkach. Od osób fizycznych wpłynęły 1263 wnioski (w tym 6 od osób innych niż sam pacjent), a 125 wniosków wpłynęło od innych podmiotów (od sądów, prokuratur, ZUS, NFZ, podmioty ubezpieczeniowe, Żandarmerii Wojskowej, Policji i ABW, Państwowego Inspektora Sanitarnego). Od podmiotów ubezpieczeniowych wpłynęło 30 wniosków. Do 06.03.2019 r. do Szpitala wpłynęło 247 wniosków o udostepnienie dokumentacji medycznej. Dokumentację udostępniono w 247 przypadkach. Od osób fizycznych wpłynęły 214 wnioski (w tym 7 od osób innych niż sam pacjent), a 33 wnioski wpłynęły od innych podmiotów. Od podmiotów ubezpieczeniowych wpłynęło 9 wniosków. Szczegółowej analizie poddano 30 spraw w zakresie udostępniania danych instytucjom ubezpieczeniowym oraz wszystkie 13 przypadków udostępnienia dokumentacji innym osobom fizycznym niż pacjent w latach 2018 - 2019 (06.03.). Ponadto analizą objęto 4 (100%) przypadki udostępnienia dokumentacji osób nieletnich. W wyniku analizy stwierdzono, że dokumentacja medyczna została udostępniona osobom, które posiadały upoważnienie pacjenta do dostępu do tej dokumentacji na podstawie wniosków o jej udostępnienie, określonych w regulacjach wewnętrznych Szpitala. We wszystkich 30 przypadkach instytucje ubezpieczeniowe, którym udostępniono dokumentację medyczną, posiadały upoważnienie pacjenta do dostępu do tej dokumentacji.

(dowód: akta kontroli str. 32-33, 436-444, 449-451)

2.9. Regulacje dotyczące ochrony danych przed ich utratą w wyniku awarii, błędów lub nieuprawnionej modyfikacji zostały opisane w IZSI służącym do przetwarzania danych osobowych. W dokumencie tym określono m.in. procedury nadawania uprawnień do przetwarzania danych, stosowane metody i środki uwierzytelniania, procedury rozpoczęcia, zwieszenia i zakończenia pracy przez użytkownika systemu, procedury tworzenia kopii zapasowych i sposobu ich przechowywania, sposoby zabezpieczania systemów informatycznych oraz procedury wykonywania przeglądów technicznych i konserwacji systemów.

(dowód: akta kontroli str. 308-359)

Oględziny jedynej serwerowni Szpitala (przeprowadzone 7.03.2019 r.) wykazały, m.in. że: dostęp do tego pomieszczenia, zabezpieczony był drzwiami przeciwpożarowymi, okna nie posiadały żadnych zabezpieczeń, nie stwierdzono systemu alarmowego/monitoringu dostępu do pomieszczeń; w pomieszczeniu umieszczono gaśnicę oraz zainstalowano układ klimatyzacji; w celu zapobieżenia zalaniu wszystkie urządzenia znajdowały się na tzw. podłodze technicznej, tj. powyżej poziomu posadzki; na wypadek czasowego zaniku zasilania zastosowano układy podtrzymujące napięcie UPS; wszystkie urządzenia informatyczne zamontowano w specjalnie do tego przystosowanych szafach typu RACK. Kopie zapasowe baz danych Szpitala były w tym samym pomieszczeniu, co szerzej opisano w dalszej części wystąpienia, *Stwierdzone nieprawidłowości*.

(dowód: akta kontroli str. 534-539)

Dyrektor wyjaśnił, że *podjęto działania zwiększające bezpieczeństwo serwerowni, w szczególności zamontowano system monitoringu w serwerowni. Poza tym trwają prace nad zamontowaniem żaluzji okiennych i alarmu przeciwpożarowego.*

(dowód: akta kontroli str. 541-542)

W wyniku oględzin zabezpieczeń serwerowni przeprowadzonych 29.03.2019 r., stwierdzono, że dostęp do serwerowni został objęty monitoringiem.

(dowód: akta kontroli str. 544-547)

Oględziny 30 komputerów stacjonarnych Szpitala, w tym 20 wykorzystywanych na oddziałach Szpitala przez lekarzy i pielęgniarki oraz 10 użytkowanych w dziale Administracji Szpitala, wykazały m.in., że: na wszystkich zainstalowany był program antywirusowy, posiadający aktualną wersję bazy sygnatur wirusów, w żadnym z 20 komputerów na oddziałach nie zostały zablokowane porty USB, umożliwiając podłączenie do nich nośników pamięci i kopiowanie danych i wszyscy użytkownicy posiadali pełne uprawnienia w systemie operacyjnym[25], które pozwalały na wprowadzanie zmian w konfiguracji tych urządzeń oraz instalację oprogramowania, 10 komputerów (w Administracji) zarządzanych było domenowo, a 20 funkcjonowało poza tym systemem, każdy z komputerów miał zainstalowany system Infomedica (dostęp ograniczony indywidualnymi uprawnieniami), w 20 komputerach na oddziałach Szpitala dostęp do systemu operacyjnego wymagał podania ogólnego loginu i hasła, z którego korzystali wszyscy pracownicy, a hasła nie posiadały odpowiedniej złożoności i nie podlegały okresowej zmianie, co szerzej opisano w dalszej części wystąpienia, *Stwierdzone nieprawidłowości*.

(dowód: akta kontroli str. 548-560)

W kwestii tworzenia i testowania kopii zapasowych, Dyrektor (z up. Zastępca Dyrektora) wyjaśnił, że *backupy* wykonywane są na poziomie maszyn wirtualnych raz na tydzień, a w przypadku baz danych AMMS codziennie przyrostowo przez podmiot zewnętrzny. *Backup* przechowywany jest na tej samej macierzy co

[25] System operacyjny Windows 7.

maszyny wirtualne i testowany jest automatycznie w wirtualnym laboratorium raz na tydzień.

(dowód: akta kontroli str. 540-543)

Ustalone nieprawidłowości

W działalności kontrolowanej jednostki w przedstawionym wyżej zakresie stwierdzono nieprawidłowości:

1. Do dnia 18 marca 2019 r., żadnej z 30 osób objętych badaniem, z którymi w okresie od 25.05.2018 r. do 09.02.2019 r. Szpital rozwiązał stosunek pracy, nie odebrano uprawnień dostępowych do systemu AMMS/Infomedica. Stanowiło to naruszenie § 20 ust. 2 pkt 5 rozporządzenia KRI, zgodnie z którym należy podejmować działania polegające na bezzwłocznej zmianie uprawnień, w przypadku zmiany zadań osób zaangażowanych w proces przetwarzania informacji. Ponadto zgodnie z § 15 pkt 5 Polityki ADO jest zobowiązany do zabezpieczenia danych przed ich udostępnieniem osobom nieupoważnionym, w tym do niezwłocznego odebrania uprawnień osobom, z którymi rozwiązano stosunek pracy.

(dowód: akta kontroli str. 473-475)

Dyrektor wyjaśnił, że *w dniu 19.03.2019 r. dokonano weryfikacji na podstawie, której osobom z którymi rozwiązano stosunek pracy (…) odebrano uprawnienia dostępowe do systemu HIS. Osobom tym nie odebrano wcześniej uprawnień dostępowych wychodząc błędnie z założenia, że wystarczająca była automatyczna blokada konta po 30 dniach (…).*

(dowód: akta kontroli str. 540-542)

W wyniku oględzin przeprowadzonych 22 marca 2019 r. ustalono, że dostęp do systemu AMMS/Infomedica dla 30 ww. osób został odebrany z dniem 19 marca 2019 r.

(dowód: akta kontroli str. 561-562)

2. Kopie bezpieczeństwa (backup) przechowywane były w tym samym pomieszczeniu, w którym znajdowały się dane produkcyjne podlegające procesowi tworzenia kopii bezpieczeństwa, co było niezgodne z postanowieniami Rozdziału XXIII ust. 4 IZSI z 17.01.2019 r. oraz zaleceniami z audytu przeprowadzonymi przez IOD.

(dowód: akta kontroli str. 543-539)

Dyrektor wyjaśnił, że *w audycie IOD wydała zalecenie w zakresie konieczności zwiększenia bezpieczeństwa kopii bezpieczeństwa. W związku z tym aktualnie trwają prace nad zapewnieniem większego bezpieczeństwa, w tym odrębnej lokalizacji dla kopii danych. Pomimo trudności finansowych Szpitala, w ciągu najbliższego miesiąca nasza jednostka zamierza sfinalizować zakup serwera typu NAS, który umożliwi wykonanie beckupu w dwóch różnych lokalizacjach.*

(dowód: akta kontroli str. 540-542)

3. Lekarze oraz personel medyczny logowali się do systemów operacyjnych przy użyciu jednego identyfikatora oraz hasła - nie posiadali indywidualnych loginów i haseł dostępowych do systemów operacyjnych komputerów Szpitala znajdujących się na poszczególnych oddziałach. Ponadto nadane hasło nie spełniało wymogu złożoności. Stanowiło to naruszenie § 8, § 9 i § 10 IZSI z 17.01.2019 r., w których określono, m.in. że podstawowym mechanizmem uwierzytelniania użytkownika w systemach informatycznych są indywidualne identyfikatory i hasła o odpowiedniej złożoności (min 8 znaków), które są poufne i mogą być wykorzystywane tylko przez jednego użytkownika oraz, że nie dopuszczalne jest funkcjonowanie kilku takich samych nazw użytkowników.
W myśl § 20 ust. 2 pkt 7 lit. a i c oraz § 21 ust. 2 pkt 3 w związku z § 20 ust. 1 rozporządzenia KRI, należy zapewnić środki uniemożliwiające nieautoryzowany dostęp na poziomie systemów operacyjnych, które pozwolą na prawidłową

rozliczalność systemów informatycznych.

(dowód: akta kontroli str. 308-359, 554-560)

Dyrektor wyjaśnił, że *aktualnie trwają prace dostosowawcze do wymogów postanowień § 8 i § 9 IZSI (…) co jest bardzo trudne do zrealizowania z powodu braku środków finansowych. Lekarze oraz personel medyczny logują się jednakowym loginem i hasłem w związku z wymogiem praw administracyjnych oprogramowania Infomedica. (…) Obecnie trwają prace nad przyłączeniem stacji roboczych do domeny, co skutkowało będzie posiadaniem indywidualnego profilu wraz z loginem i hasłem każdego użytkownika.*

(dowód: akta kontroli str. 563-564)

4. W systemach operacyjnych lekarze oraz personel medyczny posiadali pełne uprawnienia, które pozwalały na wprowadzanie zmian w konfiguracji tych urządzeń oraz instalację oprogramowania co było niezgodne z § 7 ust. 2 pkt 2 i § 14 ust. 2 IZSI z 17.01.2019 r., który stanowił, że użytkownicy mają ograniczony dostęp do systemu zgodnie zasadą przywilejów i wiedzy koniecznej. Analogiczne regulacje określone są w § 20 ust. 2 pkt 4 rozporządzenia KRI, zgodnie z którym osoby zaangażowane w proces przetwarzania informacji posiadają stosowne uprawnienia i uczestniczą w tym procesie w stopniu adekwatnym do realizowanych przez nich zadań oraz obowiązków.

(dowód: akta kontroli str. 554-560)

Dyrektor wyjaśnił, że *głównym warunkiem poprawnego działania programu informatycznego Infomedica jest posiadanie przez profil użytkownika pełnych uprawnień administratora.*

(dowód: akta kontroli str. 563-564)

OCENA CZĄSTKOWA

Szpital wprowadził rozwiązania organizacyjne zmierzające do zapewnienia ochrony danych osobowych pacjentów oraz poszanowania ich prywatności. Nie były one jednak w pełni przestrzegane. Personelowi szpitala zapewniono odpowiedni dostęp do danych medycznych, jednak stwierdzono, że posiadał on również uprawnienia administratora systemu operacyjnego komputerów, które użytkował. Stwierdzono również niewłaściwe zabezpieczenie systemu operacyjnego, z uwagi na stosowanie jednego hasła i loginu dla wszystkich użytkowników. W okresie od 25 maja 2018 r. do 15 marca 2019 r. nie odbierano uprawnień dostępowych do systemów informatycznych Szpitala byłym pracownikom, z którymi Szpital rozwiązał stosunek pracy. Uprawnienia te zostały odebrane w trakcie kontroli 19 marca 2019 r. Ponadto stwierdzono, że kopie bezpieczeństwa były przechowywane w tym samym pomieszczeniu, w którym znajdowały się dane produkcyjne poddawane procesowi tworzenia tych kopii. Powyższe działania były niezgodne z zasadami określonymi przepisami art. 5 pkt 1 lit. c RODO oraz § 20 ust. 2 pkt 4 i 5 rozporządzenia KRI. Stanowiły także naruszenie przyjętych w Szpitalu regulacji wewnętrznych wyrażonych IZSI służącym do przetwarzania danych osobowych w Szpitalu.

IV. Uwagi i wnioski

Wnioski

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

1. Wdrożenie odpowiednich środków technicznych i organizacyjnych zapewniających minimalizację ryzyka utraty danych osobowych poprzez przechowywanie kopii bezpieczeństwa w odrębnym pomieszczeniu od pomieszczenia, w którym znajdują się dane produkcyjne poddawane procesowi tworzenia tych kopii.
2. Nadawanie uprawnień administratora systemów operacyjnych jedynie osobom do tego upoważnionym.

3. Bezzwłoczne odbieranie uprawnień w systemach informatycznych pracownikom, z którymi rozwiązano stosunek pracy.
4. Nadanie wszystkim użytkownikom komputerów indywidualnych danych do autoryzacji w systemach operacyjnych oraz wprowadzenie rozwiązań uniemożliwiających pracę kilku osób na jednym koncie użytkownika.

Najwyższa Izba Kontroli nie formułuje uwag.

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

Obowiązek poinformowania NIK o sposobie wykonania wniosków

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

Szczecin, 11 kwietnia 2019 r.

Kontroler

Jarosław Pułka

Główny specjalista k.p

Najwyższa Izba Kontroli

Delegatura w Szczecinie

p.o. Dyrektora