NAJWYŻSZA IZBA KONTROLI

Delegatura w Olsztynie

LOL.411.5.6.2023

Andrzej Bujnowski
Prezes Zarządu
Giżycka Ochrona Zdrowia Sp. z o.o.
ul. Warszawska 41
11-500 Giżycko

WYSTĄPIENIE POKONTROLNE

I/23/003 – Ochrona danych pacjentów przed cyberatakami w podmiotach leczniczych na terenie województwa warmińsko-mazurskiego

NAJWYŻSZA IZBA KONTROLI
Delegatura w Olsztynie
ul. Artyleryjska 3e, 10-165 Olsztyn
T +48 89 678 82 00, F +48 89 678 82 30
lol@nik.gov.pl

I. Dane identyfikacyjne

Jednostka kontrolowana

Giżycka Ochrona Zdrowia Spółka z o.o., ul. Warszawska 41, 11-500 Giżycko, dalej: Spółka lub Szpital.

Kierownik jednostki kontrolowanej

Andrzej Bujnowski, Prezes Zarządu, od 1 października 2021 r.

W okresie objętym kontrolą funkcję kierownika jednostki poprzednio pełniła Anita Karnacewicz, Prezes Zarządu, od 28 listopada 2019 r. do 30 września 2021 r.

Zakres przedmiotowy kontroli

1. Działania związane z przygotowaniem technicznym i organizacyjnym dotyczącym przetwarzania i ochrony danych pacjentów przed cyberatakami.
2. Funkcjonowanie przyjętych rozwiązań i ich wpływ na ochronę danych pacjentów przed cyberatakami.

Okres objęty kontrolą

Lata 2020-2023 (I półrocze), z uwzględnieniem okresów wcześniejszych i późniejszych, jeżeli miało to wpływ na realizowane zadania.

Podstawa prawna podjęcia kontroli

Art. 2 ust. 2 ustawy z dnia 23 grudnia 1994 r. o Najwyższej Izbie Kontroli[1].

Jednostka przeprowadzająca kontrolę

Najwyższa Izba Kontroli
Delegatura w Olsztynie

Kontrolerzy

1. Krzysztof Śleszyński, doradca ekonomiczny, upoważnienie do kontroli nr LOL/161/2023 z 30 listopada 2023 r.
2. Justyna Lis, starszy inspektor kontroli państwowej, upoważnienie do kontroli nr LOL/158/2023 z 28 listopada 2023 r.

(akta kontroli str. 1-5)

II. Ocena ogólna[2] kontrolowanej działalności

OCENA OGÓLNA

W Szpitalu podjęto działania na rzecz zapewnienia bezpieczeństwa informacji, w tym danych pacjentów. Jednakże nie zostały stworzone odpowiednie rozwiązania organizacyjne i techniczne w tym zakresie, które byłyby zgodne z wymaganiami określonymi w rozporządzeniu 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[3]. Ponadto, samo przetwarzanie danych pacjentów w Szpitalu odbywało się bez stosowania w prawidłowy sposób niektórych zasad w ramach podjętych działań na rzecz zapewnienia bezpieczeństwa.

W Spółce, wbrew przepisom rozporządzenia KRI, nie opracowano, nie ustanowiono i nie wdrożono Systemu Zarządzania Bezpieczeństwem Informacji[4]. Spowodowało to

[1] Dz. U. z 2022 r. poz. 623, dalej: ustawa o NIK.

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

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

[4] Dalej: SZBI.

m.in. nieterminowe wywiązanie się przez Spółkę (jako Operatora Usługi Kluczowej[5]) z obowiązków wynikających z ustawy z dnia 5 lipca 2018 r. o krajowym systemie cyberbezpieczeństwa[6]. Podjęte działania dotyczące bezpieczeństwa informacji obejmowały m.in. ustanowioną Politykę bezpieczeństwa informacji. Wprawdzie pracownicy Szpitala zostali przeszkoleni w zakresie bezpieczeństwa informacji, w tym ochrony danych osobowych, lecz w niewłaściwy sposób dokumentowano ten fakt. Nieterminowo zamieszczono na stronie internetowej Szpitala informacje o zagrożeniach cyberbezpieczeństwa i o stosowaniu skutecznych sposobów zabezpieczania się przed nimi. Nierzetelnie realizowano obowiązek w zakresie odbierania byłym pracownikom Szpitala uprawnień dostępu do systemu Medicus On Line, zaś przy nadawaniu uprawnień nie dochowano należytej staranności w ich dokumentowaniu. W przypadku niektórych rozwiązań sprzętowych i systemowych były one realizowane niezgodnie z obowiązującą w Spółce polityką.

We właściwy sposób wyznaczono Inspektora Ochrony Danych[7] ustalając mu obowiązki zgodne z rozporządzeniem Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE[8], a posiadane przez niego kwalifikacje były odpowiednie do pełnienia tej funkcji. Pracownicy Szpitala, zgodnie z obowiązującymi wymaganiami, posiadali upoważnienia do przetwarzania danych osobowych, a zakres tych upoważnień był zgodny z obowiązkami i zadaniami tych pracowników. Również dostęp do systemów informatycznych Szpitala ustanowiony był odpowiednio do miejsca i zakresu wykonywanych czynności. Ponadto prawidłowo zareagowano na incydent zagrażający bezpieczeństwu systemu informatycznemu jaki miał miejsce w okresie objętym kontrolą, a umowy powierzenia danych osobowych pacjentów były zawierane prawidłowo.

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

OBSZAR

1. Działania związane z przygotowaniem technicznym i organizacyjnym dotyczącym przetwarzania i ochrony danych pacjentów przed cyberatakami

Opis stanu faktycznego

1.1. Spółka, w której 100% udziałów posiadała Gmina Miejska Giżycko, została zarejestrowana w Krajowym Rejestrze Sądowym 9 stycznia 2020 r.[10] Wpis do Rejestru Podmiotów Wykonujących Działalność Leczniczą[11] prowadzonego przez Wojewodę Warmińsko-Mazurskiego Szpital uzyskał 20 lutego 2020 r., a działalność leczniczą rozpoczął 1 lipca 2020 r. Wcześniej, tj. od 31 grudnia 1992 r. do 30 czerwca 2020 r., działalność leczniczą w siedzibie Szpitala prowadziły spółki: Szpital Giżycki Sp. z o.o., a następnie Szpital Giżycki Sp. z o.o. w upadłości, których udziałowcem był Powiat Giżycki (100%).

(akta kontroli str. 7-24)

[5] Dalej: OUK.

[6] Dz.U. z 2023 r. poz. 913, ze zm. dalej: ustawa o cyberbezpieczeństwie.

[7] Dalej: IOD.

[8] Dz. Urz. UE L 119 z 4 maja 2016 r., str. 1, dalej: rozporządzenie RODO.

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

[10] KRS nr 0000822215.

[11] W księdze rejestrowej nr 000000226702.

1.2. W okresie objętym kontrolą w Szpitalu funkcjonowały procedury, będące elementami Polityki bezpieczeństwa informacji[12], tj.:

- „Polityka ochrony danych w Spółce"[13] wraz z załącznikami, w tym załącznikiem nr 6 „Instrukcja zarządzania systemem informatycznym w Spółce"[14],
- „Uzupełnienie do Polityki ochrony danych w Spółce"[15],
- „Szacowanie ryzyka zgodnie z RODO[16] w Spółce"[17],
- „Rejestr naruszeń ochrony danych osobowych w Spółce"[18],
- „Zasady obsługi i korzystania z monitoringu wizyjnego w Spółce"[19],
- „Procedura wydawania i zdawania kluczy w Spółce"[20],
- „Plan ciągłości działania Spółki"[21],
- „Plan ciągłości działania systemów informatycznych w Spółce"[22],
- „Zasady pracy zdalnej"[23].

(akta kontroli str. 25-191, 441-482)

W okresie od 1 lipca 2020 r.[24] do 31 grudnia 2023 r. nie opracowano i w konsekwencji nie wdrożono SZBI, o którym mowa w § 20 ust. 1 rozporządzenia KRI. Zgodnie z ww. przepisem jednostki realizujące zadania publiczne mają obowiązek opracowania i ustanowienia, wdrożenia i eksploatacji, monitorowania i przeglądania oraz utrzymania i doskonalenia SZBI zapewniającego poufność, dostępność i integralność informacji z uwzględnieniem takich atrybutów, jak autentyczność, rozliczalność, niezaprzeczalność i niezawodność. Wymagania dotyczące opracowania SZBI uznaje się za spełnione, jeżeli został opracowany na podstawie Polskiej Normy PN-ISO/IEC 27001 (§ 20 ust. 3 ww. rozporządzenia), a ustanawianie zabezpieczeń, zarządzanie ryzykiem oraz audytowanie odbywa się na podstawie Polskich Norm związanych z tą normą, w tym: PN-ISO/IEC 27002 – w odniesieniu do ustanawiania zabezpieczeń, PN-ISO/IEC 27005 - w odniesieniu do zarządzania ryzykiem, PN-ISO/IEC 24762 - w odniesieniu do odtwarzania techniki informatycznej po katastrofie w ramach zarządzania ciągłością działania.

Ustanowiona przez Spółkę Polityka ochrony danych miała na celu ochronę danych osobowych, a nie wszystkich informacji przetwarzanych w Szpitalu. Mimo, iż we wstępie do ww. polityki wskazano, iż została ona opracowana w oparciu o wytyczne zawarte m.in. w rozporządzeniu KRI, to nie stanowi ona SZBI w rozumieniu tego rozporządzenia. Umieszczenie tych zasad bezpieczeństwa informacyjnego w dokumencie dedykowanym ochronie danych osobowych, zawęża zakres ich stosowania do danych osobowych i systemów informatycznych przetwarzających dane osobowe.

Prezes stwierdził, że w ramach SZBI, jak i polityki bezpieczeństwa informacji, Szpital opracowuje, ustanawia, wdraża i eksploatuje, monitoruje i przegląda oraz utrzymuje

---

[12] Dalej: PBI.

[13] Dalej: Polityka ochrony danych; dokument z 30 listopada 2020 r.

[14] Dalej: Instrukcja zarządzania systemem informatycznym; dokument z 30 listopada 2020 r.

[15] Dalej: Uzupełnienie do polityki ochrony danych; dokument z 30 listopada 2020 r.

[16] RODO – rozporządzenie Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (ogólne rozporządzenie o ochronie danych) (Dz. Urz. UE L 119 z 4 maja 2016 r., str. 1).

[17] Dalej: Szacowanie ryzyka; dokument z 30 listopada 2020 r.

[18] Dalej: Rejestr naruszeń ochrony danych osobowych; dokument z 30 listopada 2020 r.

[19] Dalej: Zasady monitoringu wizyjnego; dokument z 25 sierpnia 2023 r.

[20] Dalej: Polityka kluczy; dokument z 30 listopada 2020 r.

[21] Dalej: Plan ciągłości działania; dokument z 6 listopada 2023 r.

[22] Dalej: Plan ciągłości działania systemów informatycznych; dokument z 6 listopada 2023 r.

[23] Dalej: Zasady pracy zdalnej; dokument z 20 czerwca 2023 r.

[24] Rozpoczęcie działalności leczniczej przez Giżycką Ochronę Zdrowia Sp. z o.o.

i doskonali szereg procedur, regulaminów, zasad i polityk dotyczących bezpieczeństwa informacji, w tym danych osobowych. Podał także, że obecnie Szpital jest na etapie opracowywania aktualnej, szeroko rozumianej Polityki bezpieczeństwa informacji z wykorzystaniem Polskiej Normy PN-ISO/IEC 27001.

W odpowiedziach Prezesa Zarządu na pytania kontrolera NIK o przyczyny nieopracowania, nieustanowienia i niewdrożenia SZBI w zakresie o jakim mowa w § 20 rozporządzenia KRI oraz przyczyny nieopracowania obowiązującej w Szpitalu Polityki ochrony danych na podstawie Polskiej Normy PN-ISO/IEC 27 0001 nie podano wyjaśnień w tym zakresie.

Inspektor ochrony danych w Spółce[25] podał, że w Szpitalu funkcjonuje system zarządzania bezpieczeństwem informacji i praktycznie wszystkie wytyczne art. 20 ust. 2 rozporządzenia KRI są realizowane. Stwierdził także, że nie wie, czy i na podstawie jakich norm była opracowana dokumentacja z zakresu ochrony danych osobowych przez byłego IOD. Podał, że aktualna PBI jest opracowywana w oparciu o ww. normy, a prace w tym zakresie powinny się zakończyć do końca marca 2024 r.

(akta kontroli str.25-191, 410-421,437-440, 483-485)

1.3. Spółka określiła i przypisała odpowiedzialność za bezpieczeństwo informacji w zakresie ochrony danych osobowych w Polityce ochrony danych. W dokumencie wskazano, że za przetwarzanie danych osobowych oraz ich ochronę zgodnie z przepisami odpowiadają: Administrator Danych Osobowych[26], IOD, Lokalny Administrator Systemów Informatycznych[27] oraz osoby upoważnione do przetwarzania danych osobowych. Poszczególnym wyżej wskazanym osobom przypisano zadania i odpowiedzialności. Wskazano m.in., że ADO odpowiada za zapewnienie odpowiednich środków organizacyjnych i technicznych w celu zapewnienia i wykazania przetwarzania danych osobowych zgodnie z RODO, wdrożenie odpowiednich procedur ochrony danych osobowych, dokumentowanie wszelkich naruszeń ochrony danych osobowych oraz raportowanie takich naruszeń organowi nadzorczemu, nadawanie upoważnień do przetwarzania danych osobowych oraz prowadzenie ewidencji osób upoważnionych do przetwarzania danych osobowych. W ww. polityce wskazano, że ADO wyznacza ASI. Do zadań ASI należało m.in.: organizowanie i techniczne utrzymanie w sprawności systemów i sprzętu łączności i informatyki zgodnie z obowiązującymi zasadami i standardami, kontrola poprawności wykorzystania przydzielonych środków łączności i informatyki oraz bieżące szkolenie i instruowanie użytkowników o sposobie ich wykorzystania, administracja sieciami (Internet, system, strona internetowa), nadzór i administracja systemami informatycznymi, zgłaszanie zagrożeń oraz ocena ryzyka, na które może być narażone przetwarzanie danych osobowych w systemach informatycznych, nadawanie uprawnień do pracy w systemach na wniosek kierownika kadr lub IOD i po zatwierdzeniu wniosku przez Prezesa Zarządu.

W latach 2000-2023[28] ADO wyznaczył osobę spoza pracowników Szpitala do pełnienia funkcji ASI. Szpital zawarł z tą osobą umowy na świadczenie kompleksowej usługi wsparcia informatycznego, określonej jako Help desk[29]. W umowach tych zobowiązano wykonawcę usługi do zarządzania i ochrony całego systemu informatycznego zgodnie z zapisami Polityki bezpieczeństwa informacji i Instrukcji zarządzania systemem informatycznym, funkcjonującymi w Szpitalu.

[25] Na stanowisku od 7 sierpnia 2022 r.

[26] Dalej: ADO.

[27] Dalej: ASI.

[28] Do 31 grudnia.

[29] Umowa nr n/02/01/20 z 28 stycznia 2020 r., umowa nr n/02/01/21 z 3 lutego 2021 r., umowa nr n/02/01/22 z 2 lutego 2022 r., umowa nr n/01/01/23 z 1 lutego 2023 r.

W wyżej wymienionym okresie w Szpitalu zatrudniony był także Starszy informatyk[30], do którego zadań (zgodnie z zakresem obowiązków służbowych, uprawnień i odpowiedzialności z 10 grudnia 2019 r.) należało m.in.: przegląd i konserwacja sprzętu komputerowego w komórkach organizacyjnych Szpitala, usuwanie awarii sprzętu komputerowego, wdrażanie nowych zakresów informatyzacji w Szpitalu, wstępne i bieżące szkolenia pracowników, co do zasad użytkowania sprzętu komputerowego i stosowanego oprogramowania, dbanie o poprawność funkcjonowania sieci strukturalnej, administrowanie, aktualizowanie oraz dostosowywanie systemu medycznego w Szpitalu.

(akta kontroli str. 26-84, 192-242, 410-421)

W okresie objętym kontrolą w Szpitalu wyznaczono IOD, tj.:

- od 6 sierpnia 2020 r. do 6 sierpnia 2022 r. zadania te wykonywał pan M.C., na podstawie zawartej ze Szpitalem umowy na świadczenie usług z 6 sierpnia 2020 r.,
- od 7 sierpnia 2022 r. do 7 sierpnia 2024 r. obowiązki te powierzono panu P.G, na podstawie umowy na świadczenie usług z 11 sierpnia 2022 r.

Kwalifikacje osób wyznaczonych w Spółce na stanowisko IOD spełniały wymagania określone w art. 37 ust. 5 RODO, tj. posiadały odpowiednie przygotowanie zawodowe, a w szczególności wiedzę fachową na temat prawa i praktyk w dziedzinie ochrony danych osobowych oraz umiejętności wypełnienia zadań, o których mowa w art. 39 RODO. Wskazane w ww. umowach na świadczenie usług zadania IOD wpisywały się w katalog czynności określonych w art. 39 RODO oraz były zgodne z zadaniami jakie wskazano dla IOD w Polityce ochrony danych.

(akta kontroli str. 26-71, 243-259, 410-421)

Personel medyczny oraz pracownicy zostali zobowiązani w Polityce ochrony danych m.in. do: współdziałania z IOD w zakresie przestrzegania zasad przetwarzania i ochrony danych w Szpitalu, jak również identyfikacji i analizy ryzyka i niezwłocznego poinformowania IOD o każdym stwierdzeniu lub podejrzeniu naruszenia bezpieczeństwa danych osobowych lub systemu informatycznego, w którym są przetwarzane dane osobowe oraz do współdziałania przy usuwaniu skutków takiego naruszenia.

(akta kontroli str. 26-71)

1.4. W dniu 4 lipca 2022 r. Szpital został uznany za operatora usługi kluczowej[31] w sektorze ochrony zdrowia[32], w myśl art. 5 ust. 2, art. 41 pkt 5 oraz art. 42 ust. 1 pkt 2 ustawy o cyberbezpieczeństwie.

Szpital w terminach określonych ww. ustawą wywiązał się lub częściowo wywiązał się z następujących obowiązków będących następstwem decyzji Ministra Zdrowia o uznaniu Spółki za OUK:

- wyznaczył osobę odpowiedzialną za utrzymywanie kontaktów z podmiotami krajowego systemu cyberbezpieczeństwa[33],
- co do zasady częściowo wdrożył środki techniczne i organizacyjne mające zapewnić: utrzymanie i bezpieczną eksploatację systemu informacyjnego,

[30] Od 10 grudnia 2019 r.

[31] Podmiot o istotnym znaczeniu dla utrzymania krytycznej działalności społecznej lub gospodarczej, wchodzący w skład krajowego systemu cyberbezpieczeństwa mającego na celu zapewnienie cyberbezpieczeństwa na poziomie krajowym, w tym niezakłóconego świadczenia usług kluczowych i usług cyfrowych, przez osiągnięcie odpowiedniego poziomu bezpieczeństwa systemów informacyjnych służących do świadczenia tych usług oraz zapewnienie obsługi incydentów.

[32] Decyzja Ministra Zdrowia nr DIWP.550.77.2022.MP z 4 lipca 2022 r.

[33] Zgłoszenie z 7 września 2022 r.

bezpieczeństwo fizyczne i środowiskowe, uwzględniające kontrolę dostępu, bezpieczeństwo i ciągłość dostaw usług, od których zależy świadczenie usługi kluczowej, objęcie systemu informacyjnego wykorzystywanego do świadczenia usługi kluczowej systemem monitorowania w trybie ciągłym[34], ponieważ posiadał uregulowania w tym zakresie dla danych osobowych, określone w obowiązującej w Spółce Polityce ochrony danych;

- zapewnił zbieranie informacji o zagrożeniach cyberbezpieczeństwa i podatnościach na incydenty systemu informacyjnego wykorzystywanego do świadczenia usługi kluczowej[35],
- co do zasady częściowo zapewnił procedury zapobiegające i ograniczające wpływ incydentów na bezpieczeństwo systemu informacyjnego wykorzystywanego do świadczenia usługi kluczowej, w tym: stosowanie mechanizmów zapewniających poufność, integralność, dostępność i autentyczność danych przetwarzanych w systemie informacyjnym, dbałość o aktualizację oprogramowania, ochronę przed nieuprawnioną modyfikacją w systemie informacyjnym[36], ponieważ posiadał uregulowania w tym zakresie dla danych osobowych, określone w obowiązującej w Spółce Polityce ochrony danych.

(akta kontroli str. 26-84, 260-276)

1.5. W dniu uzyskania przez Spółkę decyzji o uznaniu jej za OUK w Szpitalu funkcjonowały wewnętrzne struktury odpowiedzialne za cyberbezpieczeństwo, co opisano w punkcie 1.3.

Z informacji przedstawionych przez Spółkę wynikało, że struktury te spełniały wymagania art. 14 ustawy o cyberbezpieczeństwie, tj.:

- spełniały warunki organizacyjne i techniczne pozwalające na zapewnienie cyberbezpieczeństwa obsługiwanemu OUK,
- dysponowały pomieszczeniami służącymi do świadczenia usług w zakresu reagowania na incydenty, zabezpieczonymi przed zagrożeniami fizycznymi i środowiskowymi,
- stosowały zabezpieczenia w celu zapewnienia poufności, integralności, dostępności i autentyczności przetwarzanych informacji, z uwzględnieniem bezpieczeństwa osobowego, eksploatacji i architektury systemów.

Natomiast audyt bezpieczeństwa systemu informacyjnego wykorzystywanego do świadczenia usługi kluczowej z dnia 6 lutego 2024 r.[37], wykazał niedostosowanie pomieszczeń zespołu odpowiedzialnego za realizację zadań w zakresie cyberbezpieczeństwa w Szpitalu z wymaganiami wynikającymi z ustawy o cyberbezpieczeństwie.

W latach 2020-2023[38] koszty Spółki dotyczące utworzenia i funkcjonowania ww. struktury wyniosły ok. 960 tys. zł.

(akta kontroli str.192-257, 410-421, 437-440, 890-958)

[34] 30 listopada 2020 r. w Spółce przyjęto Politykę ochrony danych, w tym m.in. Instrukcję zarządzania systemem informatycznym, w której ujęto szereg zasad zarządzania bezpieczeństwem w systemie informacyjnym Szpitala. Ponadto Szpital w 2022 r. i w 2023 r. zakupił w ramach wsparcia otrzymanego z Narodowego Funduszu Zdrowia systemy do zarządzania bezpieczeństwem w systemie informacyjnym Szpitala, tj.: system SOC, system EDR, biblioteka taśmowa, system backupowy, system SIEM, system ochrony poczty.

[35] Monitorowanie zasobów sieciowych i systemów informatycznych poprzez wdrożenie w 2022 r. usługi Security Operation Center (SOC) oraz w 2023 r. usługi SIEM.

[36] Zasady ujęte od 30 listopada 2020 r. w Instrukcji zarządzania systemem informatycznym.

[37] „Sprawozdanie z analizy proceduralnej cyberbezpieczeństwa na podstawie wymagań ustawy o Krajowym Systemie Cyberbezpieczeństwa, Giżycka Ochrona Zdrowia Sp z o.o. w Giżycku", MedFormatica Sp. z o.o.

[38] Do 31 grudnia 2023 r.

1.6. Do 31 grudnia 2023 r. Szpital, jako OUK, nie wdrożył w terminie wyznaczonym ustawą o cyberbezpieczeństwie systemu zarządzania bezpieczeństwem w systemie informacyjnym, wykorzystywanym do świadczenia usługi kluczowej, zapewniającego: prowadzenie systematycznego szacowania ryzyka wystąpienia incydentu i zarządzania tym ryzykiem oraz zarządzanie incydentami, pomimo że termin na wdrożenie tego systemu upłynął 4 października 2022 r. Zgodnie bowiem z art. 8 pkt 1 oraz pkt 4 ww. ustawy, w związku z art. 16 pkt 1, OUK wdraża ww. system zapewniający zarzadzania ryzykiem i zarządzania incydentami w terminie trzech miesięcy od dnia doręczenia decyzji o uznaniu go za OUK.

Polityka ochrony danych wprowadziła wzór formularza szacowania ryzyka. Na tej podstawie IOD 30 listopada 2020 r. dokonał szacowania ryzyka w Szpitalu (dokument - Szacowanie ryzyka) w zakresie naruszenia praw lub wolności osób fizycznych, na podstawie rozporządzenia ws. RODO. Od 30 listopada 2020 r. do końca 2023 r. nie dokonano ponownego szacowania ryzyka.

Ustawa o cyberbezpieczeństwie określała natomiast ryzyko jako kombinację prawdopodobieństwa wystąpienia zdarzenia niepożądanego i jego konsekwencji (nie tylko w zakresie danych osobowych), a szacowanie ryzyka jako całościowy proces identyfikacji, analizy i oceny ryzyka. Ustawodawca wskazał, że incydent to zdarzenie, które ma lub może mieć niekorzystny wpływ na cyberbezpieczeństwo, a zarządzanie ryzykiem jako skoordynowane działania w zakresie zarządzania cyberbezpieczeństwem w odniesieniu do oszacowanego ryzyka.

W Szpitalu nie określono procedury zarządzania incydentami w rozumieniu przepisów ww. ustawy. W Polityce ochrony danych (załącznik nr 8) określono jedynie procedurę postępowania w przypadku naruszenia ochrony danych osobowych.

Prezes stwierdził, że w Szpitalu funkcjonuje procedura postępowania w przypadku naruszenia danych osobowych uwzględniająca reakcje na wszelkie incydenty związane z bezpieczeństwem informacji. Podał także, że obecnie Szpital opracowuje aktualną instrukcję zarządzania incydentami związanymi z bezpieczeństwem informacji, która będzie załącznikiem do Polityki bezpieczeństwa informacji.

Ponadto IOD podał, że w jego ocenie obecne dokumenty Szpitala dotyczące szacowania ryzyka nie odnoszą się jedynie do zagrożeń dla ochrony danych osobowych. Dodał także, że jest przygotowywana aktualna PBI, obejmująca politykę zarządzania ryzykiem w oparciu o normę PN-ISO/IEC-27005.

(akta kontroli str. 25, 136-141, 155-168, 273-276, 410-421, 437-440, 484-485)

1.7. Do końca 2023 r. Szpital (jako OUK) nie wywiązał się z obowiązku aktualizacji w terminie określonym w ustawie o cyberbezpieczeństwie, tj. do 4 stycznia 2023 r. dokumentacji dotyczącej cyberbezpieczeństwa systemu informacyjnego wykorzystywanego do świadczenia usługi kluczowej. Zgodnie bowiem z art. 10 ust. 1 ww. ustawy, w związku z art. 16 pkt 2, OUK opracowuje, stosuje i aktualizuje dokumentację dotyczącą cyberbezpieczeństwa systemu informacyjnego wykorzystywanego do świadczenia usługi kluczowej w terminie sześciu miesięcy od dnia doręczenia decyzji o uznaniu za OUK.

Prezes Zarządu podał, że Szpital jest obecnie na etapie aktualizacji SZBI.

(akta kontroli str.273-276, 410-421)

1.8. Szpital nie przeprowadził do końca 2023 r. audytu bezpieczeństwa systemu informacyjnego wykorzystywanego do świadczenia usługi kluczowej, naruszając tym samym art. 15 ust. 1, w związku z art. 16 pkt 3 ustawy o cyberbezpieczeństwie. W myśl tych przepisów był bowiem zobowiązany w terminie roku od dnia doręczenia

decyzji o uznaniu za operatora usługi kluczowej, tj. do dnia 4 lipca 2023 r., do wykonania takiego audytu.

Prezes Zarządu podał, że wewnętrzny audyt bezpieczeństwa systemu informacyjnego wykorzystywanego do świadczenia usługi kluczowej, tj. systemu Medicus On-Line[39], przeprowadził IOD w dniu 18 lipca 2023 r. Kompleksowy audyt informatyczny jest zaplanowany i zostanie wykonany do 31 stycznia 2024 r.

Zdaniem jednak Najwyższej Izby Kontroli audyt wewnętrzy systemu Medicus dotyczył tylko jednego z systemów informacyjnych funkcjonujących w Spółce, będącej OUK.

W trakcie trwania czynności kontrolnych NIK Spółka, w dniu 5 stycznia 2024 r., podpisała umowę nr n/02/01/24 na wykonanie audytu zgodności z ustawą o cyberbezpieczeństwie dla operatorów usługi kluczowej. Termin realizacji umowy, w tym sporządzenie raportu z audytu, określono na 31 stycznia 2024 r. Wykonawca przedstawił 6 lutego 2024 r. sprawozdanie z audytu[40], w którym zidentyfikował w ramach 132 badanych zagadnień[41]: 18 o priorytecie wysokim, 71 o średnim i jedno o niskim, niezgodnych lub częściowo niezgodnych z wymogami cyberbezpieczeństwa. Całkowity koszt przeprowadzenia audytu wyniósł 15 tys. zł.

(akta kontroli str. 273-284, 410-421, 512-523, 890-958)

1.9. Wg stanu na 7 grudnia 2023 r. na stronie internetowej Szpitala (https://zozgiz.pl/ oraz https://bip.zozgiz.pl/) nie zamieszczono informacji zapewniającej użytkownikowi usługi kluczowej dostępu do wiedzy pozwalającej na zrozumienie zagrożeń cyberbezpieczeństwa i stosowanie skutecznych sposobów zabezpieczania się przed tymi zagrożeniami w zakresie związanym ze świadczoną usługą kluczową. Zgodnie natomiast z art. 9 ust. 1 pkt 2 ustawy o cyberbezpieczeństwie oraz w związku z art. 16 pkt 1 tej ustawy, OUK powinien zapewnić taką wiedzę użytkownikom, w szczególności przez publikowanie informacji na ten temat na swojej stronie internetowej do 4 października 2022 r, tj. w terminie trzech miesięcy od dnia doręczenia decyzji o uznaniu Spółki za OUK.

Starszy informatyk Szpitala oświadczył, że pacjenci mają możliwość i są zobowiązani do zapoznania się z polityką prywatności zamieszczoną na https://zozgiz.pl/polityka-prywatnosci/ oraz polityką cookies, zamieszoną na https://zozgiz.pl/ciasteczka-internetowe/.

Ponadto Prezes Zarządu podał, że Szpital zapewnił pacjentom dostęp do wiedzy z zakresu cyberbezpieczeństwa potwierdzając to, co oświadczył Starszy informatyk oraz wskazując dodatkowo jako źródło tej wiedzy regulamin portalu e-usługi (zamieszczony na https://euslugi.zozgiz.pl/1/auth/login).

NIK zwraca jednak uwagę, że polityka prywatności, zamieszczona na stronie internetowej Szpitala, zawierała dane wymagane rozporządzeniem RODO, tj.: informacje o ADO i IOD, cel i okres przetwarzania danych osobowych, zasady udostępniania i przetwarzania danych osobowych. Polityka cookies określała natomiast zasady przechowywania i dostępu do informacji na urządzeniach użytkownika strony za pomocą plików cookies, służących realizacji usług świadczonych drogą elektroniczną żądanych przez użytkownika. W polityce tej wskazano m.in., że administrator wykorzystuje cookies własne w celu: poprawnej

[39] Dalej: system Medicus.

[40] „Sprawozdanie z analizy proceduralnej cyberbezpieczeństwa na podstawie wymagań ustawy o Krajowym Systemie Cyberbezpieczeństwa, Giżycka Ochrona Zdrowia Sp. z o.o."

[41] Przeprowadzona analiza dotyczyła weryfikacji zgodności formalnej w obszarze systemu zarządzania bezpieczeństwem informacji dla dwóch usług kluczowych: udzielanie świadczeń opieki zdrowotnej przez podmiot leczniczy oraz obrót i dystrybucja produktów leczniczych.

konfiguracji serwisu, realizacji procesów niezbędnych dla pełnej funkcjonalności stron internetowych, dostosowania zawartości stron internetowych serwisu do preferencji użytkownika oraz optymalizacji korzystania ze stron internetowych serwisu, analiz i badań oraz audytu oglądalności. Natomiast regulamin portalu e-usługi zawierał zasady korzystania z elektronicznej rezerwacji wizyt w Szpitalu, w tym m.in.: zasady wygenerowania loginu i tworzenia hasła do konta na portalu, zadania administratora i obowiązki użytkownika portalu, informację o ochronie i przetwarzaniu danych osobowych na portalu.

Zdaniem NIK powyższe informacje, które Szpital zamieścił na swojej stronie internetowej, nie obejmowały swym zakresem wiedzy pozwalającej użytkownikowi usługi kluczowej na zrozumienie zagrożeń cyberbezpieczeństwa i stosowanie skutecznych sposobów zabezpieczania się przed tymi zagrożeniami w zakresie związanym ze świadczoną usługą kluczową.

W trakcie kontroli NIK, Spółka zamieściła[42] na stronie internetowej Szpitala (www.zozgiz.pl w zakładce „dla pacjenta") informację związaną z ochroną danych i bezpieczeństwem w sieci.

(akta kontroli str. 285-308, 410-421)

1.10. Z dokumentów przedłożonych w trakcie kontroli wynikało, że Spółka nie prowadziła harmonogramów szkoleń oraz nie posiadała informacji o liczbie pracowników przeszkolonych w zakresie ochrony danych osobowych i bezpieczeństwa informacji w okresie 2020-2023[43].

Prezes Zarządu wyjaśnił, że Szpital zapewnił swojemu personelowi szkolenie związane z wejściem w życie przepisów RODO w 2021 r. na spotkaniach grupowych zorganizowanych przez IOD. Listy obecności ze szkoleń wewnętrznych Spółki w większości nie były prowadzone. Dodał także, że Szpital posiada natomiast oświadczenia osób, którym zostały nadane uprawnienia do przetwarzania danych w systemach informatycznych, w których znajduje się potwierdzenie przeprowadzenia szkoleń w tym zakresie.

W wyniku badania dokumentacji dotyczącej 20 pracowników Spółki, w zakresie zapewnienia przez Szpital personelowi szkoleń związanych z RODO oraz szkoleń z bezpieczeństwa danych, ustalono m.in., że: 19 z nich złożyło w 2021 r. oświadczenia o przeszkoleniu z zakresu bezpieczeństwa i ochrony danych przetwarzanych w systemach, na które otrzymali upoważnienie. Oświadczenia te były składane na wnioskach o nadanie uprawnień do przetwarzania danych osobowych w systemach teleinformatycznych (wg wzoru określonego w Uzupełnieniu do polityki ochrony danych). W jednym z 20 przypadków (dotyczy pracownika, który nie złożył ww. oświadczenia), w aktach osobowych znajdowała się karta szkolenia wstępnego z zakresu ochrony danych osobowych z 2019 r., potwierdzająca odbycie takiego szkolenia. Badanie wykazało, że takie karty szkolenia z 2019 r. posiadało jeszcze 15 pracowników. Ponadto w 15 przypadkach w aktach osobowych pracownika znajdował się także certyfikat z 2018 r. potwierdzający odbycie szkolenia „Ochrona danych osobowych zgodnie z RODO w placówkach medycznych"[44]. W dwóch przypadkach pracownicy Szpitala uczestniczyli 3 października 2023 r. w spotkaniu informacyjno-szkoleniowym z IOD[45], na którym omawiano zgodnie z agendą: obowiązki Szpitala, jako administratora danych, obowiązki i odpowiedzialność osób upoważnionych do przetwarzania danych osobowych, organizacyjne i techniczne

[42] Styczeń 2024 r.

[43] Do 31 grudnia.

[44] Organizator szkolenia - firma zewnętrzna Akademia Rozwoju eConomic.

[45] Na podstawie list obecności uczestników spotkania.

środki bezpieczeństwa niezbędne do zapewnienia odpowiedniej ochrony danych osobowych.

W wyniku badania stwierdzono również, że we wszystkich 20 przypadkach nie udokumentowano przeszkolenia pracowników Szpitala w zakresie ochrony danych osobowych w sposób określony w pkt 6 Polityki ochrony danych, tj. poprzez wystawienia zaświadczenia wg wzoru określonego w załączniku nr 7 do ww. polityki, mimo iż taki sposób dokumentowania szkoleń określono w obowiązujących w Szpitalu regulacjach wewnętrznych.

Prezes Zarządu podał, że zgodnie z rekomendacją nowego IOD, udokumentowanie wstępnego szkolenia z zakresu ochrony danych osobowych, stanowi zapoznanie się i podpisanie informacji „obowiązki informacyjne dla pracowników/ współpracowników"; zmiana procedur jest w opracowaniu.

(akta kontroli str. 309-313, 410-416, 424-440, 504-511)

1.11. W okresie objętym kontrolą Spółka występowała do Narodowego Funduszu Zdrowia[46] o wsparcie finansowe inwestycji poprawiających bezpieczeństwo infrastruktury technicznej i dwukrotnie uzyskała takie dofinasowanie z Funduszu Przeciwdziałania COVID-19, tj.:

- w ramach umowy nr 8/2022 z 21 czerwca 2022 r. Szpital otrzymał wsparcie w wysokości 396,4 tys. zł na pokrycie w 100% wydatków związanych z zakupem: systemu monitorowania infrastruktury SOC, systemu bezpieczeństwa sieci EDR dla 200 urządzeń, biblioteki taśmowej, systemu backup oraz usługi szkoleniowej z zakresu cyberbezpieczeństwa[47];
- w ramach umowy nr 5/2023 z 23 sierpnia 2023 r. Szpital otrzymał 399,8 tys. zł na pokrycie w 100% wydatków związanych z zakupem: systemu do zbierania i monitorowania informacji w sieci SIEM, systemu ochrony poczty[48].

W ramach ww. wsparcia przeprowadzono także w Szpitalu dwa audyty[49]. Zespół audytorów stwierdził, że środki finansowe pochodzące z ww. umów o dofinasowanie, wydatkowane na działania podnoszące poziom bezpieczeństwa systemów teleinformatycznych świadczeniobiorców, znacząco wpłynęły na podniesienie poziomu bezpieczeństwa, w zakresie systemów teleinformatycznych Szpitala.

Ww. audyty były prowadzone metodą próbkową, tzn. nie obejmowały swym zakresem wszystkich zagadnień dotyczących cyberbezpieczeństwa, niemniej jednak zespół audytowy w swoich raportach wskazał m.in., że należy uszczegółowić i sformalizować proces zarządzania ryzykiem w bezpieczeństwie informacji, uzupełnić dokumentację poświadczającą faktyczny przebieg działań z tym związanych, zaangażować cały zespół w tworzenie analizy ryzyka i planu postępowania z ryzykiem, zadbać o uszczelnienie zakresu systemu zarządzania bezpieczeństwem informacji, wprowadzić mechanizm kontroli w postaci audytów wewnętrznych w zakresie bezpieczeństwa informacji, uzupełnić dokumentację w zakresie obowiązków OUK, zdefiniować i zaktualizować cele z zakresu bezpieczeństwa informacji. Jedno ze spostrzeżeń sformułowanych przez zespół audytowy dotyczące doprecyzowania planów ciągłości działania odwzorowanych w dokumentach, zostało przez Spółkę wdrożone, bowiem 6 listopada 2023 r. opracowano Plan ciągłości działania oraz Plan ciągłości działania systemów informatycznych w Spółce.

(akta kontroli str.314-392)

[46] Dalej: NFZ.

[47] Protokoły odbioru końcowego i dostawy z: 17 października 2022 r. i 25 listopada 2022 r.

[48] Protokół obioru końcowego z 19 października 2023 r.

[49] Umowa nr n/39/10/22 z 9 listopada 2022 r. oraz umowa nr n/56/10/23 z 19 października 2023 r.

Prezes Zarządu podkreślił, że Szpital od momentu ogłoszenia go OUK, rozwija rozwiązania z dziedziny cyberbezpieczeństwa dzięki dotacjom z NFZ na: sprzęt, oprogramowanie oraz usługi. Z uwagi na krótki czas wdrożenia decyzji wydanej przez Ministerstwo Zdrowia, Szpital nie był w stanie wywiązać się w szczególności z dostosowania swojej dokumentacji. Wskazał także, że Szpital utrzymuje się głównie ze świadczenia usług zdrowotnych ze środków publicznych NFZ i nie są tam wkalkulowane żadne koszty związane z cyberbezpieczeństwem. Działania związane ze spełnianiem wszystkich wymagań są niezwykle kosztowne, co w sytuacji corocznego zamykania rocznej działalności kilkumilionową stratą, bez zewnętrznych środków celowanych, staje się niemożliwe. Ponadto przyjęty scenariusz następujących po sobie przekształceń w podmiocie leczniczym niesie ze sobą realne ryzyko przejmowania reguł organizacyjnych po poprzednikach, odpowiednio: ZOZ, SPZOZ, Szpital Giżycki, Szpital Giżycki w upadłości.

W ocenie Prezesa Zarządu należałoby zapewnić m.in.: stosowne finansowanie działań w zakresie cyberbezpieczeństwa dla podmiotów będących OUK, gotowe wzory procedur, czy też dostępność dedykowanych specjalistów o pożądanych kwalifikacjach.

(akta kontroli str. 437-440, 508-511)

Stwierdzone nieprawidłowości

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

1) od 1 lipca 2020 r. do 31 grudnia 2023 r. nie opracowano i w konsekwencji nie wdrożono SZBI, spełniającego w pełni wymogi określone rozporządzeniem KRI (opisano w punkcie 1.2 wystąpienia pokontrolnego),

2) niewdrożenie (według stanu na 31 grudnia 2023 r.) systemu zarządzania bezpieczeństwem w systemie informacyjnym, wykorzystywanego do świadczenia usługi kluczowej, zapewniającego prowadzenie systematycznego szacowania ryzyka wystąpienia incydentu i zarządzania tym ryzykiem oraz zarządzanie incydentami, pomimo że termin do jego wprowadzenia (określony w ustawie o cyberbezpieczeństwie) upłynął 4 października 2022 r. (opisano w punkcie 1.6),

3) niewywiązanie się (według stanu na 31 grudnia 2023 r.) z obowiązku aktualizacji dokumentacji dotyczącej cyberbezpieczeństwa systemu informacyjnego wykorzystywanego do świadczenia usługi kluczowej w terminie określonym w ustawie o cyberbezpieczeństwie, gdyż termin na dokonanie takiej aktualizacji upłynął 4 stycznia 2023 r. (opisano w punkcie 1.7),

4) nieprzeprowadzenie przez Spółkę (według stanu na 31 grudnia 2023 r.), w terminie określonym ustawą o cyberbezpieczeństwie, audytu bezpieczeństwa systemu informacyjnego wykorzystywanego do świadczenia usługi kluczowej, tj. do 4 lipca 2023 r. (opisano w punkcie 1.8),

5) niezamieszczenie na stronie internetowej Szpitala (wg stanu na 7 grudnia 2023 r.), w terminie określonym ustawą o cyberbezpieczeństwie, informacji zapewniającej użytkownikowi usługi kluczowej dostęp do wiedzy pozwalającej na zrozumienie zagrożeń cyberbezpieczeństwa i stosowanie skutecznych sposobów zabezpieczania się przed tymi zagrożeniami w zakresie związanym ze świadczoną usługą kluczową, tj. do 4 października 2022 r. (opisano w punkcie 1.9),

6) w 20 poddanych badaniu przypadkach nie udokumentowano przeszkolenia pracowników Szpitala w zakresie ochrony danych osobowych w sposób wymagany Polityką ochrony danych, tj. poprzez wystawienia zaświadczenia wg wzoru określonego w załączniku nr 7 do ww. polityki (opisano w punkcie 1.10).

OCENA CZĄSTKOWA

W latach 2020-2023 (I półrocze) w Spółce nie zostały stworzone odpowiednie rozwiązania organizacyjne i techniczne dotyczące bezpieczeństwa informacji, w tym danych pacjentów, które stanowiłyby SZBI zgodne z wymaganiami określonymi w rozporządzenu KRI.

Głównym uzasadnieniem powyższej oceny jest stwierdzona nieprawidłowość dotycząca nieopracowania, nieustanowienia i niewdrożenia w Spółce SZBI, wbrew wymogowi określonemu w rozporządzeniu KRI, obejmującego swoim zakresem wszystkie kategorie przetwarzanych w Szpitalu informacji. Spowodowało to m.in. niewywiązanie się przez Spółkę (jako OUK), w określonych ustawą o cyberbezpieczeństwie terminach, z obowiązków dotyczących: wdrożenia systemu zarządzania bezpieczeństwem w systemie informacyjnym wykorzystywanym do świadczenia usługi kluczowej, aktualizacji dokumentacji Szpitala dotyczącej cyberbezpieczeństwa oraz wykonania audytu bezpieczeństwa systemu informacyjnego wykorzystywanego do świadczenia usługi kluczowej. Niemniej funkcjonowała w Szpitalu Polityka bezpieczeństwa informacji, ktora obejmowała m.in. procedury określające zasady zarządzania bezpieczeństwem w systemie informacyjnym, mające zapewnić poufność, integralność, dostępność i autentyczność danych osobowych. Ponadto nieterminowo zamieszczono na stronie internetowej Szpitala informację o zagrożeniach cyberbezpieczeństwa i o stosowaniu skutecznych sposobów zabezpieczania się przed tymi zagrożeniami. Pracownicy Szpitala zostali przeszkoleni w zakresie ochrony danych osobowych i bezpieczeństwa informacji, lecz dokumentowanie tych szkoleń nie było realizowane zgodnie z wewnętrznymi uregulowaniami.

We właściwy sposób określono i przypisano odpowiednim pracownikom odpowiedzialność za bezpieczeństwo informacji. IOD wyznaczony zgodnie z rozporządzeniem RODO, posiadał odpowiednie kwalifikacje, a zakres jego obowiązków określono w sposób wskazany we wspomnianym rozporządzeniu.

OBSZAR

2. Funkcjonowanie przyjętych rozwiązań i ich wpływ na ochronę danych pacjentów przed cyberatakami

Opis stanu faktycznego

2.1. W latach 2020-2023 (I półrocze) w Spółce funkcjonowało sześć systemów informatycznych, w tym system: do diagnostyki obrazowej Alteris RIS/PACS, kadrowo-płacowy KS-ZZL, TOPSOR zarządzający trybami obsługi pacjentów w Szpitalnym Oddziale Ratunkowym (system kolejkowy), Enova 365 ERP[50], „Planowanie pracy", wspomagający tworzenie harmonogramów pracy personelu medycznego oraz Medicus, będący kompleksowym systemem informatycznym klasy HIS[51] do obsługi jednostek służby zdrowia. Zarządzanie zasobami sieci informatycznej Spółki odbywało się za pomocą usługi Active Directory[52].

(akta kontroli str. 524-530)

2.2.1. Według stanu na 30 listopada 2023 r. w Spółce na stanowiskach niemedycznych zatrudnionych było 80 osób, a dostęp do systemu Medicus posiadało

[50] ERP (z ang. Enterprise Resource Planning), system wspomagający planowanie zasobów przedsiębiorstwa.

[51] HIS – z ang. Hospital Information System. System ten, jako kompleksowe rozwiązanie, łączy w sobie część medyczną, zintegrowaną z zewnętrznym laboratorium analitycznym, szpitalną pracownią diagnostyki obrazowej, jak również z systemem Enova 365 ERP. Zapewnia zarządzanie każdą medyczną komórką organizacyjną dzięki automatyzacji prac i elektronicznym przepływom informacji. Pozwala rozliczać się z NFZ i podmiotami komercyjnymi.

[52] Active Directory pozwala administratorom sieci, centralnie, z poziomu jednego komputera (odpowiednio skonfigurowanego serwera) zarządzać całym zbiorem użytkowników w sieci, określać ich uprawnienia do zasobów sieciowych, a także konfigurować komputery, na których pracują.

27 z nich[53]. Analiza uprawnień do tego systemu dziewięciu pracowników niemedycznych (tj. 33,3% takich pracowników posiadających dostęp do ww. systemu) wykazała m.in., że:

- Każdy z nich posiadał, zatwierdzone przez Prezesa Zarządu Spółki (ADO), pisemne upoważnienie do przetwarzania danych osobowych w zakresie obowiązków i zadań służbowych wykonywanych na zajmowanym stanowisku, wymagane punktem C4. (Obowiązki osób uprawnionych do przetwarzania danych osobowych) Polityki ochrony danych;
- W ośmiu badanych przypadkach Spółka dysponowała pisemnymi wnioskami o nadanie pracownikom niemedycznym Spółki uprawnień w systemie Medicus, podpisanymi przez tych pracowników lub przez ich przełożonych, podczas gdy zgodnie z punktem 3 (Nadawanie uprawnień) Instrukcji zarządzania systemem informatycznym uprawnienia te są nadawane na wniosek kierownika kadr lub IOD. Kierownik Działu ds. Pracowniczych wyjaśniła, że w tych przypadkach pracownicy błędnie wypełniali wnioski o nadanie uprawnień w związku z pośpiechem i niedokładnym zapoznaniem się z zapisami na druku. Dodała, że dokument ten, po wypełnieniu przez pracownika, trafiał bezpośrednio do inspektora ochrony danych osobowych, gdzie był ewidencjonowany i archiwizowany;
- Spółka nie posiadała, według stanu na 26 stycznia 2024 r., dokumentu potwierdzającego nadanie jednemu z pracowników niemedycznych[54] uprawnień do przetwarzania danych osobowych w systemie Medicus, wymaganego punktem 3 (Nadawanie uprawnień) ww. Instrukcji. Kierownik Działu ds. Pracowniczych wyjaśniła, że wniosek „zawieruszył się" w związku ze zmianą na stanowiskach inspektorów RODO i brakiem bezpośredniego przekazania sobie dokumentów. Podała również, że każdorazowo ona, lub wskazany przez nią pracownik, wydawali informatykowi polecenie ustne, lub poprzez wiadomość e-mail, o nadanie uprawnień dla pracowników;
- Pracownicy niemedyczni zatrudnieni byli na stanowiskach:
  - Statystyka medycznego, tj. dwóch pracowników, prowadzących rozliczenia z NFZ, zatrudnionych w Dziale Rozrachunku Usług Medycznych, Planowania i Analiz, posiadających w systemie Medicus dostęp do wszystkich oddziałów, pododdziałów, pracowni i poradni szpitalnych;
  - Sekretarza/sekretarki medycznej, tj. czterech pracowników, w tym: dwóch[55] posiadających w ww. systemie dostęp do wszystkich oddziałów i pododdziałów szpitalnych, jeden[56] – dodatkowo dostęp do wszystkich pracowni i poradni, a jeden[57], oprócz dostępu do swojej komórki organizacyjnej, posiadał również dostęp do Poradni Chorób Zakaźnych, Izby Przyjęć i Oddziału Urazowo-Ortopedycznego. Prezes Zarządu wyjaśnił, że sekretarki medyczne w treści swoich zakresów obowiązków posiadają zapis „inne zadania zlecone przez przełożonego" i związku z tym obejmował on również inne oddziały, na których nie wykonywały stale swoich zadań. W przypadku długotrwałej nieobecności jednej sekretarki jej zastępstwo

[53] Po odpowiednim przeprowadzeniu autoryzacji użytkownika, tj. wprowadzeniu przez niego loginu i hasła.

[54] Spółka, według stanu na 26 stycznia 2024 r., nie przedłożyła, zatwierdzonego przez Prezesa Zarządu, wniosku o nadanie temu pracownikowi (rejestrator medyczny) uprawnień do przetwarzania danych osobowych w systemach teleinformatycznych, ani dokument ten nie był ujęty w Rejestrze wydanych upoważnień do systemów teleinformatycznych. Użytkownik ten posiadał, według stanu na 19 grudnia 2023 r., aktywne konto użytkownika w systemie Medicus.

[55] Wykonujący obowiązki służbowe w Szpitalnym Oddziale Ratunkowym, a druga z tych osób – w Oddziale Pediatrycznym, Pododdziale Noworodkowym i Oddziale Anestezjologii i Intensywnej Terapii.

[56] Wykonujący obowiązki w Oddziale Wewnętrznym z Pododdziałem Gastroenterologicznym.

[57] Wykonujący obowiązki na Oddziale Chorób Zakaźnych.

musiało być pełnione przez inną. Ponadto pacjenci przenoszeni są pomiędzy oddziałami i sekretarka medyczna może mieć rozszerzony dostęp o inne oddziały w ramach realizowania zadań i potrzebnych uprawnień na stanowisku pracy;

- Rejestratora medycznego – dwie osoby, w tym: jedna posiadająca w ww. systemie wyłącznie dostęp do poradni, w których wykonywała obowiązki służbowe, a jedna, wykonująca obowiązki w Poradni Chorób Płuc i Gruźlicy, posiadająca dostęp również do poradni: Urazowo-Ortopedycznej, Urologicznej i Endokrynologicznej. Prezes Zarządu wyjaśnił, że w przypadku tego pracownika zaszła konieczność pomocy w innych poradniach, w ramach posiadanego uprawnienia;
- Referenta – jedna osoba zatrudniona w statystyce medycznej, do której obowiązków należało m.in. sporządzanie i przesyłanie korespondencji dotyczącej pobytu chorego oraz prowadzenie księgi głównej chorych, posiadająca uprawnienia w ww. systemie do wszystkich komórek organizacyjnych Szpitala.

(akta kontroli str. 26-152, 531-692 i 697-736)

W sprawie uprawnień w systemie Medicus ww. dziewięciu pracowników niemedycznych, a także 30 pracowników medycznych (opis zawarto w punkcie 2.2.2) Prezes Zarządu Spółki podał, że pracownicy ci posiadali uprawnienia do tego systemu zgodnie z zakresem przypisanych im obowiązków i zadań służbowych. Miejscem zatrudnienia każdego pracownika jest Spółka, a wszystkie grupy pracowników mają ujednolicone zakresy obowiązków, zgodnie z wykonywanym zawodem. Zarówno miejsce zatrudnienia, jak i ujednolicone zakresy obowiązków w grupach pracowniczych mają za cel zachowanie ciągłości udzielania świadczeń zdrowotnych, zgodnie umową z NFZ. Prezes Zarządu dodał, że osoby te są obowiązane do zachowania w tajemnicy informacji związanych z pacjentem uzyskanych w związku z wykonywaniem zadań.

(akta kontroli str. 685-692)

2.2.2. Według stanu na 30 listopada 2023 r. w Spółce zatrudnionych było 259 pielęgniarek i położnych (personel medyczny). Analiza uprawnień do systemu Medicus 30 pielęgniarek i położnych (11,6%) wykazała m.in., że:

- Każda z nich posiadała, zatwierdzone przez Prezesa Zarządu Spółki (ADO), pisemne upoważnienie do przetwarzania danych osobowych w zakresie obowiązków i zadań służbowych wykonywanych na zajmowanym stanowisku, wymagane punktem C4 (Obowiązki osób uprawnionych do przetwarzania danych osobowych) Polityki ochrony danych;
- W przypadku 23 pielęgniarek i położnych Spółka posiadała pisemne wnioski o nadanie im uprawnień w systemie Medicus, podpisane przez tych pracowników lub przez ich przełożonych, podczas gdy zgodnie z punktem 3 (Nadawanie uprawnień) ww. Instrukcji uprawnienia te są nadawane na wniosek kierownika kadr lub IOD. Wyjaśnienia Kierownika Działu ds. Pracowniczych w tej sprawie podano w punkcie 2.2.1 ppkt 2;
- Sześcioro z ww. pracowników medycznych posiadało, według stanu na 9 stycznia 2024 r., uprawnienia do systemu Medicus, podczas gdy zatwierdzone przez ADO wnioski o nadanie im uprawnień w tym systemie wygasły w latach 2022-2023 (do 30 listopada). Kierownik Działu ds. Pracowniczych wyjaśniła, że uprawnienia tym osobom nie zostały odebrane, gdyż są one nadal zatrudnione w Giżyckiej Ochronie Zdrowia. Pracownik wypełniający druk wpisał datę zakończenia trwania umowy, zamiast zaznaczenia pozycji: „do odwołania”;

- Spółka nie posiadała, według stanu na 26 stycznia 2024 r., dokumentu potwierdzającego nadanie siedmiu pracownikom medycznym[58] (23,3%), spośród 30 badanych, uprawnień do przetwarzania danych osobowych w systemie Medicus, wymaganego punktem 3 (Nadawanie uprawnień) Instrukcji zarządzania systemem informatycznym. Wyjaśnienia Kierownika Działu ds. Pracowniczych w tej sprawie podano w punkcie 2.2.1 ppkt 3;
- 10 pielęgniarek i położnych posiadało dostęp w systemie Medicus wyłącznie do komórek organizacyjnych, w których, zgodnie z umowami o pracę/ kontraktami/ umowami zleceniami, wykonywały swoje obowiązki służbowe;
- 20 pielęgniarek i położnych, oprócz dostępu w ww. systemie do komórek organizacyjnych przypisanych im w zakresach czynności lub w umowach zleceniach, posiadały również dostęp do innych oddziałów, pododdziałów, poradni. Prezes Zarządu podał, że osoby te posiadają rozszerzony dostęp do innych komórek organizacyjnych niż komórka, w której wykonują na co dzień obowiązki służbowe, z uwagi na bieżącą współpracę oddziału z innymi komórkami, np. poradniami, czy pracowniami. W złożonych wyjaśnieniach Prezes Zarządu odniósł się indywidualnie do każdego z 20 pracowników, podając że m.in.:
  - czterej pracownicy Izby Przyjęć i Szpitalnego Oddziału Ratunkowego posiadają dostęp do wszystkich oddziałów w związku z koniecznością prawidłowej rejestracji pacjenta i przekazania go na odpowiednie oddziały szpitalne,
  - dwaj pracownicy Bloku Operacyjnego oraz Oddziału Anestezjologii i Intensywnej Terapii posiadają dostęp do oddziałów zabiegowych ze względu na konieczność dostępu do wyników badań i historii choroby pacjenta, w tym wskazań uczulenia na leki,
  - dwóch pracowników Oddziału Chorób Zakaźnych ma również dostęp do Izby Przyjęć w związku z koniecznością zapewnienia pacjentom bezpośredniego przyjęcia na ten oddział 24 godziny na dobę przez 7 dni w tygodniu, a pracownik Oddziału Ginekologiczno-Położniczego posiada dostęp do Izby przyjęć w związku z rejestracją pacjentek, które trafiają w nocy do porodu bezpośrednio na ten oddział,
  - w przypadku dwóch pracowników uprawnienia do Oddziału Chorób Zakaźnych zostały nadane w związku z zabezpieczeniem dyżuru na tym oddziale (zastępstwa).

  Jednocześnie Prezes Zarządu podał, że w trakcie kontroli NIK została przeprowadzona weryfikacja uprawnień w systemie Medicus, w wyniku której uprawnienia w nim do dodatkowych komórek organizacyjnych odebrano trzem, spośród ww. 20 pracowników medycznych, które były nadane m.in. na okres zastępstwa.

(akta kontroli str. 26-152, 531-536, 685-736 i 742-821)

2.2.3. Wprowadzony Uzupełnieniem do polityki ochrony danych wzór wniosku o nadanie uprawnień do przetwarzania danych osobowych w systemach teleinformatycznych nie określał szczegółowo w jakim zakresie mają być przyznawane danemu pracownikowi uprawnienia do systemu Medicus On-Line. Wymagał natomiast m.in. skreślenia odpowiedzi „Tak/Nie" w pozycji „Zakres uprawnień" przy wskazanym systemie informatycznym.

[58] Spółka nie przedłożyła, zatwierdzonego przez Prezesa Zarządu, wniosku o nadanie tym pracownikom uprawnień do przetwarzania danych osobowych w systemach teleinformatycznych, ani dokumenty te nie były ujęte w Rejestrze wydanych upoważnień do systemów teleinformatycznych. Pracownicy ci posiadali, według stanu na 9 stycznia 2024 r., aktywne konto użytkownika w systemie Medicus.

W sprawie przekazywania w latach 2020-2023 ASI informacji, do jakich zasobów systemu Medicus (m.in. do jakich komórek organizacyjnych) i w jakim zakresie (m.in. klasa użytkownika, tj. czy administrator, czy np. pielęgniarka, czynności – tj. przeglądanie, dodawanie, edycja, usuwanie, dostęp do historii) mają być nadane uprawnienia danemu pracownikowi, Prezes Zarządu podał, że zakres dostępu dla każdego pracownika wynikał z informacji o komórce organizacyjnej. Szczegółowy dostęp do zasobów ustalał informatyk w uzgodnieniu z bezpośrednim przełożonym pracownika. W większości reguły dostępu były standardowe i wynikały z zajmowanego stanowiska i wskazanej komórki organizacyjnej. Wybór klas dla danego pracownika w systemie był niejednokrotnie dopasowywany indywidualnie w porozumieniu z bezpośrednim przełożonym.

(akta kontroli str. 85-95 i 822-840)

2.3. W latach 2020-2023 (do 30 listopada) Spółka zatrudniała 11 lekarzy z zagranicy[59], z których jeden uzyskał w Polsce tytuł lekarza specjalisty, jednemu, decyzją Ministra Zdrowia, uznano tytuł specjalisty otrzymany za granicą za równoważny z tytułem specjalisty w danej dziedzinie w Polsce, dwóch było po nostryfikacji dyplomu ukończenia studiów medycznych za granicą, a siedmiu, decyzją Ministra Zdrowia, otrzymało zgodę na wykonywanie w Polsce zawodu lekarza. Lekarzom tym Spółka nadała uprawnienia m.in. do systemu Medicus.

(akta kontroli str. 841-843)

2.4. W latach 2022-2023 (do 18 grudnia) w przypadku 62 pracowników medycznych Spółki ustał ich stosunek pracy, przy czym 53 z nich posiadało uprawnienia do systemu Medicus, z których:

- jednemu pracownikowi uprawnienia do niego odebrano trzy dni przed dniem ustania stosunku pracy,
- 42 z nich (79,2%) uprawnienia odebrano po ustaniu stosunku pracy (średnio po 244 dniach), w tym:
  - 9 pracownikom – po upływie od 2 do 6 dni od ustania stosunku pracy,
  - 5 pracownikom – od 8 do 23 dni,
  - 8 pracownikom – od 44 do 168 dni,
  - 6 pracownikom – od 198 do 348,
  - 14 pracownikom – od 409 do 667 dni,
- 10 z nich (18,9%), z którymi po przerwie w zatrudnieniu trwającej od 4 do 325 dni (średnio 64 dni) nawiązano ponownie stosunek pracy, uprawnienia nie były odbierane w tym okresie.

Jednocześnie w przypadku 29 pracowników (spośród 53 uprawnionych, tj. 54,7%) uprawnienia do ww. systemu odebrano w trakcie kontroli NIK, po upływie od 14 do 667 dni od rozwiązania z nimi stosunku pracy (średnio po 322 dniach).

Zgodnie z punktem 3 (Nadawanie uprawnień) Instrukcji zarządzania systemem informatycznym ADO (tj. Prezes Zarządu Spółki) zobowiązany był do dokonywania bieżącej weryfikacji uprawnień nadanych w systemach informatycznych, a także do wnioskowania o ich odebranie m.in. w przypadku ustania stosunku pracy.

Posiadanie przez ww. 52 pracowników uprawnień do systemu informatycznego Medicus po rozwiązaniu z nimi stosunku pracy, umożliwiło dziewięciu z nich (17,3%), dokonanie logowań do systemu. Ostatnie takie logowania danego pracownika wystąpiły po upływie od 3 do 149 dni (średnio 42 dni) od wygaśnięcia stosunku pracy.

[59] Z Białorusi, Mołdawii, Syrii i Ukrainy.

Prezes Zarządu Spółki wyjaśnił, że uprawnienia nie były odbierane osobom, którym zmieniała się jedynie forma zatrudnienia lub wygasała umowa na czas określony, a współpraca była kontynuowana bez zmian w zakresie uprawnień. Pracownikom nie były zabierane uprawnienia do systemu, w przypadku gdy pomiędzy pracodawcą, a pracownikiem doszło do ustnego porozumienia się co do kontynuacji zatrudnienia w Spółce. W przypadku lekarzy, którzy zmieniali formę zatrudnienia podpisana została promesa dotycząca przyszłego zatrudnienia. Prezes dodał, że uprawnienia odbierane są na podstawie uzyskanych informacji z działu ds. pracowniczych, przekazywanych w formie elektronicznej (email) lub ustnie. W latach 2020-2023 trwały intensywne prace nad wdrożeniem programu kadrowo-płacowego i większość czynności wykonywana była ręcznie, przy jednoczesnym wykonywaniu bieżących zadań, co przyczyniło się do bardzo dużego obciążenia działu kadr, jak również informatyków, w związku z problemami wdrożenia systemu do bieżącej obsługi zatrudnionych pracowników.

(akta kontroli str. 74-84, 685-692, 695-696 i 844-856)

NIK zwraca uwagę, że art. 29 oraz art. 32 ust. 4 RODO wskazują, że to ADO podejmuje działania w celu zapewnienia, by każda osoba fizyczna mająca dostęp do danych osobowych, przetwarzała je wyłącznie na podstawie jego upoważnienia i na jego polecenie. Natomiast, w myśl motywu 39 RODO, dane osobowe powinny być przetwarzane w sposób zapewniający im odpowiednie bezpieczeństwo i odpowiednią poufność, w tym ochronę przed nieuprawnionym dostępem do nich i do sprzętu służącego ich przetwarzaniu oraz przed nieuprawnionym korzystaniem z tych danych i z tego sprzętu.

Prezes Zarządu Spółki określił w trakcie kontroli NIK nowe zasady współpracy m.in. pomiędzy działem ds. pracowniczych, a informatykami Szpitala, w zakresie nadawania i odbierania pracownikom uprawnień do systemów informatycznych. W piśmie z 28 grudnia 2023 r. zobowiązał kierownika działu ds. pracowniczych do bieżącego przekazywania informatykom Szpitala informacji o zatrudnieniu i rozwiązaniu umów z pracownikami, najpóźniej w dniu podjęcia pracy lub w dniu rozwiązania lub wygaśnięcia umowy. Prezes Zarządu polecił w ww. piśmie informatykom Szpitala każdorazowe, na bieżąco i bez zbędnej zwłoki, nadawanie lub anulowanie uprawnień w przypadku zawarcia lub zakończenia umowy.

(akta kontroli str. 694)

2.5. Spółka, będąca operatorem usługi kluczowej w sektorze służby zdrowia, otrzymała 16 października 2023 r. pismo z Departamentu Innowacji Ministerstwa Zdrowia z 10 października 2023 r., w którym zarekomendowano wdrożenie rozwiązań mających na celu wyeliminowanie określonych podatności w systemie bezpieczeństwa w czterech obszarach: poczta elektroniczna, dostęp do serwerów VPN lub proxy, zablokowanie portów USB oraz zablokowanie wykonywania komend i makr. Informatycy Spółki podali, że zostały podjęte działania w celu wdrożenia zalecanych rozwiązań. Zablokowano dostęp do poczty elektronicznej z popularnych portali (m.in. interia.pl, wp.pl, onet.pl, o2.pl) oraz dostęp do serwerów VPN lub proxy. Podali również, że podjęto bezskuteczną próbę zablokowania z domeny Szpitala dostępu do portów USB i obecnie trwają prace nad wyłączeniem portów USB w komputerach służbowych poprzez zakupiony system EDR Eset.

Przeprowadzone w toku kontroli NIK[60] oględziny pięciu stanowisk komputerowych[61] oraz systemu operacyjnego Windows i systemu informatycznego Medicus[62] w zakresie stosowanych przez Spółkę rozwiązań służących ochronie przetwarzanych informacji i prawidłowego stosowania Instrukcji zarządzania systemem informatycznym, wykazały m.in., że:

- Dostęp do pulpitu użytkownika systemu operacyjnego Windows[63] oraz do systemu Medicus wymagał podania danych uwierzytelniających, tj. nazwy użytkownika i hasła, którego długość spełniała wymogi ww. Instrukcji, składało się ono bowiem minimum z 8 znaków;
- Użytkownicy komputerów pracowali wyłącznie na własnych kontach utworzonych w domenie Windows;
- Użytkownicy korzystali z indywidualnych kont domenowych i nie posiadali uprawnień administratora domeny Windows, a poddane oględzinom stanowiska komputerowe nie posiadały dostępu do służbowej poczty elektronicznej[64];
- Na wszystkich stanowiskach komputerowych poddanych oględzinom umożliwiony był dostęp do portów USB;
- Komputery posiadały dostęp do internetu, a zainstalowane na nich programy antywirusowe posiadały aktualne bazy sygnatur;
- Na żadnym z pięciu stanowisk poddanych oględzinom nie włączono w ustawieniach sytemu Windows wygaszacza ekranu po określonym czasie braku aktywności użytkownika, pomimo że w punkcie 5 (Procedury użytkowania systemu) ww. Instrukcji określono, iż wygaszacz ekranu powinien aktywować się po 15 minutach braku aktywności użytkownika.

  Informatycy Szpitala wyjaśnili, że zamiast wygaszacza ekranu włączono jego wymuszone wyłączenie[65], dzięki czemu występuje dużo mniejsze zużycie prądu w Spółce. Ze względu na charakter pracy lekarzy, pielęgniarek oraz pozostałej kadry w Szpitalu wydłużony został czas wyłączenia ekranu z 15 na 20 minut. Informatycy podali, że Spółka jest w trakcie zmiany polityki bezpieczeństwa, w tym Instrukcji zarządzania systemem informatycznym, i w nowych zapisach zostanie ujęte ostateczne ustalenie co do czasu wyłączania ekranu na komputerach.

  NIK zauważa jednak, że ustawione na komputerach Spółki automatyczne wyłączenie ekranu komputera po 20 minutach braku aktywności użytkownika nie jest tym samym co aktywacja wygaszacza ekranu. Oba te rozwiązania mogą funkcjonować niezależnie od siebie. Zdaniem Izby w przypadku stwierdzenia przez Szpital niższej funkcjonalności danego rozwiązania, w pierwszej kolejności należałoby dokonać odpowiednich zmian w obowiązującej procedurze, a dopiero w następnym kroku – wdrożyć je w życie. Natomiast odwrotna kolejność

[60] W dniu 16 stycznia 2024 r.

[61] Komputery nr: SZP-CHIR-7, SZP-ORTO-25, LAP-SZP-ORTO-2, SZP-NEUR-24, SZP-SOR-22, znajdujące się na Oddziale Urazowo-Ortopedycznym, Oddziale Neurologii oraz Izbie Przyjęć, obsługiwane przez lekarzy, pielęgniarki lub rejestratorki medyczne.

[62] Głównie w zakresie ustawień parametrów oby tych systemów, odnoszących się do ochrony przetwarzanych informacji.

[63] Wersje: 10 Pro lub 11 Pro.

[64] Uprawnienia do skrzynek poczty elektronicznej posiadały inne stanowiska pracy, tj. m.in. Prezes Zarządu, kierownicy komórek organizacyjnych oraz wybrane stanowiska wymagające posiadania takiego dostępu (m.in. sekretarki medyczne oddziałów szpitalnych, stanowiska jednoosobowe w administracji Szpitala). Spółka w okresie objętym kontrolą korzystała z komercyjnych, wykupionych u dostawcy usług internetowych home.pl, skrzynek pocztowych. Szpital korzystał ze spersonalizowanego adresu e-mail we własnej domenie, tj. zozgiz.pl. Skrzynki pocztowe posiadały filtry antyspamowe, a od 19 października 2023 r., wiadomości przychodzące i wychodzące były filtrowane poprzez system ochrony poczty Trend Macro Email Security.

[65] W ustawieniach domeny systemu Windows wprowadzono wymóg ponownego wpisania hasła przez użytkownika w przypadku wystąpienia automatycznego wyłączenia ekranu komputera.

postępowania powoduje, że zastosowane rozwiązanie jest niezgodne z przyjętymi zasadami.

- W ustawienia dotyczących wspólnych parametrów kont użytkowników systemu Medicus określono czas ważności hasła na 365 dni, a w parametrach domeny systemu Windows – na 40 dni. Było to niezgodne z punktem 4 (Metody i środki uwierzytelniania) ww. Instrukcji, w której określono, że maksymalny okres ważności hasła wynosi 30 dni, a wymuszenie jego zmiany następuje po tym okresie automatycznie.

  Informatycy Spółki wyjaśnili, że zmiany w długościach haseł oraz częstotliwości ich wymuszonych zmian dostosowują do zaleceń CERT[66]. Ponieważ testują rozwiązania z tym związane, to w domenie Windows ustawiono czas ważności hasła na 40 dni, a w Medicus – 365 dni. Chociaż CERT zaleca nie zmieniać haseł w ogóle, są oni za rozwiązaniem, aby wszyscy użytkownicy zmieniali hasło raz do roku, a jego złożoność wynosiła minimum 12 znaków, w tym mała i duża litera oraz co najmniej 1 cyfra, bez użycia imienia czy nazwiska użytkownika oraz wyrazów kojarzonych ze Spółką, takich jak szpital czy poradnia. Informatycy podali, że Spółka jest w trakcie zmiany polityki bezpieczeństwa i w nowych zapisach zostanie ujęte ostateczne ustalenie co do złożoności haseł oraz ich zmian.
  NIK zauważa jednak, że stosowane w praktyce powyższe rozwiązania nie są zgodne z obowiązującą w Spółce procedurą wewnętrzną.

- W ustawieniach systemu Medicus, dostępnych z konta jego administratora w Spółce, nie stwierdzono parametrów odnoszących się do: maksymalnej liczby błędnych logowań, minimalnej liczby dużych liter, małych liter, cyfr i znaków specjalnych w haśle, a minimalną liczbę znaków w haśle ustawiono na 12, podczas gdy system dopuszczał utworzenie hasła składającego się z minimum 8 znaków. Jednocześnie, po wielokrotnym (tj. 20-krotnym) wprowadzeniu błędnego hasła do tego systemu, nie następowała blokada dostępu do niego. Informatycy Szpitala wyjaśnili, że administrator systemu nie ma możliwości zmiany długości hasła z 8 znaków na więcej, ponieważ jest to ustawienie globalne narzucone przez dostawcę oprogramowania, a ustawiony parametr w Medicus na 12 znaków nie ma zastosowania. Również z tego samego powodu administrator systemu nie ma możliwości ustalenia złożoności znaków w haśle. Informatycy podali, że Spółka będzie monitować do dostawcy oprogramowania o włączenie takiej funkcjonalności. Natomiast brak blokowania, w wyniku błędnych logowań, konta użytkownika w ww. systemie, wynikał z błędu systemowego, zgłoszonego 22 stycznia 2024 r., który ma zostać wyeliminowany przez dostawcę oprogramowania przy kolejnych aktualizacjach.

(akta kontroli str. 72-84, 724-728, 731, 737-741 i 857-866)

2.6. W latach 2020-2023 (I półrocze), według prowadzonego przez Spółkę Rejestru naruszeń ochrony danych osobowych, wystąpił jeden zarejestrowany incydent zagrażający bezpieczeństwu systemu informatycznego[67]. Był to tzw. atak hakerski, mający na celu zaszyfrowanie danych, w wyniku którego utracono czasowo dane dotyczące części komórek administracyjnych Szpitala. W ocenie Spółki nie wystąpiły przesłanki do zgłoszenia naruszenia organowi nadzorczemu, ponieważ nie stwierdzono naruszenia poufności i integralności chronionych danych osobowych, ani ryzyka naruszenia praw lub wolności osób fizycznych. Zaszyfrowane w wyniku ataku

[66] CERT – zespół CERT Polska, działa w strukturach NASK – Państwowego Instytutu Badawczego, prowadzącego działalność naukową, krajowy rejestr domen .pl i dostarczającego zaawansowane usługi teleinformatyczne. CERT Polska to pierwszy powstały w Polsce zespół reagowania na incydenty. Rekomendowane wymagania dla polityki haseł CERT opublikował na stronie internetowej https://cert.pl/posts/2022/01/kompleksowo-o-haslach/.

[67] W dniu 13 lipca 2022 r. w godzinach od 0.51 do 2.33.

dane zostały odzyskane i sprawdzone. W związku z wystąpieniem powyższego zdarzenia Spółka postąpiła zgodnie z procedurą określoną w jej Polityce ochrony danych, bowiem m.in.:

- administrator systemów informatycznych powiadomił o ww. incydencie IOD,
- przeprowadzono udokumentowane postępowanie wyjaśniające, w wyniku którego ustalono m.in. przyczynę sytuacji, skutki oraz jakie działania należy podjąć,
- dokonano oceny ryzyka naruszenia praw i wolności osoby fizycznej,
- incydent został prawidłowo odnotowany w Rejestrze naruszeń ochrony danych osobowych.

(akta kontroli str. 26-71, 96-152 i 867-874)

W latach 2020-2023 (do 3 grudnia) do Spółki nie wpłynęły skargi dotyczące ewentualnego naruszenia ochrony danych osobowych.

(akta kontroli str. 876-879)

2.7. W latach 2020-2023 (I półrocze) Spółka zawarła osiem umów dotyczących powierzenia przetwarzania danych osobowych pacjentów. Analiza treści dwóch takich umów, podpisanych 26 marca 2021 r. z Uniwersyteckim Szpitalem Klinicznym w Białymstoku i 30 czerwca 2022 r. z Grupą Medicus sp. z o.o. w Toruniu, wykazała, że zawierały one postanowienia wymagane art. 28 RODO. Określono w nich bowiem m.in. zobowiązanie podmiotu przetwarzającego dane osobowe do ich zabezpieczenia poprzez stosowanie odpowiednich środków technicznych i organizacyjnych oraz do zwrotu Spółce i usunięcia wszelkich tych danych po zakończeniu świadczenia usług związanych z ich przetwarzaniem, obowiązek zgłaszania Spółce bez zbędnej zwłoki stwierdzenia naruszenia ich ochrony oraz do zachowania ich w tajemnicy. Przesłankami zawarcia tych umów było zapewnienie prawidłowej oraz należytej realizacji umów na: badania poekspozycyjne w zakresie wirusa HIV oraz badania rezonansem magnetycznym.

(akta kontroli str. 880-889)

Stwierdzone nieprawidłowości

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

1) sporządzenie przez inne osoby, niż wskazane w Instrukcji zarządzania systemem informatycznym, wniosków o nadanie pracownikom uprawnień do przetwarzania danych osobowych w systemach teleinformatycznych oraz nieposiadanie przez Spółkę, wymaganych tą procedurą, wniosków o nadanie pracownikom uprawnień do przetwarzania danych osobowych w systemach teleinformatycznych (opisano w punkcie 2.2.1 i 2.2.2 wystąpienia pokontrolnego),
2) nierzetelna realizacja obowiązku w zakresie odbierania byłym pracownikom Spółki dostępu do systemu informatycznego Medicus (opisano w punkcie 2.4),
3) niestosowanie się do wewnętrznych uregulowań Spółki w zakresie bezpieczeństwa danych w systemach informatycznych, a dotyczących funkcjonowania wygaszania ekranu komputera po odpowiednim czasie braku aktywności użytkownika oraz maksymalnego okresu ważności hasła (opisano w punkcie 2.5).

OCENA CZĄSTKOWA

Przetwarzanie danych pacjentów w Szpitalu odbywało się bez stosowania w prawidłowy sposób niektórych zasad dotyczących bezpieczeństwa przetwarzania danych osobowych pacjentów w systemach teleinformatycznych. Nierzetelnie bowiem realizowano obowiązek w zakresie odbierania byłym pracownikom Szpitala uprawnień dostępu do systemu Medicus. Większości tym pracownikom (54,7% zbadanych przypadków) odebranie uprawnień nastąpiło dopiero w trakcie kontroli

NIK. Ponadto nie dochowano należytej staranności przy przestrzeganiu wewnętrznych regulacji w zakresie nadawania ww. uprawnień. Spółka nie dysponowała bowiem pisemnymi wnioskami o ich nadanie (20,5% badanych przypadków), a 31 pozostałych badanych wniosków o nadanie uprawnień do systemu Medicus było podpisanych przez inne osoby, niż określono to w Instrukcji zarządzania systemem informatycznym. Rozwiązania sprzętowe i systemowe zastosowane w zakresie bezpieczeństwa informacji w systemach informatycznych były w niektórych przypadkach niezgodne z wewnętrznymi przepisami Szpitala.

Wszyscy objęci badaniem pracownicy Szpitala, zgodnie z obowiązującymi wymaganiami, posiadali upoważnienia do przetwarzania danych osobowych. Zakres tych upoważnień był zgodny z zakresem obowiązków i zadań służbowych wykonywanych na zajmowanym stanowisku. Również nadany dostęp do systemu Medicus, w przypadkach tego wymagających, był adekwatnie rozszerzony o inne komórki organizacyjne i poprawnie ustalony do realizowanych przez te osoby zadań. Spółka prawidłowo zastosowała procedurę w związku z zaistniałym w okresie objętym kontrolą incydentem zagrażającym bezpieczeństwu jej systemu informatycznemu (atak hakerski). Również prawidłowo zawierała umowy dotyczące powierzenia innym podmiotom danych osobowych pacjentów.

IV. Uwagi i wnioski

W wyniku kontroli Najwyższa Izba Kontroli nie formułuje uwag. Uwzględniając podjęte w trakcie kontroli działania Najwyższa Izba Kontroli nie formułuje wniosków w zakresie stwierdzonych nieprawidłowości dotyczących: nieprzeprowadzenia audytu bezpieczeństwa systemu informacyjnego, niezamieszczenia na stronie internetowej Szpitala informacji o zasadach cyberbezpieczeństwa, nieodebrania byłym pracownikom uprawnień do systemu informatycznego. W związku ze stwierdzonymi pozostałymi nieprawidłowościami, Najwyższa Izba Kontroli, na podstawie art. 53 ust. 1 pkt 5 ustawy o NIK, przedstawia następujące wnioski:

Wnioski

1. Opracowanie i wdrożenie SZBI w pełni zgodnego z wymogami określonymi w rozporządzeniu KRI oraz ustawie o cyberbezpieczeństwie.
2. Dokumentowanie przeszkolenia pracowników Szpitala w zakresie ochrony danych osobowych i bezpieczeństwa informacyjnego w sposób zgodny z wewnętrznymi uregulowaniami.
3. Rzetelne sporządzanie wymaganych wewnętrzną procedurą Spółki wniosków o nadanie pracownikom uprawnień do przetwarzania danych osobowych w systemach teleinformatycznych.
4. Stosowanie rozwiązań dotyczących bezpieczeństwa danych w systemach informatycznych zgodnych z procedurą wewnętrzną Spółki lub wprowadzenie w nich zmian w celu zapewnienia zgodności podejmowanych działań w tym zakresie z wewnętrznymi uregulowaniami.

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 Olsztynie. 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 21 od otrzymania wystąpienia pokontrolnego, o sposobie wykonania wniosków pokontrolnych oraz o podjętych działaniach lub przyczynach niepodjęcia tych działań.

W przypadku wniesienia zastrzeżeń do wystąpienia pokontrolnego, termin przedstawienia informacji liczy się od dnia otrzymania uchwały o oddaleniu zastrzeżeń w całości lub zmienionego wystąpienia pokontrolnego.

Olsztyn, 19 lutego 2024 r.

Najwyższa Izba Kontroli
Delegatura w Olsztynie
Dyrektor
z up.
Piotr Wanic
Wicedyrektor

.....
podpis

Kontrolerzy
Krzysztof Śleszyński
doradca ekonomiczny

.....
podpis

Justyna Lis
starszy inspektor kontroli państwowej

.....
podpis