LBI.430.004.2019
Nr ewid. 149/2019/P/19/063/LBI

Informacja o wynikach kontroli

WDROŻENIE PRZEZ PODMIOTY LECZNICZE REGULACJI DOTYCZĄCYCH OCHRONY DANYCH OSOBOWYCH

DELEGATURA W BIAŁYMSTOKU

MISJĄ
Najwyższej Izby Kontroli jest dbałość o gospodarność i skuteczność w służbie publicznej dla Rzeczypospolitej Polskiej

WIZJĄ
Najwyższej Izby Kontroli jest cieszący się powszechnym autorytetem najwyższy organ kontroli państwowej, którego raporty będą oczekiwanym i poszukiwanym źródłem informacji dla organów władzy i społeczeństwa

Informacja o wynikach kontroli
Wdrożenie przez podmioty lecznicze regulacji dotyczących ochrony danych osobowych

p.o. Dyrektor Delegatury w Białymstoku

Agata Ciupa

Akceptuję:
Wiceprezes Najwyższej Izby Kontroli

Ewa Polkowska

Zatwierdzam:
Prezes Najwyższej Izby Kontroli

Krzysztof Kwiatkowski
Warszawa, dnia 19.08.2019 r.

Najwyższa Izba Kontroli
ul. Filtrowa 57
02-056 Warszawa
T/F +48 22 444 50 00

www.nik.gov.pl

SPIS TREŚCI

Wykaz stosowanych skrótów, skrótowców i pojęć

ABI	administrator bezpieczeństwa informacji – osoba, o której mowa w art. 36a ust. 1 obowiązującej do 25 maja 2018 r. ustawy o ochronie danych osobowych, od 25 maja 2018 r. inspektor ochrony danych;
ADO	administrator danych – osoba fizyczna lub prawna, organ publiczny, jednostka lub inny podmiot, który samodzielnie lub wspólnie z innymi ustala cele i sposoby przetwarzania danych osobowych (art. 4 pkt 7 RODO);
działalność lecznicza	udzielanie świadczeń zdrowotnych oraz wykonywanie czynności z zakresu promocji zdrowia lub realizacja zadań dydaktycznych i badawczych w powiązaniu z udzielaniem świadczeń zdrowotnych i promocją zdrowia (art. 3 u.o.d.l.);
Grupa Robocza ds. Ochrony Danych	Grupa Robocza – niezależny organ doradczy w zakresie ochrony danych i prywatności, powołany na mocy art. 29 Dyrektywy 95/46/WE Parlamentu Europejskiego i Rady z dnia 24 października 1995 r. *w sprawie ochrony osób fizycznych w zakresie przetwarzania danych osobowych i swobodnego przepływu tych danych* (Dz. Urz. UE L 281 z 1995 r., s. 31, ze zm.); Grupa została rozwiązana 25 maja 2018 r., a w jej miejsce powstała Europejska Rada Ochrony Danych;
IOD	inspektor ochrony danych, o którym mowa w art. 37 RODO;
Prezes Urzędu	Prezes Urzędu Ochrony Danych Osobowych – organ właściwy w sprawie ochrony danych osobowych oraz organ nadzorczy w rozumieniu RODO;
przewodnik po RODO	*Przewodnik po RODO dla służby zdrowia* – materiał edukacyjny, będący efektem prac zespołu zadaniowego ds. ochrony zdrowia, działającego w ramach Grupy Roboczej ds. Ochrony Danych Osobowych, utworzonej w Ministerstwie Cyfryzacji (opublikowany 24 września 2018 r.);
pseudonimizacja	proces polegający na zmianie identyfikatorów, które są danymi osobowymi na takie, które nimi nie są (np. imiona i nazwiska osób fizycznych zastępowane są liczbami); pseudonimizacja jest procesem odwracalnym;
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 (Dz. Urz. UE L 119 z 4.05.2016 r., s. 1, ze zm.);
rozporządzenie KRI	rozporządzenie Rady Ministrów z dnia 12 kwietnia 2012 r. *w sprawie Krajowych Ram Interoperacyjności, minimalnych wymagań dla rejestrów publicznych i wymiany informacji w postaci elektronicznej oraz minimalnych wymagań dla systemów teleinformatycznych* (Dz. U. z 2017 r. poz. 2247);
szpital lub podmiot leczniczy	zakład opieki zdrowotnej, podmiot wykonujący działalność leczniczą, zgodnie z u.o.d.l.;
SP ZOZ	Samodzielny Publiczny Zakład Opieki Zdrowotnej;
system HIS	Hospital Information System – system informatyczny do obsługi szpitala; głównym jego zadaniem jest obsługa pacjenta w poradniach i na oddziałach, tworzenie elektronicznej dokumentacji medycznej;
u.o.k.s.c.	ustawa z dnia 5 lipca 2018 r. *o krajowym systemie cyberbezpieczeństwa* (Dz. U. poz. 1560);
u.o.d.l.	ustawa z dnia 15 kwietnia 2011 r. *o działalności leczniczej* (Dz.U z 2018 r. poz. 2190, ze zm.);
u.o.d.o.	ustawa z dnia 10 maja 2018 r. *o ochronie danych osobowych* (Dz. U. poz. 1000, ze zm.);
u.o.p.p.	ustawa z dnia 6 listopada 2008 r. *o prawach pacjenta i Rzeczniku Praw Pacjenta* (Dz. U. z 2017 r. poz. 1318, ze zm.).

1. WPROWADZENIE

Pytanie definiujące cel główny kontroli

Czy dane osobowe w podmiotach leczniczych są prawidłowo chronione i przetwarzane?

Pytania definiujące cele szczegółowe kontroli

1. Czy prawidłowo opracowano wymaganą dokumentację i procedury związane z ochroną przetwarzanych danych osobowych?
2. Czy wdrożone rozwiązania zapewniają prawidłowe przetwarzanie i ochronę danych osobowych?

Jednostki kontrolowane

Kontrolą objęto 24 podmioty lecznicze z sześciu województw.

Okres objęty kontrolą

Od 25 maja 2018 r. do zakończenia kontroli NIK w poszczególnych jednostkach (ostatnia 23 kwietnia 2019 r.). Badania kontrolne dotyczyły działań sprzed tego okresu, jeśli mały związek z zagadnieniami będącymi przedmiotem kontroli.

Z dniem 25 maja 2018 r. zaczęły obowiązywać przepisy RODO oraz regulacje z nim związane określone w u.o.d.o. Obowiązek stosowania tych norm dotyczy wszystkich placówek medycznych – publicznych i niepublicznych. Nie ma znaczenia skala działalności takiego podmiotu. RODO dotyczy zarówno dużych szpitali, zatrudniających wielu lekarzy, pielęgniarek i położnych, jak i gabinetów z jednym lub kilkoma lekarzami.

RODO zmieniło zasady przetwarzania, wykorzystywania i przechowywania danych osobowych, zwiększając ochronę tych danych oraz nakładając nowe obowiązki na ADO. Jednostki prowadzące działalność leczniczą w związku z wejściem w życie nowych przepisów obowiązane były do dokonania przeglądu stosowanych rozwiązań i sprawdzenia, czy są skuteczne.

RODO już na etapie preambuły definiuje pojęcie danych osobowych dotyczących zdrowia. Zgodnie z motywem 35., za takie dane uważane są *wszystkie dane o stanie zdrowia osoby, której dane dotyczą, ujawniające informacje o przeszłym, obecnym lub przyszłym stanie fizycznego lub psychicznego zdrowia konkretnej osoby.* Do danych medycznych zaliczane są także informacje pochodzące z badań laboratoryjnych lub lekarskich części ciała lub płynów ustrojowych, w tym (co jest nowością w szczególności z punktu widzenia obowiązujących do tej pory krajowych przepisów), dane genetyczne i próbki biologiczne oraz wszelkie informacje, na przykład o chorobie, niepełnosprawności, ryzyku choroby, historii medycznej, leczeniu klinicznym lub stanie fizjologicznym, lub biomedycznym osoby, której dane dotyczą, niezależnie od ich źródła, którym może być na przykład lekarz lub inny pracownik służby zdrowia, szpital, urządzenie medyczne lub badanie diagnostyczne in vitro. Zgodnie ze wspomnianym motywem 35. preambuły RODO, do danych dotyczących zdrowia zaliczają się także numery, symbole lub oznaczenia przypisane danej osobie fizycznej w celu jednoznacznego zidentyfikowania tej osoby do celów zdrowotnych, przy czym, co ważne, chodzi tutaj o oznaczenia nadawane nie tylko podczas świadczenia usług opieki zdrowotnej, ale także rejestracji do tych usług.

Zgodnie z art. 51 ust. 1 Konstytucji RP, *nikt nie może być obowiązany inaczej niż na podstawie ustawy do ujawniania informacji dotyczących jego osoby.* W preambule RODO wskazano, że *osoby fizyczne powinny mieć kontrolę nad własnymi danymi osobowymi*[1]. Wynikające jednak z postępu technicznego nowe mechanizmy i usługi stwarzają poważne zagrożenie dla prywatności i ochrony danych. Coraz trudniej jest zatem zachować kontrolę nad własnymi danymi osobowymi.

Dane dotyczące zdrowia stanowią, zgodnie z art. 9 ust. 1 RODO, szczególną kategorię danych osobowych, których przetwarzanie jest zabronione, chyba że spełniony jest jeden z 10 warunków, wskazanych w art. 9 ust. 2 RODO. Przestrzeganie tych postanowień jest istotne dla ochrony prywatności pacjentów. Szczególnie ważne jest tam, gdzie ujawnienie danych może wiązać się z pewnego rodzaju stygmatyzacją.

[1] Motyw 7. preambuły RODO.

RODO wprowadza jedynie ogólne zasady zarządzania bezpieczeństwem danych osobowych. Nie określa, w jaki sposób powinna być prowadzona dokumentacja ich przetwarzania. Nie wskazuje też, jakie metody powinien zastosować zarządzający jednostką do właściwej ochrony tych danych.

Jeszcze przed wejściem w życie przepisów RODO, podmioty prowadzące działalność leczniczą zgłaszały wątpliwości dotyczące sposobu wywiązywania się z nałożonych przez ten dokument obowiązków związanych z ochroną danych osobowych. Odpowiedzią na to było m.in. podjęcie już w 2017 r. działań zmierzających do opracowania *Kodeksu postępowania dla sektora ochrony zdrowia.* Miały być w nim doprecyzowane regulacje zawarte w RODO, co miało ułatwić ADO ich interpretację. Jak wynika z informacji zamieszczonych na stronie www.rodowzdrowiu.pl, dokument ten 13 listopada 2018 r. został wraz z wnioskiem o jego przyjęcie złożony do Prezesa Urzędu.

Kolejnym działaniem związanym z właściwą implementacją RODO było powołanie w lipcu 2018 r., Grupy Roboczej ds. Ochrony Danych Osobowych w Ministerstwie Cyfryzacji. Efektem pracy zespołu było opublikowanie we wrześniu 2018 r. *Przewodnika po RODO dla Służby Zdrowia.* W materiale tym wskazano odpowiedzi na pytania związane z RODO, dotyczące m.in.: metod rejestracji pacjentów z poszanowaniem ich prywatności, kwestii związanych z opisywaniem leków danymi pacjenta, zagadnień dotyczących możliwości zamieszczania tabliczek ze specjalnością lekarza na drzwiach gabinetów oraz tabliczek o stanie zdrowia na tzw. kartach przyłóżkowych[2].

Coraz częściej do gromadzenia, przechowywania i przetwarzania danych osobowych, w tym dotyczących stanu zdrowia w podmiotach leczniczych wykorzystywane są systemy informatyczne. Jak wskazuje Ministerstwo Zdrowia, *jednym z głównych założeń Unii Europejskiej jest rozwój gospodarki oparty na nowoczesnych technologiach informatycznych, dotyczących również ochrony zdrowia, w której zastosowanie nowoczesnych rozwiązań zwiększa skuteczność opieki zdrowotnej*[3].

Korzystanie z narzędzi informatycznych (np. Internetu), które umożliwiają wymianę informacji i przepływ danych medycznych stwarza jednak ryzyko wystąpienia nieuprawnionego dostępu, przejęcia lub zniszczenia tych zasobów. Nie bez znaczenia jest również fakt, że dane medyczne są bardzo cennymi informacjami dla cyberprzestępców. W ostatnich kilku latach pojawiło się wiele doniesień medialnych dotyczących m.in. ujawnienia dokumentów z danymi osobowymi i medycznymi pacjentów, znajdującymi się w wielu szpitalach. Były tam również dane dostępowe do różnych systemów informatycznych oraz dane osobowe pracowników szpitali[4]. Część upublicznionych informacji dotyczyła szpitali psychiatrycznych oraz osób, które były ich pacjentami. Ujawnienie danych tego rodzaju może być szczególnie dotkliwe dla pacjentów.

---

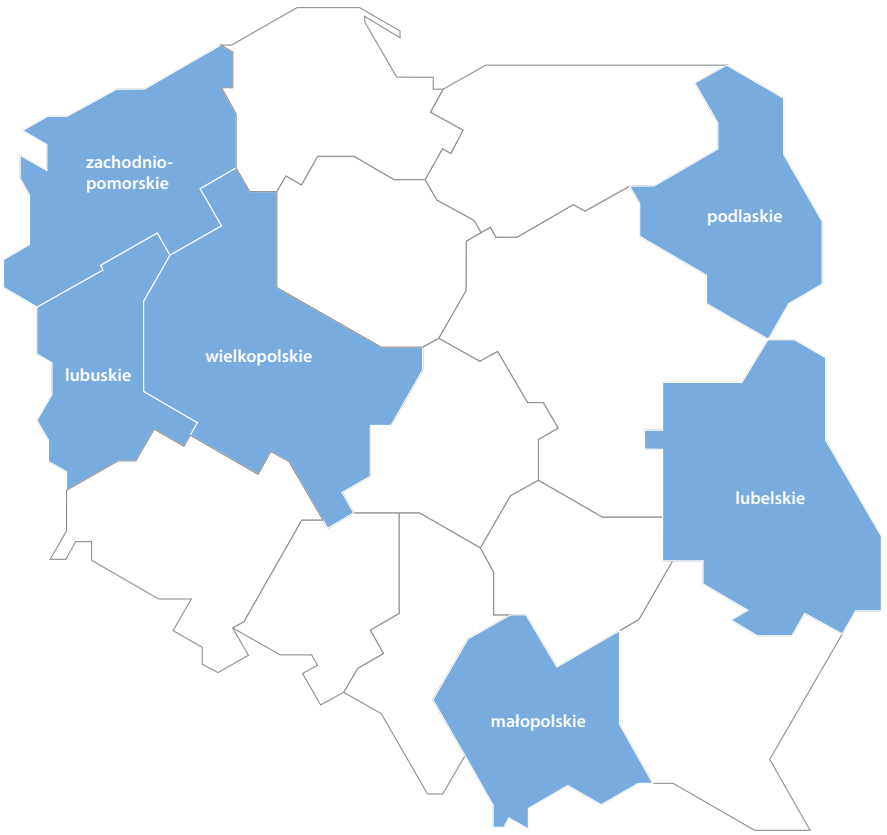
2 https://www.gov.pl/cyfryzacja/rodo-w-sluzbie-zdrowia-po-pierwsze-pacjent, [dostęp z dnia 2 października 2018 r.].

3 http://www.archiwum.mz.gov.pl/rozwoj-i-inwestycje/informatyzacja-w-ochronie-zdrowia/, [dostęp 15 grudnia 2018 r.].

4 https://niebezpiecznik.pl/post/dane-pacjentow-i-szpitali-wyciekly-z-helpdesku-eskulapa-szpitale-powinny-zmienic-hasla/, [dostęp 6 października 2018 r.].

Kontrola objęła okres od wejścia w życie przepisów RODO (25 maja 2018 r.) do 23 kwietnia 2019 r., tj. do zakończenia czynności kontrolnych w ostatnim ze szpitali. Była ona kontrolą zgodności. NIK przeprowadziła ją w 24 podmiotach leczniczych z terenu sześciu województw: podlaskiego, lubelskiego, lubuskiego, małopolskiego, wielkopolskiego i zachodniopomorskiego. W każdym z województw do kontroli wytypowano cztery szpitale (dwa miejskie lub powiatowe oraz dwa wojewódzkie). Taki dobór próby pozwolił na ocenę badanego zagadnienia w różnych regionach kraju oraz w szpitalach o różnej wielkości i statusie właścicielskim.

Infografika nr 1
Województwa, w których położone były podmioty objęte kontrolą



Źródo: Opracowanie własne NIK.

2. OCENA OGÓLNA

Dane osobowe pacjentów nie były właściwie chronione i przetwarzane

Niemal w żadnym ze skontrolowanych podmiotów leczniczych dane osobowe pacjentów nie były prawidłowo chronione i przetwarzane po wejściu w życie przepisów RODO[5]. W konsekwencji kierownicy tych podmiotów i Inspektorzy Ochrony Danych nie zapewnili pacjentom pełnego zabezpieczenia ich danych. Personel medyczny i administracyjny postępował rutynowo, według schematów wypracowanych przed wejściem w życie nowych uregulowań.

Niewłaściwie opracowywano dokumentację i procedury związane z RODO

Szesnaście z 24 skontrolowanych podmiotów leczniczych (67%) nie było właściwie przygotowanych do wejścia w życie RODO. Dokumenty i procedury związane z wejściem w życie RODO zostały w nich bowiem wdrożone z opóźnieniem lub do zakończenia kontroli NIK ich nie wprowadzono:

- w dziewięciu szpitalach analiza ryzyka procesów przetwarzania danych osobowych, która powinna poprzedzić przyjęcie właściwych środków do ochrony danych osobowych, została przeprowadzona po upływie od 35 do 201 dni od dnia wejścia w życie RODO, a w dwóch kolejnych wykonano ją dopiero w trakcie kontroli NIK,
- w siedmiu podmiotach leczniczych wewnętrzną dokumentację, opisującą stosowane środki techniczne i organizacyjne związane z zapewnieniem bezpieczeństwa danych osobowych, zaktualizowano po upływie od 37 do 263 dni od wejścia w życie RODO, a w czterech jej nie uaktualniono,
- w siedmiu szpitalach rejestr czynności przetwarzania założono od 12 do 263 dni od wejścia w życie RODO, a w jednym go nie opracowano.

Jedną z głównych przyczyn wymienionych nieprawidłowości była nieznajomość zagadnień bezpieczeństwa danych osobowych. Tylko w dziewięciu szpitalach szkoleniami w tym zakresie objęto prawie cały personel (co najmniej 95%). W rezultacie w podmiotach tych stwierdzono najmniej istotnych nieprawidłowości dotyczących ochrony danych osobowych pacjentów.

Przyjęte rozwiązania nie zapewniały prawidłowego przetwarzania i ochrony danych osobowych

Jedynie w trzech szpitalach (12,5%) przyjęte rozwiązania organizacyjne i techniczne stworzyły odpowiednie warunki do rejestracji na wizyty do lekarza, identyfikacji pacjenta na oddziale i przechowywania jego dokumentacji medycznej. W pozostałych nie zapewniono skutecznej ochrony danych osobowych i medycznych pacjentów przed ujawnieniem osobom postronnym.

Nie przestrzegano też ustalonej w RODO zasady ograniczania dostępu do danych osobowych do zakresu niezbędnego do osiągnięcia celu ich przetwarzania. W rezultacie średnio co 11 pielęgniarka posiadała przyznane w systemie informatycznym uprawnienia do danych medycznych pacjentów leczonych na innych oddziałach szpitala, a byłym pracownikom personelu medycznego 15 podmiotów leczniczych (62,5%) nie odebrano niezwłocznie dostępu do systemów informatycznych. Z kolei 11 szpitali (45,8%) w nieuprawniony sposób przekazało dane osobowe pacjentów podmiotom serwisującym systemy informatyczne. Prawidłowo natomiast przyznawano dostęp do systemu HIS pracownikom działów administracyjnych. Był on odpowiedni i niezbędny do wykonywania obowiązków służbowych.

W 18 szpitalach (75%) nie przestrzegano wymogów dotyczących nadawania właściwych uprawnień do administrowania systemami informatycznymi, ochrony przed złośliwym oprogramowaniem oraz odpowiedniej autoryzacji. W pięciu (20,8%) zaś kopie bezpieczeństwa danych przechowywano w niewłaściwym miejscu. Nie gwarantowało to zabezpieczenia zasobów elektronicznych przed nieuprawnionym dostępem, przejęciem i zniszczeniem.

[5] Kontrolą objęto okres od 25 maja 2018 r. do 23 kwietnia 2019 r. (data zakończenia czynności kontrolnych w ostatniej z jednostek).

3. SYNTEZA WYNIKÓW KONTROLI

Właściwe rozwiązania organizacyjne i techniczne

Tylko w trzech skontrolowanych szpitalach (12,5%) stwierdzono właściwe rozwiązania organizacyjne i techniczne, stwarzające odpowiednie warunki rejestracji na wizyty do lekarza, identyfikacji pacjenta na oddziale i przechowywania jego papierowej dokumentacji medycznej[6]. [str. 29–37]

Niewłaściwa realizacja zadań związanych z powołaniem IOD

We wszystkich 24 skontrolowanych szpitalach wywiązano się z obowiązku powołania IOD, przy czym w 13 z nich funkcję tę powierzono dotychczasowym ABI. Pięciu ADO poinformowało o tym fakcie Prezesa Urzędu z opóźnieniem, wynoszącym od 14 do 109 dni. Z kolei na stronach internetowych trzech podmiotów leczniczych nie zamieszczono danych IOD oraz sposobu i formy kontaktu z nim, mimo że obowiązek taki wynikał z przepisów RODO. [str. 17–19]

Zapewnienie niezależności IOD

Kierownicy niemal wszystkich skontrolowanych podmiotów leczniczych podjęli działania umożliwiające IOD wykonywanie obowiązków w sposób niezależny, wynikający z art. 38 ust. 3 RODO. Konflikt interesów stwierdzono w jednym szpitalu, w którym IOD był jednocześnie kierownikiem Działu Informatyki, a zatem brał udziału w określaniu celów i sposobów przetwarzania danych osobowych. [str. 19]

Nieprzeprowadzanie analizy ryzyka procesów związanych z przetwarzaniem i ochroną danych osobowych przed wejściem w życie przepisów RODO

Do 25 maja 2018 r. (daty bezpośredniego zastosowania RODO w porządku krajowym) jedynie w 13 skontrolowanych szpitalach (54%) przeprowadzono analizę ryzyka procesów przetwarzana danych osobowych, wynikającego z przypadkowego lub niezgodnego z prawem ich zniszczenia, utraty, modyfikacji, nieuprawnionego ujawnienia lub nieuprawnionego dostępu do takich danych przesyłanych, przechowywanych albo w inny sposób przetwarzanych. W kolejnych dziewięciu podmiotach leczniczych wykonano ją do końca 2018 r., a w dwóch pozostałych – dopiero w trakcie kontroli NIK. [str. 23–24]

Brak ocen skutków dla ochrony danych

Przeprowadzenie oceny skutków przetwarzania danych zalecała Grupa Robocza ds. Ochrony Danych dla operacji przetwarzania danych trwających przed 25 maja 2018 r. Zdaniem Grupy, ocena taka mogła być przydatnym narzędziem, pomocnym w zapewnieniu zgodności z prawem ochrony danych. Pozwalała na uzyskanie bieżącej wiedzy o występujących ryzykach w zakresie bezpieczeństwa, w celu podjęcia właściwych decyzji dotyczących zapewnienia środków technicznych i organizacyjnych związanych z bezpieczeństwem danych osobowych. [str. 24–25]

Ocenę skutków dla ochrony danych przeprowadzono w 12 szpitalach (50%), przy czym w pięciu przed przyjęciem do stosowania przepisów RODO, w pozostałych siedmiu – po tej dacie. W żadnym przypadku analizy te nie były jednak związane z rozpoczęciem przetwarzania nowych kategorii danych, stanowiąc często element audytu wewnętrznego. W dwóch szpitalach oceny skutków dla ochrony danych były niepełne, gdyż nie zawierały informacji, czy operacje przetwarzania są niezbędne oraz proporcjonalne w stosunku do celów i ryzyka naruszenia praw lub wolności osób, których dane dotyczą. [str. 24–25]

[6] Niepubliczny ZOZ Szpital im. prof. Z. Religi w Słubicach sp. z o.o., Szpital Specjalistyczny im. Stanisława Staszica w Pile, Wielkopolskie Centrum Onkologii im. Marii Skłodowskiej-Curie w Poznaniu.

Opóźnienia w aktualizacji wewnętrznej dokumentacji związanej z bezpieczeństwem przetwarzania danych

W 11 skontrolowanych podmiotach leczniczych (45,8%) nie zaktualizowano wraz z wejściem w życie RODO podstawowych dokumentów opisujących bezpieczeństwo danych osobowych oraz sposoby ich przetwarzania. Chociaż posiadana dokumentacja nie zawierała niezbędnych uregulowań dotyczących m.in. powołania IOD w miejsce ABI, prawa do sprostowania danych, prawa do usunięcia danych, prawa do ograniczenia przetwarzania, czy też obowiązku zgłaszania naruszenia ochrony danych osobowych organowi nadzorczemu oraz prowadzenia oceny skutków dla ochrony danych osobowych, jej aktualizację w siedmiu szpitalach przeprowadzono dopiero po upływie od 37 do 263 dni od wejścia w życie nowych uregulowań. W kolejnych zaś czterech podmiotach nie zaktualizowano jej do zakończenia kontroli NIK. [str. 20–21]

Brak zmian w strukturze organizacyjnej szpitali

Dziewięć podmiotów leczniczych (37,5%) w związku z powołaniem IOD nie zmieniło swojej struktury oraz nie wprowadziło odpowiednich zapisów w regulaminach organizacyjnych. W trzech skontrolowanych szpitalach (12,5%) nie dokonano tego do zakończenia kontroli. [str. 21]

Nieterminowe opracowanie i nierzetelne prowadzenie rejestrów czynności przetwarzania

W sześciu skontrolowanych szpitalach (25%) nie wywiązano się z terminowego obowiązku założenia i prowadzenia rejestru czynności przetwarzania (opóźnienia wyniosły od 12 do 263 dni), który zastąpił stosowane do 25 maja 2018 r. zbiory danych osobowych, prowadzone na podstawie u.o.d.o. W kolejnym zaś rejestru tego nie założono do zakończenia kontroli NIK, argumentując to zmianą na stanowisku IOD oraz dużą ilością innych obowiązków. W trzech kolejnych szpitalach rejestry czynności przetwarzania były prowadzone nierzetelnie. Nie uwzględniono w nich na przykład: uregulowań wymaganych przepisami art. 30 ust 1 lit. a RODO bądź niektórych czynności związanych z przetwarzaniem danych osobowych pacjentów. [str. 21–22]

Błędy związane z zawieraniem umów powierzenia przetwarzania danych osobowych

Podmioty lecznicze były obowiązane do zawierania pisemnych umów powierzenia przetwarzania danych, gdy udostępniają takie dane podmiotom zewnętrznym. W pięciu ze skontrolowanych szpitali (21%) stwierdzono błędy w tym zakresie. Polegały one głównie na: niepodpisaniu niektórych z umów powierzenia przetwarzania danych, nieprzestrzeganiu uregulowań wewnętrznych podmiotów leczniczych dotyczących wymogów formalnych wobec umów oraz konieczności prowadzenia ich ewidencji, wskazaniu w umowie niewłaściwego zakresu danych osobowych, jakiego powierzenie dotyczyło. [str. 22–23]

Brak klauzul informacyjnych dla pacjentów

W trzech skontrolowanych szpitalach (12,5%) nie we wszystkich rejestracjach zamieszczono informacje, o których mowa w art. 13 ust. 1–2 RODO, tj. wskazujące dane personalne oraz adresy ADO i IOD, cele i podstawy przetwarzania danych oraz ich kategorie i okres przechowywania. [str. 31]

Brak szkoleń pracowników

Jedynie w dziewięciu skontrolowanych szpitalach (37,5%) szkolenia związane z wejściem w życie przepisów RODO oraz bezpieczeństwem danych osobowych w systemach informatycznych objęły co najmniej 95% personelu. W rezultacie w podmiotach tych stwierdzono najmniej istotnych nieprawidłowości w zakresie ochrony danych osobowych pacjentów. W pozostałych siedmiu wskaźnik ten wynosił od 51 do 94%, a w ośmiu kolejnych – mniej niż połowę. Szkolenie powinno być zaś jednym z najistot-

niejszych elementów przygotowania podmiotu leczniczego do wejścia w życie RODO, którego obowiązek przeprowadzenia został określony w art. 39 ust. 1 lit. b RODO i spoczywał na IOD. Brak szkoleń argumentowano głównie specyfiką działalności podmiotów leczniczych, która znacząco utrudnia przeszkolenie całej kadry w jednym ustalonym terminie. Należy jednak zauważyć, że 25-miesięczne vacatio legis dla RODO pozwalało na odpowiednie zaplanowanie i przeprowadzenie szkoleń dla większej grupy pracowników. [str. 25–27]

Podmioty lecznicze korzystały ze wskazówek zawartych w przewodniku po RODO

Wszystkie skontrolowane podmioty lecznicze korzystały i udostępniły pracownikom *Przewodnik po RODO dla służby zdrowia*, opracowany przez Ministerstwo Cyfryzacji. [str. 27–29]

Niewprowadzenie rozwiązań gwarantujących pacjentom zachowanie prywatności w procesie rejestracji

W dziewięciu skontrolowanych szpitalach (37,5%) organizacja procesu rejestracji pacjentów do poradni nie gwarantowała zachowania ich prawa do prywatności. Wystąpiły bowiem przypadki niezapewnienia odpowiednich odległości pomiędzy oknami rejestracji lub niewyznaczenia (w sześciu z tych jednostek) stref oddzielających pacjentów obsługiwanych przy okienkach od osób oczekujących w kolejce. W trzech kolejnych zaś, mimo zapewnienia odpowiedniego usytuowania okien rejestracji, nie wprowadzono środków gwarantujących zachowanie odległości pomiędzy osobami rejestrującymi się i oczekującymi w kolejce. Wszystkie te rozwiązania wskazane zostały w przewodniku po RODO, jako sposoby na wdrożenie w praktyce rozwiązań wymaganych przez to rozporządzenie. [str. 27–29]

Wzywanie pacjentów do gabinetów lekarskiego z zachowaniem anonimowości

W 23 skontrolowanych szpitalach (96%) wdrożono rozwiązania, dzięki którym nie posługiwano się imionami i nazwiskami pacjentów podczas wywoływania ich na wizytę do gabinetów poradni specjalistycznych. Wzywano ich np. poprzez podawanie imienia i godziny wizyty, numeru ustalonego przy rejestracji, bezosobowo lub przy użyciu komunikatu: „proszę kolejną osobę". W jednym z podmiotów leczniczych wywieszano zaś listy pacjentów, na których przy planowanej godzinie wizyty widniały pierwsze trzy litery imienia oraz cztery litery nazwiska pacjenta. Stosowanie takiego rozwiązania w odniesieniu do pacjentów o krótkich imionach i nazwiskach mogło nie zagwarantować ochrony danych osobowych. [str. 31–32]

Zamieszczanie danych osobowych pacjentów na opaskach indentyfikacyjnych i kartach przyłóżkowych

We wszystkich 24 skontrolowanych szpitalach wywiązano się z – określonego w art. 36 ust. 3 u.o.d.l. – obowiązku zaopatrzenia pacjentów w znaki identyfikacyjne. W 11 z nich (46%) obowiązek ten zrealizowano jednak w sposób niewłaściwy. Opaski noszone przez pacjentów zawierały bowiem – poza numerem księgi głównej bądź kodem kreskowym – imię i nazwisko, a niektórych przypadkach nr PESEL, co stanowiło naruszenie przepisu art. 36 ust. 5 u.o.d.l., w myśl którego opaska zawierać powinna informacje zapisane w sposób uniemożliwiający identyfikację pacjenta przez osoby nieuprawnione. W trzech podmiotach leczniczych, dane osobowe pacjentów były także zamieszczane na szpitalnych kartach przyłóżkowych, mimo funkcjonujących na innych oddziałach tych szpitali rozwiązań, polegających na stosowaniu ramek na karty przyłóżkowe, zasłaniających dane medyczne pacjentów. Umieszczanie danych osobowych pacjentów w sposób umożliwiający odczytanie ich przez osoby postronne stanowiło naruszenie art. 24 ust. 1 RODO, zobowiązującego ADO m.in. do wdrożenia odpowiednich środków technicznych i organizacyjnych zapewniających ochronę danych osobowych. [str. 32–34]

Błędy w sposobie przechowywania papierowej dokumentacji medycznej pacjentów

W dziewięciu szpitalach (37,5%) nie zapewniono odpowiedniego sposobu przechowywania papierowej wersji dokumentacji medycznej pacjentów w pokojach dyżurek pielęgniarskich. Znajdowała się ona bowiem w niezamykanych szafkach usytuowanych w otwartych pomieszczeniach. Podobna sytuacja miała miejsce w dyżurkach lekarzy na oddziałach. Naruszało to przepisy art. 23 ust. 2 u.o.p.p. oraz przyjęte w niektórych podmiotach leczniczych regulacje wewnętrzne związane z ochroną dokumentacji papierowej. Za szczególnie niepokojącą należy uznać sytuację stwierdzoną w jednym ze szpitali, w którym rejestratorka opuściła pomieszczenie, pozostawiając niezamknięte drzwi i włączony komputer, niezabezpieczony przed dostępem do systemu operacyjnego osób nieupoważnionych. [str. 34–36]

Ograniczenie dostępu do danych pacjentów pracownikom działów administracyjnych

Niemal we wszystkich skontrolowanych szpitalach pracownikom działów administracyjnych przyznano dostęp do systemu HIS, który był odpowiedni i niezbędny do wykonywania obowiązków służbowych. Każdy z analizowanych pracowników posiadał stosowne upoważnienie ADO do przetwarzania danych osobowych. W jednym ze szpitali niewłaściwie przyznano dostęp do systemu HIS dwóm pracownikom, którzy nie wykonywali czynności pomocniczych przy udzielaniu świadczeń zdrowotnych, w rozumieniu art. 24 ust. 2 pkt 1 u.o.p.p. i posiadanie przez nich takiego dostępu było nieuprawnione. [str. 36–37]

Nieodpowiednie uprawnienia pielęgniarek w dostępie do danych osobowych pacjentów w systemie HIS

W ośmiu szpitalach (33,3%) pielęgniarkom przyznano w systemie HIS uprawnienia dostępu do danych pacjentów z oddziałów lub poradni szpitala, na których nie świadczyły pracy. Stanowiło to naruszenie zasady adekwatności i minimalizacji, określonej w art. 5 ust. 1 lit. c RODO. Było to także niezgodne z § 20 ust. 2 pkt 4 rozporządzenia KRI, w którym zawarto zobowiązanie dla kierownictwa podmiotu publicznego do podejmowania działań zapewniających, że osoby zaangażowane w proces przetwarzania informacji mają stosowne uprawnienia i uczestniczą w tym procesie w stopniu adekwatnym do realizowanych zadań. [str. 37–38]

Brak odpowiednich upoważnień do przetwarzania danych osobowych pacjentów

W pięciu podmiotach leczniczych (21%) stwierdzono, że pracownikom, którym przyznano dostęp do danych osobowych pacjentów w systemie HIS, ADO nie wydali lub wydali z opóźnieniem upoważnienia, wymagane w art. 32 ust. 4 RODO oraz regulacjami wewnętrznymi tych jednostek. W konsekwencji pracownicy ci nie mieli uprawnień do dostępu do tych danych oraz nie został im wskazany zakres, w jakim mogą te dane przetwarzać. [str. 38]

Upoważnienia dla osób, które nie powinny przetwarzać danych osobowych

W siedmiu skontrolowanych szpitalach (29,2%) personelowi pomocniczemu i pracownikom obsługi (salowym i sanitariuszom) ADO wydali upoważnienia do przetwarzania danych osobowych (także medycznych), chociaż ich obowiązki nie wiązały się bezpośrednio z udzielaniem świadczeń opieki zdrowotnej. Było to niezgodne z przepisami art. 5 ust. 1 i art. 6 ust. 1 RODO, zobowiązującymi do ograniczenia i zminimalizowania przetwarzania danych do tego, co jest niezbędne do celów przetwarzania. [str. 39]

Nieodbieranie byłym pracownikom uprawnień w systemach informatycznych

W 15 skontrolowanych podmiotach leczniczych (62,5%) nie wywiązano się z obowiązku niezwłocznego odbierania byłym pracownikom uprawnień do systemów informatycznych tych jednostek. Stanowiło to naruszenie § 20 ust. 2 pkt 5 rozporządzenia KRI, zgodnie z którym zarządzanie bezpieczeństwem informacji realizowane jest poprzez bezzwłoczną zmianę uprawnień w przypadku zmiany zadań osób zaangażowanych w proces przetwarzania informacji. [str. 39–41]

Nieprzestrzeganie zasady adekwatności i minimalizacji danych podczas zgłaszania usterek oprogramowania

W 11 skontrolowanych szpitalach (46%) stwierdzono przypadki przekazania podmiotom serwisującym systemy informatyczne danych osobowych i medycznych pacjentów. Dane te zamieszczano w zgłoszeniach serwisowych przesyłanych tym podmiotom, czym naruszono zasadę adekwatności i minimalizacji danych wskazaną w art. 5 pkt 1 lit. c RODO. Przekazane dane nie były bowiem niezbędne do usunięcia usterek w oprogramowaniu. Możliwe było natomiast posługiwanie się unikalnym numerem ID pacjenta[7] jednoznacznie wskazującym osobę, której dane zgłoszenie dotyczyło. [str. 41–42]

Nieodpowiednie udostępnianie dokumentacji medycznej

W czterech podmiotach leczniczych (17%) stwierdzono przypadki nieprawidłowego udostępniania kopii dokumentacji medycznej. W dwóch z nich przekazano ją osobom, które nie posiadały upoważnienia udzielonego przez pacjenta. Stanowiło to naruszenie przepisów u.o.p.p., zobowiązujących do zachowania w tajemnicy informacji związanych z pacjentem przez osoby wykonujące zawód medyczny (art. 13 tej ustawy) oraz dopuszczających udostępnianie dokumentacji medycznej jedynie osobom posiadającym stosowne upoważnienie (art. 26 ust. 1). [str. 43–44]

Niewłaściwe zabezpieczenia danych osobowych w postaci elektronicznej

W 18 skontrolowanych szpitalach (75%) nie zastosowano odpowiednich środków technicznych do zabezpieczenia danych osobowych przechowywanych w postaci elektronicznej. Poszczególne elementy wpływające na bezpieczeństwo zostały niewłaściwie zaplanowane bądź były w nieodpowiedni sposób użytkowane. Stanowiło to naruszenie art. 5 ust. 1 lit. f RODO, zobowiązującego do przetwarzania danych osobowych w sposób zapewniający ich bezpieczeństwo (w tym ochronę przed niedozwolonym lub niezgodnym z prawem przetwarzaniem oraz przypadkową utratą, zniszczeniem lub uszkodzeniem), za pomocą odpowiednich środków technicznych lub organizacyjnych. [str. 45]

Nieodpowiednie uprawnienia w systemach operacyjnych

W 10 skontrolowanych podmiotach leczniczych (42%) pracownicy zaangażowani w proces przetwarzania danych osobowych posiadali uprawnienia administratora systemów operacyjnych wykorzystywanych komputerów, mimo że w ich zakresach obowiązków nie przypisano im zadań związanych z administrowaniem infrastrukturą informatyczną. Stanowiło to naruszenie przepisu § 20 ust. 2 pkt 4 rozporządzenia KRI, zgodnie z którym kierownictwo podmiotu publicznego jest obowiązane do podejmowania działań zapewniających, że osoby zaangażowane w proces przetwarzania informacji posiadają stosowne uprawnienia i uczestniczą w tym procesie w stopniu adekwatnym do realizowanych zadań. Taka sytuacja pozwalała tym osobom na nieograniczoną możliwość instalacji dowolnego oprogramowania na użytkowanych komputerach, wyłączenia ochrony antywirusowej i ingerowania w inne ustawienia systemów informatycznych. Stwarzało to istotne ryzyko obniżenia skuteczności ochrony przetwarzanych danych i zainstalowania na komputerze złośliwego oprogramowania, umożliwiającego penetrację systemu informatycznego. [str. 45]

[7] Każdemu pacjentowi w systemie HIS przypisany jest unikalny numer ID, będący odpowiednikiem numeru PESEL (nie ma dwóch pacjentów z takim samym numerem ID). Numer ID pacjenta jest wystarczający do identyfikacji osoby. Ma tę przewagę nad numerem PESEL, że nie ujawnia np. daty urodzenia i płci, co zawiera nr PESEL.

Brak ochrony antywirusowej systemów operacyjnych

W trzech szpitalach (12,5%) na części komputerów nie zainstalowano oprogramowania antywirusowego, a w czterech kolejnych (16,7%) programy te nie posiadały aktualnych baz sygnatur wirusów. Stanowiło to naruszenie § 20 ust. 2 pkt 7 i 9 rozporządzenia KRI, zgodnie z którymi kierownictwo podmiotu publicznego jest obowiązane do podejmowania działań zapewniających ochronę przetwarzanych informacji przed ich kradzieżą, nieuprawnionym dostępem, uszkodzeniami lub zakłóceniami, a także zabezpieczenia przetwarzanych informacji w sposób uniemożliwiający nieuprawnionemu jej ujawnienie, modyfikację, usunięcie lub zniszczenie. Zgodnie z przepisem § 20 ust. 2 pkt 12 tego rozporządzenia, zapewnienie odpowiedniego poziomu bezpieczeństwa w systemach teleinformatycznych polega również w szczególności na dbałości o aktualizację oprogramowania, minimalizowaniu ryzyka utraty informacji w wyniku awarii oraz ochronie przed błędami, utratą, nieuprawnioną modyfikacją. [str. 46]

Niewłaściwy proces autoryzacji użytkowników w systemie operacyjnym

W dwunastu podmiotach leczniczych (50%) nie wydawano indywidualnych loginów i haseł poszczególnym pracownikom, przez co tymi samymi danymi do autoryzacji w systemach operacyjnych posługiwała się grupa osób np. pracownicy danego oddziału szpitala. W trzech kolejnych szpitalach (12,5%) część komputerów nie wymagała uwierzytelniania (można było uruchomić system operacyjny bez podawania loginu i hasła). Niewprowadzenie prawidłowej autoryzacji było sprzeczne z regulacjami § 20 ust. 7 lit. c rozporządzenia KRI, którymi zobowiązano kierownictwa jednostki do zapewnienia ochrony przetwarzanych informacji przed kradzieżą, nieuprawnionym dostępem, uszkodzeniami lub zakłóceniami, poprzez zapewnienie środków uniemożliwiających nieautoryzowany dostęp na poziomie systemów operacyjnych, usług sieciowych i aplikacji. Uniemożliwiało też ustalenie pracownika korzystającego z komputera, co jest istotne w przypadku wystąpienia incydentów związanych z bezpieczeństwem. [str. 46–47]

Zastosowanie haseł dostępowych o nieodpowiedniej złożoności

W siedmiu szpitalach (29,2%) stosowano hasła dostępu do systemów operacyjnych komputerów, które nie spełniały wewnętrznie ustalonych wymogów złożoności. Sytuacja taka w znaczny sposób obniżała skuteczność ochrony dostępu do sytemu operacyjnego i podnosiła ryzyko wystąpienia incydentów związanych z zapewnieniem ochrony danych osobowych. [str. 47]

Wykorzystywanie systemów operacyjnych nieposiadających wsparcia producenta

W 12 skontrolowanych podmiotach leczniczych (50%) do przetwarzania danych osobowych wykorzystywano systemy operacyjne, dla których producent zakończył wsparcie techniczne. Nie były zatem publikowane aktualizacje zabezpieczeń tych produktów, poprawki czy też opcje asystowanej pomocy technicznej oraz aktualizacje zawartości technicznej online. Może to mieć znaczący wpływ na podatność tych systemów na wystąpienie różnego rodzaju działań niepożądanych. [str. 47–48]

Przechowywanie danych osobowych i medycznych pacjentów w lokalizacjach bez kontroli dostępu

W czterech szpitalach (17%) wystąpiły przypadki przechowywania na dysku twardym komputerów plików zawierających dane osobowe i medyczne pacjentów. Jednocześnie w dwóch z nich dostęp do tych urządzeń nie wymagał uwierzytelnienia lub w procesie autoryzacji posługiwano się loginem i hasłem wspólnym dla kilku osób. Brak kontroli nad dostępem do danych osobowych pacjentów stanowił naruszenie prawa pacjenta, o którym mowa w art. 13 u.o.p.p. [str. 48]

Zabezpieczenie serwerowni

W większości szpitali pomieszczenia serwerowni były właściwie zabezpieczone. Zastosowano w nich m.in. drzwi przeciwpożarowe, podłogę techniczną, czujniki dymu, czujniki alarmowe, wyposażone je w klimatyzację, gaśnice, system monitoringu. W dwóch skontrolowanych podmiotach leczniczych (8%) stwierdzono natomiast niedostateczne zabezpieczenie serwerowni, polegające m.in. na braku systemów antywłamaniowych i przeciwpożarowych. W kolejnych trzech (12,5%) stwierdzono zaś przypadki przechowywania materiałów łatwopalnych w tych pomieszczeniach. [str. 48–49]

Niewłaściwe przechowywanie kopii bezpieczeństwa

W pięciu szpitalach (21%) kopie bezpieczeństwa baz danych, w tym danych osobowych, były nieodpowiednio przechowywane. Gromadzono je w tej samej lokalizacji, co dane produkcyjne, które podlegały procesowi tworzenia kopii. Takie rozwiązanie było często sprzeczne z przyjętymi w jednostkach regulacjami wewnętrznymi. Nie gwarantowało również zabezpieczenia przed całkowitą utratą danych w przypadku wystąpienia pożaru, zalania lub innego zdarzenia, które zniszczyłoby macierze danych w serwerowni. [str. 49]

Odpowiednie działania związane z incydentami dotyczącymi naruszenia ochrony danych osobowych

Naruszenia ochrony danych osobowych odnotowały służby 13 skontrolowanych szpitali (54,2%). W sześciu z nich (25% skontrolowanych) rodzaj naruszeń wymagał powiadomienia Prezesa Urzędu, o którym mowa w art. 33 ust. 1 RODO i takie zostały przekazane. Pozostałe incydenty nie wiązały się z ryzykiem naruszenia praw lub wolności osób fizycznych. [str. 42–43]

Działania wpływające na poprawę ochrony danych osobowych

Zapewnienie prawidłowego przetwarzania i ochrony danych osobowych wymaga zmiany rutynowych zachowań personelu medycznego i administracyjnego. Nie sprzyjało temu późne opracowanie przewodnika po RODO, wydanego cztery miesiące po wejściu w życie tego rozporządzenia[8].

Poprawie przyjętych sposobów ochrony danych osobowych oraz właściwemu wdrożeniu regulacji RODO może sprzyjać szybkie przyjęcie przez Prezesa Urzędu *Kodeksu postępowania dla sektora ochrony zdrowia*, którego celem, jak wskazano we wstępie tego dokumentu, jest „zapewnienie adekwatnego poziomu ochrony Pacjentów, w związku z przetwarzaniem ich danych osobowych z uwzględnieniem ochrony zdrowia i życia Pacjentów będących dobrami nadrzędnymi". Kodeks postępowania zawiera zbiór zasad zgodnych z RODO i ustawodawstwem krajowym, w zakresie podnoszenia poziomu ochrony osób fizycznych w związku z przetwarzaniem danych osobowych. Stosowanie Kodeksu postępowania stanowić będzie okoliczność potwierdzającą wywiązywanie się z obowiązków nałożonych przez RODO na administratorów danych oraz podmioty przetwarzające, funkcjonujące na rynku podmiotów wykonujących działalność leczniczą. Najwyższa Izba Kontroli nie odnosi się do treści i nie ocenia proponowanych rozwiązań *Kodeksu postępowania dla sektora ochrony zdrowia*, ponieważ nie badała jego zapisów. Wskazuje jedynie na potrzebę istnienia wskazówek postępowania, skierowanych do podmiotów leczniczych.

Kolejnym elementem mogącym mieć pozytywny wpływ na jakość ochrony danych osobowych będzie opracowanie wytycznych dotyczących certyfikacji określonej w art. 42 RODO. Podmioty certyfikujące, o których mowa w art. 43 tego rozporządzenia, będą bowiem odgrywać ważną rolę w procesie „uwiarygodnienia" przedsiębiorstw i instytucji w zakresie zgodności przetwarzania danych osobowych z przepisami prawa.

[8] *Przewodnik po RODO dla służby zdrowia,* opublikowany 24 września 2018 r. na stronie Ministerstwa Cyfryzacji.

4. WNIOSKI

Kierownicy podmiotów leczniczych

W związku z ustaleniami kontroli oraz mając na celu właściwą ochronę i przetwarzanie danych osobowych w podmiotach leczniczych, Najwyższa Izba Kontroli formułuje następujące wnioski:

1. Analizowanie ryzyka dotyczącego ochrony danych osobowych, uwzględniającego aktualny stan wiedzy technicznej, a następnie stosowanie rozwiązań adekwatnych do ustalonych zagrożeń.
2. Przeprowadzanie regularnych szkoleń osób uczestniczących w procesach przetwarzania informacji, ze szczególnym uwzględnieniem zagrożeń bezpieczeństwa informacji, skutków naruszenia zasad bezpieczeństwa informacji, odpowiedzialności prawnej oraz stosowania środków zapewniających bezpieczeństwo informacji.
3. Nadawanie pracownikom uprawnień w systemach operacyjnych komputerów oraz systemach HIS w stopniu adekwatnym do realizowanych przez nich zadań.
4. Wprowadzenie zindywidualizowanej autoryzacji dostępu do posiadanych zasobów informatycznych.
5. Przechowywanie kopii bezpieczeństwa posiadanych zasobów informacyjnych w innym miejscu niż dane produkcyjne.
6. Zapewnienie zabezpieczeń fizycznych infrastruktury informatycznej, uniemożliwiających dostęp osób nieuprawnionych oraz zapewniających ochronę przed skutkami zdarzeń losowych (np. pożar, powódź, wichura).
7. Zapewnienie, aby osoby, które uzyskują dostęp do danych osobowych posiadały stosowne upoważniania ADO w tym zakresie.
8. Przekazywanie firmom świadczącym usługi serwisowe jedynie danych osobowych niezbędnych do usunięcia usterek oprogramowania.

Organy założycielskie szpitali

1. Objęcie nadzorem w podległych podmiotach leczniczych zagadnień związanych z ochroną danych osobowych pacjentów.

Prezes Urzędu Ochrony Danych Osobowych

1. Przeprowadzanie systemowych kontroli przestrzegania zasad ochrony danych osobowych w jednostkach z sektora ochrony zdrowia, z uwagi na przetwarzanie przez te podmioty szczególnych kategorii danych osobowych.
2. Niezwłoczne zakończenie działań związanych z przyjęciem *Kodeksu postępowania dla sektora ochrony zdrowia* oraz wprowadzenie regulacji dotyczących certyfikacji, o której mowa w art. 42 RODO.

5. WAŻNIEJSZE WYNIKI KONTROLI

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

Wymagania formalne związane z wejściem w życie RODO w 16 podmiotach leczniczych wdrożone zostały z opóźnieniem lub ich nie wprowadzono do zakończenia kontroli NIK:

- **analiza ryzyka procesów przetwarzania danych osobowych, która powinna być punktem wyjścia do przyjęcia właściwych środków do ochrony danych osobowych, w dziewięciu szpitalach została przeprowadzona po upływie od 35 do 201 dni od dnia wejścia w życie RODO, a w dwóch kolejnych impulsem do jej wykonania była dopiero kontrola NIK;**
- **w siedmiu podmiotach leczniczych wewnętrzną dokumentację, opisującą stosowane środki techniczne i organizacyjne związane z zapewnieniem bezpieczeństwa danych osobowych zaktualizowano po upływie od 37 do 263 dni od wejścia w życie nowych uregulowań, a w kolejnych czterech jej nie zaktualizowano;**
- **w siedmiu skontrolowanych szpitalach rejestr czynności przetwarzania założono dopiero od 12 do 263 dni od wejścia w życie RODO, a w jednym nie opracowano go wcale.**

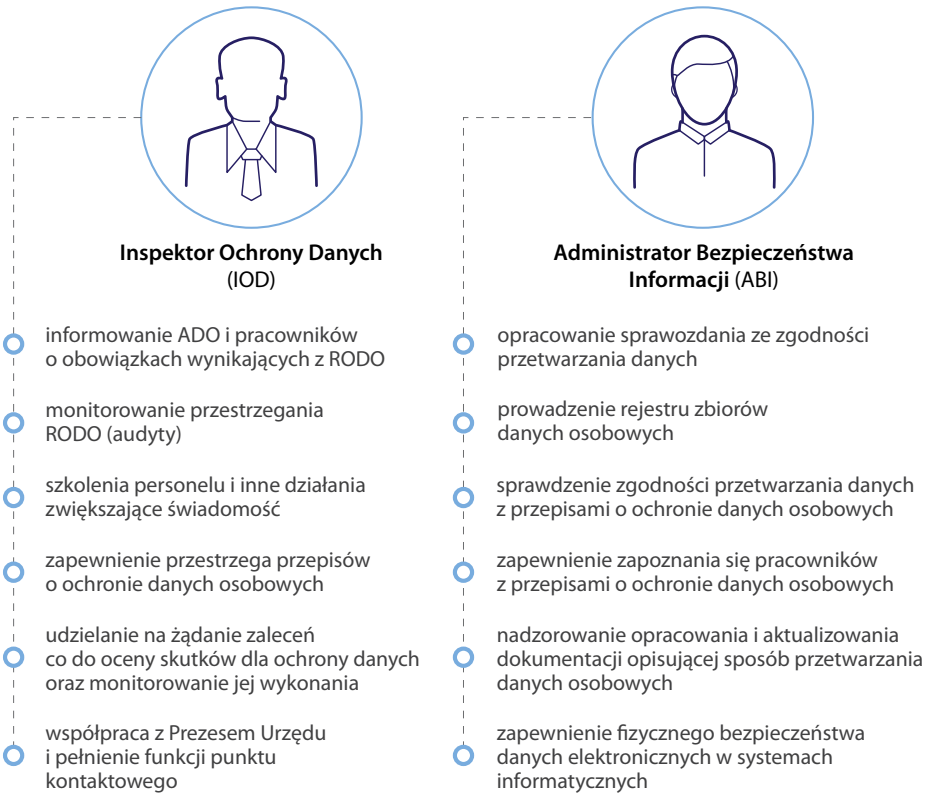
Jedną z przyczyn stwierdzonych nieprawidłowości było nieprzeszkolenie ogółu pracowników uczestniczących w procesie przetwarzania danych osobowych z zagadnień dotyczących bezpieczeństwa tych danych i obowiązywania przepisów RODO. Tylko w dziewięciu szpitalach przeszkolono prawie wszystkich pracowników (co najmniej 95%).

W każdym skontrolowanym podmiocie leczniczym wywiązano się natomiast z obowiązku wyznaczenia inspektorów ochrony danych, posiadających właściwe kompetencje i niezależność w wykonywaniu swoich obowiązków.

Wyznaczenie IOD

Wejście w życie RODO spowodowało szereg zmian w organizacji systemu ochrony danych osobowych. Jedną z nich było zastąpienie dotychczasowego ABI – IOD.

Infografika nr 2
Porównanie zadań realizowanych przez IOD i ABI



Źródło: Opracowanie własne NIK na podstawie wyników kontroli.

Rolą IOD jest doradzanie i weryfikacja prawidłowości wykonywania obowiązków wynikających z przepisów prawa dotyczących przetwarzania danych. Nie oznacza to przeniesienia na IOD odpowiedzialności za zgodne z prawem przetwarzanie danych osobowych. Pełną odpowiedzialność nadal ponosi ADO.

We wszystkich 24 skontrolowanych podmiotach leczniczych wywiązano się z obowiązku wyznaczenia IOD, ustalonego w art. 37 ust. 1 RODO. W 19 z nich wyznaczono go już 25 maja 2018 r., a w sześciu od 10 do 97 dni po tym dniu. Przepisy u.o.d.o. przewidywały bowiem, że osoba pełniąca 24 maja 2018 r. funkcję ABI, dzień później z mocy prawa stawała się IOD i pełniła tę funkcję do 1 września 2018 r. (art. 158 ust. 1). Dotychczasowi ABI stali się IOD w 13 skontrolowanych podmiotach leczniczych. ADO pięciu skontrolowanych podmiotów leczniczych zawiadomili Prezesa Urzędu o wyznaczeniu IOD z opóźnieniem wynoszącym od 14 do 109 dni[9] w stosunku do 14-dniowego terminu ustalonego w art. 10 ust. 1 u.o.d.o.

[9] SP ZOZ w Radzyniu Podlaskim 109 dni opóźnienia, Szpital Specjalistyczny im. Ludwika Rydygiera w Krakowie sp. z o.o. i Szpital Neuropsychiatryczny im. Prof. Mieczysława Kaczyńskiego SP ZOZ w Lublinie po 32 dni opóźnienia, Szpital Specjalistyczny im. Stanisława Staszica w Pile 25 dni opóźnienia, Wojewódzki Szpital Specjalistyczny im. Stefana Kardynała Wyszyńskiego SP ZOZ w Lublinie 14 dni opóźnienia.

Przykład

Powodem niedotrzymania terminu przez **Szpital Specjalistyczny im. Ludwika Rydygiera w Krakowie sp. z o.o.** były problemy techniczne związane z niemożliwością wysłania zgłoszenia wymaganą drogą elektroniczną. Zgłoszenie wysłano więc drogą papierową 32 dni po terminie, określonym w art. 10 u.o.d.o., a 8 października 2018 r. do szpitala wpłynęło pismo Prezesa Urzędu, który zwrócił się o dokonanie zgłoszenia w wymaganej, elektronicznej formie. Ostatecznie zgłoszenia takiego dokonano 143 dni po terminie.

Obowiązkiem ADO, wskazanym w art. 37 ust. 7 RODO, jest opublikowanie danych IOD oraz sposobu i formy kontaktu. W większości skontrolowanych podmiotów leczniczych obowiązek ten został spełniony. Tylko dwa szpitale[10] nie opublikowały danych IOD na swoich stronach internetowych, a trzeci[11] nie podał imienia i nazwiska IOD.

IOD byli niezależni i na ogół nie występował konflikt interesów z innymi ich obowiązkami

W każdym skontrolowanym podmiocie leczniczym IOD umożliwiono wykonywanie obowiązków w sposób niezależny, tj. stosownie do wymogu z art. 38 ust. 3 RODO. W dwóch z nich funkcję IOD pełnił podmiot zewnętrzny, specjalizujący się w tego typu usługach, a w kolejnych trzynastu IOD pełnił dodatkowo inne funkcje w szpitalu.

Przykłady

W **Specjalistycznym Psychiatrycznym ZOZ w Suwałkach** IOD część etatu pracował na stanowisku pracownika ds. administracyjnych.

W **Szpitalu Specjalistycznym im. Ludwika Rydygiera w Krakowie** sp. z o.o. IOD był z kolei administratorem aplikacji i systemów bazodanowych.

W **Szpitalu Specjalistycznym im. Stanisława Staszica w Pile** IOD był też specjalistą ds. obronności i archiwizacji.

Sytuacja taka była możliwa, o ile nie powodowała konfliktu interesów. Oznacza to, że IOD nie mógł zajmować w szpitalu stanowiska pociągającego za sobą określanie sposobów i celów przetwarzania danych[12]. Konflikt taki występował jedynie w **Wielkopolskim Centrum Onkologii im. Marii Skłodowskiej-Curie w Poznaniu**, w którym IOD był jednocześnie kierownikiem Działu Informatyki. W trakcie kontroli zmianie uległ zakres obowiązków kierownika Działu Informatyki, z którego usunięto zapisy odwołujące się do brania udziału w określaniu celów i sposobów przetwarzania danych osobowych.

Skontrolowane szpitale nie zostały dotychczas operatorami usług kluczowych

Do zakończenia kontroli żaden ze skontrolowanych szpitali nie został uznany przez Ministerstwo Zdrowia za operatora usługi kluczowej, o którym mowa w art. 5 ust. 1 u.o.k.s.c. Operator takiej usługi zobowiązany jest do powołania wewnętrznych struktur odpowiedzialnych za cyberbezpieczeństwo oraz szeregu innych obowiązków opisanych w rozdziale trzecim powołanej ustawy takich, jak np.: [1] prowadzenie systematycznego sza-

[10] Specjalistyczny Psychiatryczny ZOZ w Suwałkach, Szpital Miejski Specjalistyczny im. Gabriela Narutowicza w Krakowie.

[11] Wojewódzki Szpital dla Nerwowo i Psychicznie Chorych „Dziekanka" im. Aleksandra Piotrowskiego w Gnieźnie.

[12] Z dokumentu „Wytyczne dotyczące inspektorów ochrony danych ('DPO')", opracowanego przez Grupę Roboczą art. 29 ds. Ochrony Danych.

cowania ryzyka wystąpienia incydentu, [2] zbieranie informacji o zagrożeniach cyberbezpieczeństwa, [3] przeprowadzanie co najmniej raz na dwa lata audytu bezpieczeństwa systemu informacyjnego.

W prawie połowie skontrolowanych szpitali z opóźnieniem zaktualizowano wewnętrzną dokumentację związaną z bezpieczeństwem i przetwarzaniem danych

Zgodnie z motywem 78 RODO, ochrona praw i wolności osób fizycznych w związku z przetwarzaniem danych osobowych wymaga wdrożenia odpowiednich środków technicznych i organizacyjnych. Zobowiązany jest do tego ADO (art. 24 ust. 1 RODO).

W 11 skontrolowanych podmiotach leczniczych (46%), według stanu na dzień wejścia w życie RODO, nie były zaktualizowane podstawowe dokumenty opisujące bezpieczeństwo danych i sposoby ich przetwarzania. W siedmiu z nich (29,2% objętych kontrolą)[13] aktualizację wewnętrznej dokumentacji dokonano z opóźnieniem, a w czterech[14] (16,7%) do zakończenia kontroli NIK nadal jej nie zaktualizowano.

Elementami wymagającymi zmian były m.in. te, które dotyczyły: powołania IOD w miejsce ABI, wprowadzenia prawa do sprostowania i usunięcia danych (art. 16 i art. 17 RODO), prawa do ograniczenia przetwarzania (art. 18 RODO), obowiązku powiadamiania o sprostowaniu lub usunięciu danych osobowych bądź o ograniczeniu przetwarzania (art. 19 RODO), uwzględniania ochrony danych osobowych w fazie projektowania, domyślnej ochrony danych (art. 25 RODO), rejestrowania czynności przetwarzania (art. 30 RODO), obowiązku zgłaszania naruszenia ochrony danych osobowych organowi nadzorczemu (art. 33 RODO), prowadzenia oceny skutków dla ochrony danych osobowych (art. 35 RODO).

Przykłady

W **Szpitalu Neuropsychiatrycznym im. Prof. Mieczysława Kaczyńskiego SP ZOZ w Lublinie** opóźnienia spowodowane były zobowiązaniem IOD do zakończenia bieżących spraw służbowych, w związku ze zmianą stanowiska oraz koniecznością przeprowadzenia procesu rekrutacji i zatrudnienia na jego miejsce nowego pracownika, a po przejściu na nowe stanowisko, IOD musiał mieć czas na wdrożenie się do nowych obowiązków. Następnie pomiędzy listopadem 2018 r. a styczniem 2019 r. nie był obecny w pracy. Według stanu na dzień zakończenia kontroli w Szpitalu rozpoczęto prace nad aktualizacją Polityki Bezpieczeństwa i Instrukcji Zarządzania Systemami Informatycznym.

W **Szpitalu Wojewódzkim im. Mikołaja Kopernika w Koszalinie** aktualizacja wewnętrznej dokumentacji nie została wykonana, mimo że 31 sierpnia 2018 r. powołany został do tego celu specjalny zespół. Opóźnienia wyjaśniano złożonością zagadnień prawnych, brakiem aktów wykonawczych, okresami urlopowymi pracowników i dużą ilością przetwarzanych danych osobowych.

13 SP ZOZ w Augustowie po 263 dniach, Szpital Ogólny w Kolnie po 255 dniach, Niepubliczny ZOZ Szpital im. prof. Z. Religi w Słubicach sp. z o.o. po 234 dniach, Szpital Specjalistyczny im. Stanisława Staszica w Pile po 152 dniach, Szpital im. E. Szczeklika w Tarnowie po 102 dniach, Powiatowe Centrum Zdrowia sp. z o.o. Szpital Powiatowy w Drezdenku po 67 dniach, Samodzielny Publiczny Wielospecjalistyczny ZOZ w Stargardzie po 37 dniach od wejścia w życie RODO.

14 SP ZOZ w Kole, SP ZOZ w Radzyniu Podlaskim, Szpital Neuropsychiatryczny im. prof. Mieczysława Kaczyńskiego SP ZOZ w Lublinie, Szpital Wojewódzki im. Mikołaja Kopernika w Koszalinie.

Należy mieć na uwadze, że RODO zostało uchwalone 27 kwietnia 2016 r. i ustanowione zostało 25-miesięczne *vacatio legis* w celu właściwego przygotowania się do nowego stanu prawnego podmiotów zobowiązanych do ochrony przetwarzanych danych. Opóźnienia w opracowaniu zaktualizowanych dokumentów wewnętrznych opisujących bezpieczeństwo danych i sposoby ich przetwarzania nie można zatem tłumaczyć bieżącymi działaniami lub wydarzeniami mającymi miejsce po wejściu w życie RODO.

Regulaminy organizacyjne części szpitali nie uwzględniały w strukturze organizacyjnej stanowiska IOD

Z opóźnieniem zaktualizowano również regulaminy organizacyjne skontrolowanych szpitali w związku ze zmianą struktury organizacyjnej i powołaniem IOD. W dziewięciu[15] podmiotach leczniczych (37,5%) w dniu powołania inspektora regulaminy nie uwzględniały takiej funkcji. Jedynymi dokumentami opisującymi zadania IOD były ich zakresy czynności. W dniu zakończenia kontroli w trzech[16] szpitalach nadal nie zaktualizowano regulaminów organizacyjnych.

Przykłady

W **Szpitalu Miejskim Specjalistycznym im. Gabriela Narutowicza w Krakowie** zdaniem dyrektora IOD to funkcja, a nie stanowisko. Stąd nie zostało ono wymienione w regulaminie organizacyjnym szpitala.

W **Powiatowym Centrum Zdrowia sp. z o.o. Szpitalu Powiatowym w Drezdenku** regulamin organizacyjny jest ściśle powiązany ze statutem Powiatowego Centrum Zdrowia sp. z o.o., którego zmiana wymaga podjęcia uchwały przez zgromadzenie wspólników. W związku z tym, że wszystkie udziały w spółce należą do powiatu strzelecko-drezdeneckiego, prace związane z dostosowaniem dokumentów do obowiązujących aktów prawnych zostały zawieszone na czas ukonstytuowania się nowych władz samorządowych. NIK zauważa jednak, że wybory samorządowe odbyły się 21 października 2018 r., tj. 149 dni po wejściu w życie RODO, co dawało wystarczająco dużo czasu na aktualizację regulaminu organizacyjnego i statutu szpitala przez poprzednie władze samorządowe.

Podobna przyczyna niezawarcia w strukturze organizacyjnej stanowiska IOD wystąpiła w **Szpitalu im. E. Szczeklika w Tarnowie**, gdzie zmian dokonuje Rada Miasta Tarnowa.

Rejestr czynności przetwarzania nie został opracowany na czas w prawie ⅓ skontrolowanych podmiotów leczniczych

Rejestr czynności przetwarzania zastąpił rejestry zbiorów danych osobowych, prowadzone do 25 maja 2018 r. na podstawie przepisów dawnej u.o.d.o. Powinien on stanowić kompleksową ewidencję wszystkich operacji realizowanych przez szpitale na danych osobowych. W poprzednim stanie prawnym podmioty lecznicze nie miały obowiązku rejestracji zbiorów zawierających dane osób korzystających z usług medycznych[17], co uległo zmianie w związku z wejściem w życie RODO.

[15] Lubuski Szpital Specjalistyczny Pulmonologiczno-Kardiologiczny w Torzymiu sp. z o. o., Powiatowe Centrum Zdrowia Sp. z o.o. Szpital Powiatowy w Drezdenku, SP ZOZ w Radzyniu Podlaskim, Szpital im. E. Szczeklika w Tarnowie, Szpital Miejski Specjalistyczny im. Gabriela Narutowicza w Krakowie, Szpital Specjalistyczny im. Ludwika Rydygiera w Krakowie sp. z o.o., Wielkopolskie Centrum Onkologii im. Marii Skłodowskiej-Curie w Poznaniu, Wojewódzki Specjalistyczny Szpital Dziecięcy im. św. Ludwika w Krakowie, Specjalistyczny Psychiatryczny ZOZ w Suwałkach.

[16] Powiatowe Centrum Zdrowia Sp. z o.o. Szpital Powiatowy w Drezdenku, Szpital im. E. Szczeklika w Tarnowie, Szpital Miejski Specjalistyczny im. Gabriela Narutowicza w Krakowie.

[17] Art. 43 ust. 1 pkt 5 ustawy z dnia 29 sierpnia 1997 r. o ochronie danych osobowych (Dz. U. z 2016 r. poz. 922, ze zm.), według stanu prawnego na 24 maja 2018 r.

Większość skontrolowanych szpitali wywiązała się z obowiązku założenia i prowadzenia rejestru czynności przetwarzania, jednak sześć[18] podmiotów leczniczych (25%) rejestr ten założyło z opóźnieniem, tj. od 12 do 263 dni po wejściu w życie RODO. W **Specjalistycznym Psychiatrycznym ZOZ w Suwałkach** rejestru nie założono zaś do końca kontroli NIK, co argumentowano zmianą na stanowisku IOD oraz dużą ilością innych obowiązków.

W trzech szpitalach rejestr prowadzono nierzetelnie

W trzech skontrolowanych szpitalach (12,5%) rejestr prowadzony był nierzetelnie.

Przykłady

W **Szpitalu Wojewódzkim im. Mikołaja Kopernika w Koszalinie** w prowadzonym rejestrze nie uwzględniono elementu wymaganego przepisami art. 30 ust 1 lit. a RODO, tj. informacji zawierającej imię i nazwisko lub nazwę oraz dane kontaktowe administratora oraz wszelkich współadministratorów, a także – gdy ma to zastosowanie – przedstawiciela administratora oraz IOD. Jednocześnie rejestr nie był prowadzony w wymaganej formie elektronicznej, a jedynie papierowej.

W **Szpitalu Neuropsychiatrycznym im. Prof. Mieczysława Kaczyńskiego SP ZOZ w Lublinie** rejestr czynności przetwarzania nie zawierał m.in. czynności związanych z przetwarzaniem danych osobowych pacjentów (oprócz realizacji recept), jak również nie uwzględniono w nim wszystkich czynności wskazanych w informacjach złożonych do IOD przez kierowników poszczególnych oddziałów szpitala.

Błędy formalne podczas zawierania umów powierzenia przetwarzania danych osobowych

Regulacje art. 28 RODO wprowadziły wyraźny i jednoznaczny obowiązek zawierania pisemnych umów powierzenia przetwarzania danych[19], określających przedmiot, czas trwania oraz charakter i cel przetwarzania, rodzaj danych osobowych oraz kategorie osób, których dane dotyczą, a także obowiązki i prawa administratora. W związku z tym skontrolowane szpitale zawarły 1366 umów powierzenia przetwarzania danych, w tym 898 jako administratorzy danych i 468 jako podmioty je przetwarzające. W pięciu[20] podmiotach leczniczych (21%) stwierdzono błędy w tym zakresie.

Przykłady

W **Samodzielnym Publicznym Szpitalu dla Nerwowo i Psychicznie Chorych w Międzyrzeczu** nie zawarto dwóch umów powierzenia przetwarzania danych, w których szpital powinien wystąpić jako administrator danych. W obu przypadkach podmioty przetwarzające odmówiły podpisania umów: jeden

[18] SP ZOZ w Augustowie 263 dni opóźnienia, Białostockie Centrum Onkologii im. M. Skłodowskiej-Curie w Białymstoku 201 dni opóźnienia, SP ZOZ w Radzyniu Podlaskim 60 dni opóźnienia, Szpital im. E. Szczeklika w Tarnowie 46 dni opóźnienia, Szpital Neuropsychiatryczny im. prof. Mieczysława Kaczyńskiego Samodzielny Publiczny Zakład Opieki Zdrowotnej w Lublinie 34 dni opóźnienia, Szpital Wojewódzki im. Mikołaja Kopernika w Koszalinie 12 dni opóźnienia.

[19] Jako pisemna wskazana została także umowa w formie elektronicznej. Przetwarzanie danych osobowych przez podmiot przetwarzający odbywa się na podstawie umowy lub innego instrumentu prawnego, które podlegają prawu Unii Europejskiej lub prawu państwa członkowskiego i wiążą podmiot przetwarzający i administratora.

[20] Białostockie Centrum Onkologii im. M. Skłodowskiej-Curie w Białymstoku, Niepubliczny ZOZ Szpital im. prof. Z. Religi w Słubicach sp. z o.o., Samodzielny Publiczny Szpital dla Nerwowo i Psychicznie Chorych w Międzyrzeczu, Specjalistyczny Psychiatryczny ZOZ w Suwałkach, Zachodniopomorskie Centrum Onkologii w Szczecinie.

uzasadniał to tym, że jako sieć ogólnopolska przygotuje własny wzór umowy powierzenia przetwarzania danych, z drugim podmiotem szpital podejmie dalsze kroki w celu zawarcia umowy.

W **Niepublicznym ZOZ Szpitalu im. prof. Z. Religi w Słubicach Sp. z o.o.** przez przeoczenie nie zawarto czterech umów powierzenia przetwarzania danych. Dotyczyło to zlecanych usług zdrowotnych lub przekazywanych poza szpital wyników badań pacjentów.

W **Zachodniopomorskim Centrum Onkologii w Szczecinie** nie przestrzegano własnych uregulowań podczas zawierania umów powierzenia przetwarzania danych. W czterech z 16 analizowanych umów odstąpiono od zawarcia umowy według wzoru stanowiącego załącznik do „Polityki RODO", a jedynie rozszerzono umowy podstawowe z kontrahentami o zapisy dotyczące tej kwestii. Jednocześnie nierzetelnie prowadzono rejestr umów powierzenia przetwarzania danych, w którym nie zostały zamieszczone umowy z 14 podmiotami.

Analiza ryzyka procesów przetwarzania danych osobowych powinna być punktem wyjścia do przyjęcia właściwych środków do ochrony danych osobowych

W art. 32 RODO wskazano na obowiązek wdrożenia odpowiednich środków technicznych i organizacyjnych, aby zapewnić stopień bezpieczeństwa odpowiadający stwierdzonemu ryzyku. Wiązało się to z przeprowadzeniem analizy ryzyka procesów przetwarzana danych osobowych, wynikającego z przypadkowego lub niezgodnego z prawem zniszczenia, utraty, modyfikacji, nieuprawnionego ujawnienia lub nieuprawnionego dostępu do danych osobowych przesyłanych, przechowywanych albo w inny sposób przetwarzanych.

Do 25 maja 2018 r. analizę taką przeprowadzono w trzynastu[21] skontrolowanych szpitalach (54,2%), w kolejnych dziewięciu wykonano ją do końca 2018 r., a w dwóch pozostałych (**SP ZOZ w Augustowie i Szpital Neuropsychiatryczny im. prof. Mieczysława Kaczyńskiego SP ZOZ w Lublinie**) impulsem do jej przeprowadzenia była dopiero kontrola NIK. RODO nie precyzowało kiedy analiza miałaby zostać przeprowadzona i w jakiej formie. Bez wątpienia jednak należało wykonać ją w terminie umożliwiającym podjęcie właściwych decyzji dotyczących zapewnienia środków technicznych i organizacyjnych związanych z bezpieczeństwem danych osobowych wraz z wejściem w życie RODO. Zwlekanie z tym obowiązkiem oddziaływało niekorzystnie na poziom bezpieczeństwa danych osobowych, co opisano szerzej w punkcie 5.2. Informacji.

Przykład

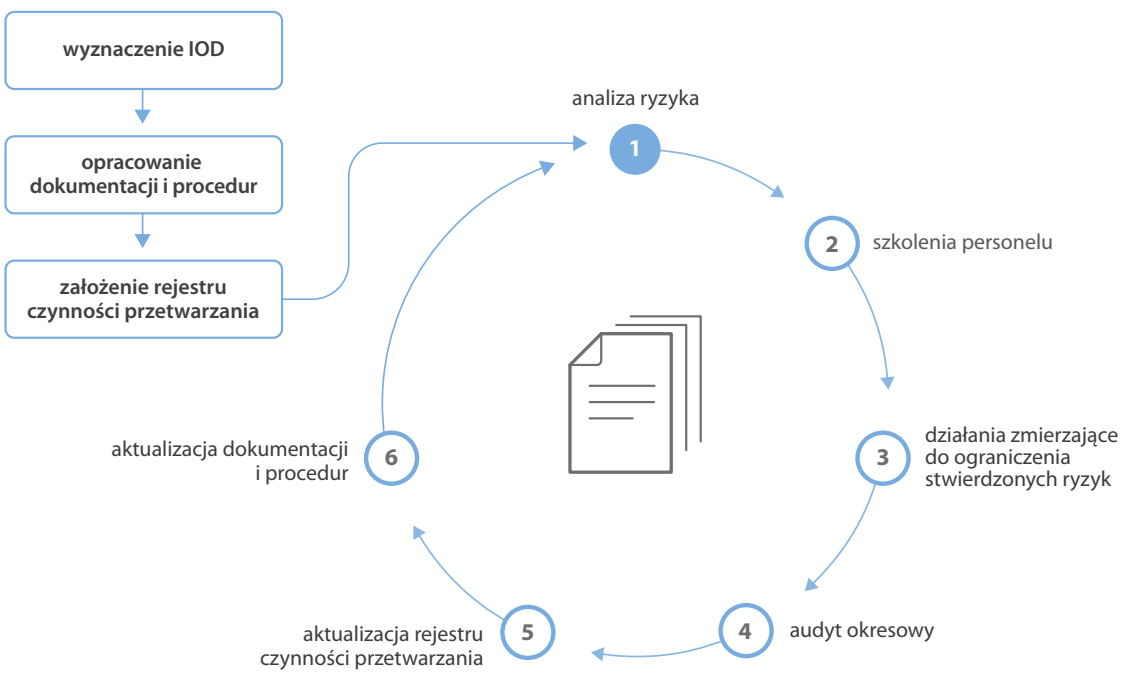
W **Wojewódzkim Szpitalu dla Nerwowo i Psychicznie Chorych „Dziekanka" im. Aleksandra Piotrowskiego w Gnieźnie** analiza ryzyka procesów przetwarzana danych osobowych obejmowała zasoby systemu teleinformatycznego i czynnik ludzki (14 rodzajów zasobów), a także zagro-

[21] Lubuski Szpital Specjalistyczny Pulmonologiczno-Kardiologiczny w Torzymiu sp. z o.o., Niepubliczny ZOZ Szpital im. prof. Z. Religi w Słubicach sp. z o.o., Samodzielny Publiczny Wielospecjalistyczny ZOZ w Stargardzie, SP ZOZ w Kole, SP ZOZ w Kraśniku, Specjalistyczny Psychiatryczny ZOZ w Suwałkach, Szpital im. E. Szczeklika w Tarnowie, Szpital Miejski Specjalistyczny im. Gabriela Narutowicza w Krakowie, Szpital Specjalistyczny im. Ludwika Rydygiera w Krakowie sp. z o.o., Szpital w Dębnie im. Świętej Matki Teresy z Kalkuty sp. z o. o., Wojewódzki Szpital dla Nerwowo i Psychicznie Chorych „Dziekanka" im. Aleksandra Piotrowskiego w Gnieźnie, Wojewódzki Szpital Specjalistyczny im. Stefana Kardynała Wyszyńskiego SP ZOZ w Lublinie, Zachodniopomorskie Centrum Onkologii w Szczecinie.

żenia ze strony sił natury oraz celowych i przypadkowych działań człowieka (35 rodzajów zagrożeń), które mogłyby spowodować ujawnienie lub utratę danych osobowych z zasobu Szpitala. W celu identyfikacji podatności na ryzyko opracowano listę potencjalnych słabych punktów systemu bezpieczeństwa informacji. Poziom podatności określono odrębnie dla ochrony: poufności, integralności i dostępności, w 5-stopniej skali z punktacją od 1 do 10 (brak – 0, niski poziom od 1 do 4, średni poziom od 5 do 7, wysoki poziom od 8 do 9, ekstremalny poziom – 10). Dla każdego z ryzyk określono prawdopodobieństwo zaistnienia i skutek, szacując ich wartość. Analiza wykazała, że najsłabszym ogniwem w systemie bezpieczeństwa przetwarzania danych osobowych był czynnik ludzki. Największą wartość ryzyka oszacowano dla ochrony dostępności, w tym kradzieży informacji zawierającej dane osobowe, kradzieży urządzeń i sprzętu mobilnego, nieuprawnionego kopiowania danych, użycia fałszywego oprogramowania, nielegalnego przetwarzanie danych, awarii, niewłaściwego działania urządzeń i utraty zasilania elektrycznego.

Analiza przeprowadzona w **Niepublicznym ZOZ Szpitalu im. prof. Z. Religi w Słubicach sp. z o.o.** nie była kompletna. Nie objęła bowiem wszystkich operacji przetwarzania danych, tj. na terminalu informatycznym, za pomocą którego przekazywano wyniki badań przesiewowych słuchu u noworodków (wraz z danymi matki i dziecka) i przetwarzanych w formie papierowej zleceń transportu medycznego.

Infografika nr 3
Schemat procesu postępowania w związku z analizą ryzyka procesów przetwarzania danych w jednostce



Źródło: Opracowanie własne NIK na podstawie zapisów RODO.

Zalecane było wykonanie oceny skutków dla ochrony danych

Kolejnym nowym elementem związanym z wejściem w życie RODO było przeprowadzenie oceny skutków dla ochrony danych – DPIA (art. 35). Obowiązek dokonywania tej oceny występował zawsze przed rozpoczęciem przetwarzania nowych kategorii danych, w szczególności z użyciem nowych technologii i przetwarzania na dużą skalę szczególnych kategorii danych

osobowych[22]. Dotyczył zatem operacji rozpoczętych po 25 maja 2018 r., a w przypadku wcześniejszych – tylko gdy doszło do istotnej zmiany przetwarzania danych (np. przez wprowadzenie nowej technologii, wykorzystywanie danych w innym celu lub rozpoczęcie ich transferu do innych państw). Ocena taka była zaś fakultatywna, gdy szpital nie rozpoczął przetwarzania nowych kategorii danych po wejściu w życie RODO. Grupa Robocza ds. Ochrony Danych zdecydowanie zalecała jednak[23] dokonanie DPIA dla operacji przetwarzania trwających przed 25 maja 2018 r., a także, gdy nie jest jasne, czy DPIA jest wymagana. Uznano bowiem, że jest ona „przydatnym narzędziem, które może pomóc administratorom danych w zapewnieniu zgodności z prawem ochrony danych".

Ocena skutków dla ochrony danych przeprowadzona została w 12 skontrolowanych szpitalach (50%): do 25 maja 2018 r. w pięciu[24] (20,8%), do końca 2018 r. – w czterech[25] (16,7%), a w trzech w 2019 r.[26] (12,5%), tj. w trakcie kontroli NIK. DPIA w tych przypadkach nie były związane z rozpoczęciem przetwarzania nowych kategorii danych, a były m.in. elementem audytu wewnętrznego[27] dla wybranego elementu związanego z przetwarzaniem danych[28] lub realizację wytycznych Grupy Roboczej art. 29 ds. ochrony danych osobowych. Oceny skutków dla ochrony danych w dwóch[29] szpitalach, które zdecydowały się je wykonać, były niepełne. Nie zawierały – przewidzianej w art. 35 ust. 1 RODO – oceny, czy operacje przetwarzania są niezbędne oraz proporcjonalne w stosunku do celów oraz oceny ryzyka naruszenia praw lub wolności osób, których dane dotyczą. W dwunastu pozostałych podmiotach leczniczych oceny skutków dla ochrony danych nie przeprowadzono, gdyż nie zaszły okoliczności nakazujące jej wykonanie.

Przeszkolonych zostało 69% pracowników szpitali

Jednym z najistotniejszych elementów przygotowania podmiotu leczniczego do nowego stanu prawnego wraz z wejściem w życie RODO było przeszkolenie personelu. Zadanie to, w myśl art. 39 ust. 1 lit. b RODO, było przypisane IOD. Pomimo 25-miesięcznego *vacatio legis* ustalonego dla RODO, we wszystkich skontrolowanych szpitalach tylko 11 017 z 15 964 pracowników (69%) przeszkolono z przepisów RODO i bezpie-

22 Określone w art. 9 ust. 1 RODO, czyli m.in.: informacje o stanie zdrowia i dane genetyczne.

23 Wytyczne WP 248, przyjęte 4 kwietnia 2017 r. i zmienione 4 października 2017 r.

24 Powiatowe Centrum Zdrowia sp. z o.o. Szpital Powiatowy w Drezdenku, SP ZOZ w Kraśniku, Szpital im. E. Szczeklika w Tarnowie, Wojewódzki Szpital Specjalistyczny im. Stefana Kardynała Wyszyńskiego SP ZOZ w Lublinie, Zachodniopomorskie Centrum Onkologii w Szczecinie.

25 Białostockie Centrum Onkologii im. M. Skłodowskiej-Curie w Białymstoku, Niepubliczny ZOZ Szpital im. prof. Z. Religi w Słubicach sp. z o.o., Szpital Specjalistyczny im. Stanisława Staszica w Pile, Wojewódzki Specjalistyczny Szpital Dziecięcy im. św. Ludwika w Krakowie.

26 Samodzielny Publiczny Szpital dla Nerwowo i Psychicznie Chorych w Międzyrzeczu, Szpital Miejski Specjalistyczny im. Gabriela Narutowicza w Krakowie, Wielkopolskie Centrum Onkologii im. Marii Skłodowskiej-Curie w Poznaniu.

27 Powiatowe Centrum Zdrowia sp. z o.o. Szpital Powiatowy w Drezdenku, Wojewódzki Szpital Specjalistyczny im. Stefana Kardynała Wyszyńskiego SP ZOZ w Lublinie.

28 Dla systemu monitoringu wizyjnego w Powiatowym Centrum Zdrowia sp. z o.o. Szpitalu Powiatowym w Drezdenku.

29 Szpital im. E. Szczeklika w Tarnowie, Wojewódzki Specjalistyczny Szpital Dziecięcy im. św. Ludwika w Krakowie.

czeństwa danych w postaci elektronicznej. Jedynie w dziewięciu[30] podmiotów leczniczych (37,5%) szkoleniami objęto 95% personelu lub więcej. W kolejnych siedmiu[31] wskaźnik ten wynosił od 51 do 94%, a w ośmiu[32] (33,3%) przeszkolono mniej niż połowę osób. Szkolenia częściowo zastępowano tam samodzielnym zapoznaniem się pracowników z wewnętrznymi uregulowaniami dotyczącymi ochrony danych osobowych i złożeniem oświadczenia o poufności, w którym ten fakt potwierdzili. Zauważyć należy też, że w części podmiotów leczniczych impulsem do przeprowadzenia szkoleń było rozpoczęcie kontroli NIK. Tak było np. w SP ZOZ w Augustowie, gdzie pierwsze szkolenie personelu zostało zrealizowane trzy dni po rozpoczęciu kontroli, chociaż audytor wewnętrzny już osiem miesięcy wcześniej rekomendował takie działanie. Nieprzeszkolenie wszystkich pracowników szpitali lub opóźnienia w ich przeprowadzaniu były jedną z przyczyn nieodpowiedniego przetwarzania i ochrony danych osobowych pacjentów szpitali, opisanego w punkcie 5.2 informacji.

Przykłady

W **Szpitalu im. E. Szczeklika w Tarnowie** szkoleniami objęto jedynie 6% personelu. Argumentowano to specyfiką działalności podmiotu leczniczego, co znacząco utrudnia przeszkolenie całej kadry w jednym ustalonym terminie i proces ten wymaga realizacji etapami.

W **Wojewódzkim Szpitalu dla Nerwowo i Psychicznie Chorych „Dziekanka" im. Aleksandra Piotrowskiego w Gnieźnie** przeszkolono 9% pracowników. Motywowano to tym, że plan szkoleń na 2018 r. obejmował 41 innych szkoleń specjalistycznych związanych z informatyzacją dla wszystkich grup zawodowych. Nie było więc możliwości przeszkolenia większej liczby pracowników szpitala z zakresu przepisów RODO, bez zaburzenia jego normalnego toku funkcjonowania.

W **Niepublicznym ZOZ Szpitalu im. prof. Z. Religi w Słubicach sp. z o.o.** przeszkolono 14% pracowników. Problemem było zebranie personelu medycznego na szkolenie i zdecydowano się na e-learning. IOD nie zwracał jednak uwagi na sposób dokumentowania realizowanych szkoleń. Na stronie intranetowej szpitala zamieszczono materiały szkoleniowe i informacyjne dla personelu, lecz IOD nie posiadał informacji ile osób faktycznie skorzystało z tej formy szkolenia.

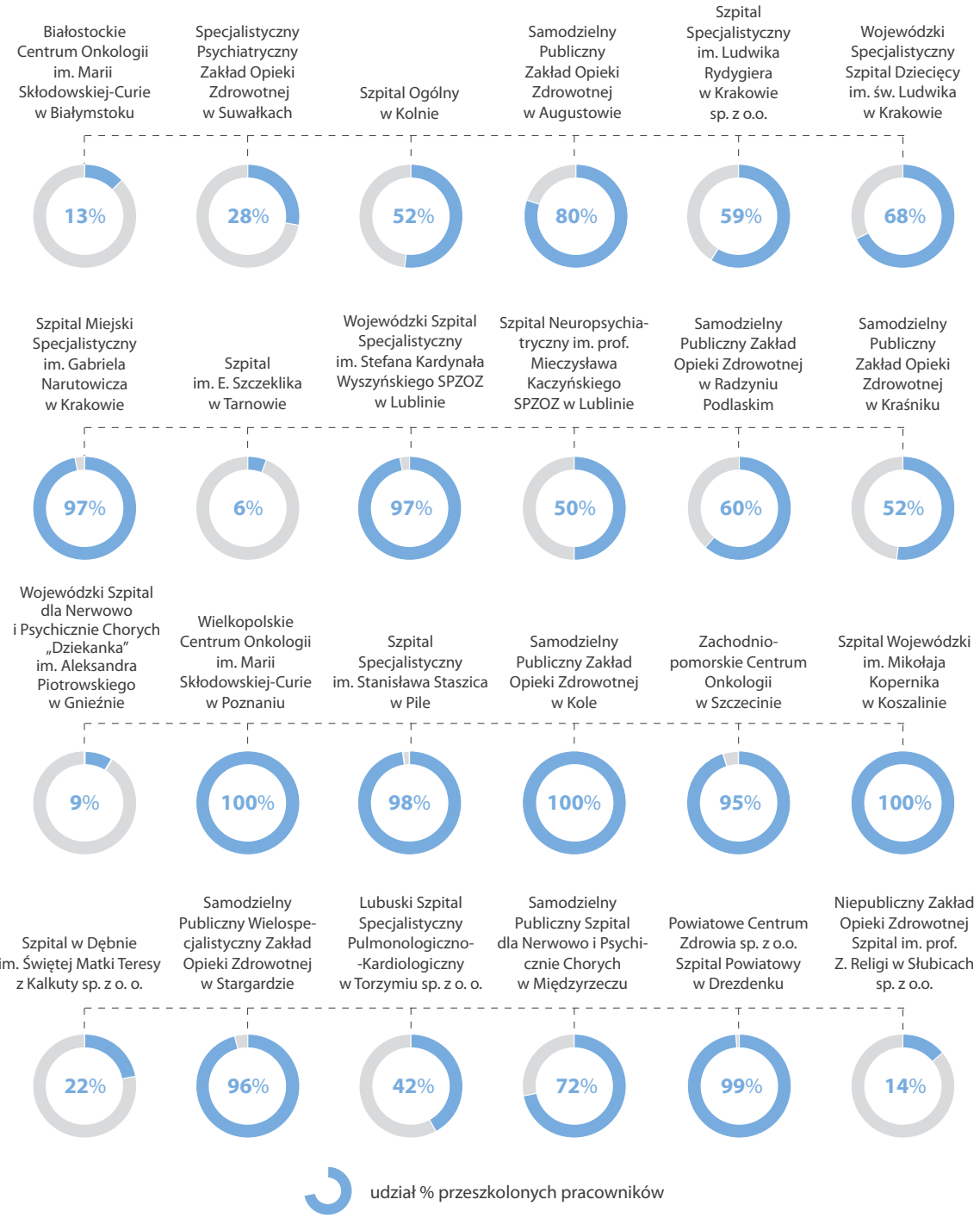
[30] Powiatowe Centrum Zdrowia sp. z o.o. Szpital Powiatowy w Drezdenku, Samodzielny Publiczny Wielospecjalistyczny ZOZ w Stargardzie, SP ZOZ w Kole, Szpital Miejski Specjalistyczny im. Gabriela Narutowicza w Krakowie, Szpital Specjalistyczny im. Stanisława Staszica w Pile, Szpital Wojewódzki im. Mikołaja Kopernika w Koszalinie, Wielkopolskie Centrum Onkologii im. Marii Skłodowskiej-Curie w Poznaniu, Wojewódzki Szpital Specjalistyczny im. Stefana Kardynała Wyszyńskiego SP ZOZ w Lublinie, Zachodniopomorskie Centrum Onkologii w Szczecinie.

[31] SP ZOZ w Augustowie – 80% pracowników przeszkolonych, Samodzielny Publiczny Szpital dla Nerwowo i Psychicznie Chorych w Międzyrzeczu – 72% przeszkolonych, Wojewódzki Specjalistyczny Szpital Dziecięcy im. św. Ludwika w Krakowie – 68% przeszkolonych, SP ZOZ w Radzyniu Podlaskim – 60% przeszkolonych, Szpital Specjalistyczny im. Ludwika Rydygiera w Krakowie sp. z o.o. – 59% przeszkolonych, Szpital Ogólny w Kolnie, SP ZOZ w Kraśniku – po 52% przeszkolonych.

[32] Białostockie Centrum Onkologii im. M. Skłodowskiej-Curie w Białymstoku, Lubuski Szpital Specjalistyczny Pulmonologiczno-Kardiologiczny w Torzymiu sp. z o. o., Niepubliczny ZOZ Szpital im. prof. Z. Religi w Słubicach sp. z o.o, Specjalistyczny Psychiatryczny ZOZ w Suwałkach, Szpital im. E. Szczeklika w Tarnowie, Szpital Neuropsychiatryczny im. prof. Mieczysława Kaczyńskiego SP ZOZ w Lublinie, Szpital w Dębnie im. Świętej Matki Teresy z Kalkuty sp. z o. o., Wojewódzki Szpital dla Nerwowo i Psychicznie Chorych „Dziekanka" im. Aleksandra Piotrowskiego w Gnieźnie.

Infografika nr 4

Szkolenia personelu w kontrolowanych podmiotach leczniczych



Źródło: Opracowanie własne NIK na podstawie wyników kontroli.

W artykule 40 RODO wskazano, że: „państwa członkowskie, organy nadzorcze, Europejska Rada Ochrony Danych oraz Komisja zachęcają do sporządzania kodeksów postępowania mających pomóc we właściwym stosowaniu tego rozporządzenia". Jednocześnie wskazano możliwość opracowania lub zmiany kodeksów postępowania bądź rozszerzania ich zakresu, przez podmioty reprezentujące określone kategorie administratorów (np. szpitale), celem doprecyzowania sposobu stosowania RODO. Pożądanym – aczkolwiek

Dotychczas nie został zaakceptowany kodeks postępowania dla sektora ochrony zdrowia

nie obligatoryjnym – stanem było zatem kierowanie się określonymi standardami pracy, które mogły być opisane w kodeksie dobrych praktyk, medycznym kodeksie branżowym lub innym dokumencie. Przykładem jest Przewodnik po RODO dla służby zdrowia, będący efektem prac zespołu zadaniowego ds. ochrony zdrowia, działającego w ramach Grupy Roboczej ds. Ochrony Danych Osobowych, utworzonej w Ministerstwie Cyfryzacji, który został opublikowany 24 września 2018 r. na stronie internetowej Ministerstwa Cyfryzacji[33]. Innym przykładem regulacji w tym zakresie jest *Kodeks postępowania dla sektora ochrony zdrowia,* który zawiera zbiór zasad zgodnych z RODO i ustawodawstwem krajowym, dotyczącym podnoszenia poziomu ochrony osób fizycznych w związku z przetwarzaniem danych osobowych. Wniosek o przyjęcie projektu kodeksu branżowego został 13 listopada 2018 r. złożony przez jego autorów do Prezesa Urzędu i nie został dotychczas zatwierdzony.

W Przewodniku po RODO dla służby zdrowia wskazano kilka przykładów rozwiązań, które ułatwiają zachowanie w poufności danych medycznych pacjentów.

Infografika nr 5
Zalecenia dotyczące standardów pracy, zawarte w przewodniku po RODO

Źródło: Opracowanie własne NIK na podstawie przewodnika po RODO.

[33] https://www.gov.pl/cyfryzacja/rodo-w-sluzbie-zdrowia-po-pierwsze-pacjent, [dostęp z 3 października 2018 r.].

W dziesięciu[34] skontrolowanych podmiotach leczniczych (42%) stosowano wspomniany kodeks lub przewodnik po RODO. W większości z nich dokumenty te zostały udostępnione w katalogu sieciowym szpitala, do którego dostęp posiadali pracownicy.

Przewodnik po RODO autorstwa Ministerstwa Cyfryzacji nie zawsze był przyjęty do stosowania

Kierownicy skontrolowanych szpitali wskazali, że głównym powodem, dla którego formalnie nie przyjęto kodeksu do stosowania lub nie kierowano się rozwiązaniami w nim zawartymi było niezatwierdzenie go przez Prezesa Urzędu.

5.2. Zapewnienie prawidłowego przetwarzania i ochrony danych osobowych

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

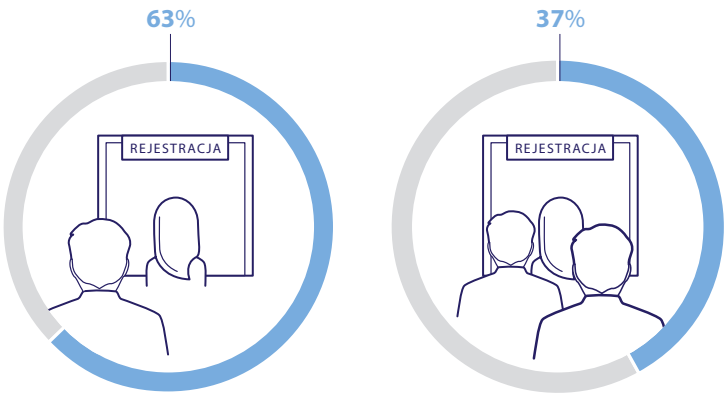
- **w 37% podmiotów leczniczych istniało ryzyko ujawnienia personaliów pacjentów lub danych zawartych w dokumentacji medycznej w trakcie rejestracji na wizytę do poradni specjalistycznej;**
- **w 13% szpitalach nie zamieszczono informacji dla pacjentów o podstawie pobierania i przetwarzania danych osobowych i prawach pacjentów związanych z przetwarzaniem ich danych;**
- **w 46% podmiotach leczniczych na opaskach indentyfikacyjnych noszonych przez pacjentów na nadgarstkach zamieszczano niezanonimizowane dane osobowe;**
- **w 37% jednostek niewłaściwie przechowywano papierową dokumentację medyczną pacjentów;**
- **w 33% szpitali pielęgniarki posiadały przyznane w systemie informatycznym zbyt szerokie uprawnienia do danych pacjentów;**
- **części personelu medycznego w 21% podmiotów leczniczych nie wydano wymaganych upoważnień do przetwarzania danych osobowych pacjentów lub nadano je wadliwie;**
- **byłym pracownikom 63% szpitali nie odbierano niezwłocznie dostępu do systemów informatycznych;**
- **w 50% podmiotów leczniczych występowały błędy w procesie zgłaszania usterek firmie świadczącej serwis systemów informatycznych oraz udostępniania kopii dokumentacji medycznej;**
- **w 75% szpitali nie przestrzegano wymogów dotyczących nadawania uprawnień w systemach informatycznych, ochrony przed złośliwym oprogramowaniem, dostępu ograniczonego hasłem;**
- **w 21% podmiotach leczniczych kopie bezpieczeństwa danych były przechowywane w niewłaściwym miejscu.**

[34] Lubuski Szpital Specjalistyczny Pulmonologiczno-Kardiologiczny w Torzymiu sp. z o.o., Niepubliczny ZOZ Szpital im. prof. Z. Religi w Słubicach sp. z o.o., Powiatowe Centrum Zdrowia sp. z o.o. Szpital Powiatowy w Drezdenku, Samodzielny Publiczny Szpital dla Nerwowo i Psychicznie Chorych w Międzyrzeczu, Samodzielny Publiczny Wielospecjalistyczny ZOZ w Stargardzie, SP ZOZ w Kraśniku, Szpital Specjalistyczny im. Ludwika Rydygiera w Krakowie sp. z o.o., Szpital Specjalistyczny im. Stanisława Staszica w Pile, Szpital Wojewódzki im. Mikołaja Kopernika w Koszalinie, Wojewódzki Szpital Specjalistyczny im. Stefana Kardynała Wyszyńskiego SP ZOZ w Lublinie.

W 37% skontrolowanych jednostek nie wprowadzono rozwiązań gwarantujących pacjentom zachowanie prywatności w procesie rejestracji

Organizacja procesu rejestracji[35] nie we wszystkich szpitalach gwarantowała pacjentom zachowanie ich prawa do prywatności. Dziewięć[36] szpitali (37,5%) nie zapewniło odpowiednich odległości między oknami rejestracji lub przesłon między nimi, a sześć[37] nie wyznaczyło stref oddzielających pacjentów obsługiwanych przy okienkach od reszty osób w kolejce. W trzech kolejnych podmiotach, mimo zapewnienia odpowiedniego usytuowania okien rejestracji, nie wprowadzono środków gwarantujących zachowanie odległości pomiędzy osobami rejestrującymi się i oczekującymi w kolejce.

Infografika nr 6
Udział szpitali zapewniających zachowanie prywatności podczas rejestracji



Źródło: Opracowanie własne NIK na podstawie wyników kontroli.

Nie zapewniono zatem odpowiedniej ochrony prywatności pacjentów oraz danych zawartych w dokumentacji medycznej. Istniało bowiem ryzyko ujawnienia tych informacji osobom nieuprawnionym. Stanowiło to naruszenie art. 24 ust. 1 RODO, zgodnie z którym administrator wdraża odpowiednie środki techniczne i organizacyjne, aby przetwarzanie odbywało się zgodnie z rozporządzeniem. Jednocześnie, w myśl motywu 39. preambuły oraz art. 5 ust. 1 lit. f RODO, dane osobowe powinny być przetwarzane w sposób zapewniający im odpowiednie bezpieczeństwo i odpowiednią poufność, w tym ochronę przed nieuprawnionym dostępem, niedozwolonym lub niezgodnym z prawem przetwarzaniem.

35 Badania kontrolne dotyczyły trzech rejestracji w każdym podmiocie leczniczym (lub wszystkich jeśli było ich mniej niż trzy), wybranych według osądu kontrolera.

36 Białostockie Centrum Onkologii im. M. Skłodowskiej-Curie w Białymstoku, Lubuski Szpital Specjalistyczny Pulmonologiczno-Kardiologiczny w Torzymiu sp. z o.o., Samodzielny Publiczny Szpital dla Nerwowo i Psychicznie Chorych w Międzyrzeczu, SP ZOZ w Augustowie, Szpital Miejski Specjalistyczny im. Gabriela Narutowicza w Krakowie, Szpital Specjalistyczny im. Ludwika Rydygiera w Krakowie sp. z o.o., Szpital w Dębnie im. Świętej Matki Teresy z Kalkuty sp. z o.o., Szpital Wojewódzki im. Mikołaja Kopernika w Koszalinie, Zachodniopomorskie Centrum Onkologii w Szczecinie.

37 Białostockie Centrum Onkologii im. M. Skłodowskiej-Curie w Białymstoku, Lubuski Szpital Specjalistyczny Pulmonologiczno-Kardiologiczny w Torzymiu sp. z o.o., SP ZOZ w Augustowie, Szpital Miejski Specjalistyczny im. Gabriela Narutowicza w Krakowie, Szpital w Dębnie im. Świętej Matki Teresy z Kalkuty sp. z o.o., Zachodniopomorskie Centrum Onkologii w Szczecinie.

Przykłady

W trzech rejestracjach **Białostockiego Centrum Onkologii im. M. Skłodowskiej-Curie w Białymstoku**, poza informacją o treści: *Przy okienku rejestracji może przebywać tylko jedna osoba,* zamieszczoną na każdym z okien rejestracji, nie wprowadzono innych rozwiązań zapewniających odpowiedni odstęp pomiędzy osobami przy okienku i kolejnymi osobami w kolejce. W konsekwencji w trakcie oględzin pacjenci stali w bezpośredniej odległości za osobą, która się rejestrowała. Taki sposób rejestracji mógł nie zapewniać należytej ochrony danych osobowych, w szczególności nie odpowiadał dobrym praktykom podanym w przewodniku po RODO, aby dążyć do minimalizacji ryzyka ujawnienia informacji osobom postronnym w procesie rejestracji, wyznaczając obszar, w którym może przebywać wyłącznie obsługiwany pacjent.

W **SP ZOZ w Augustowie** przy rejestracji do poradni specjalistycznych nie wyznaczono strefy przebywania jednego pacjenta, a w trakcie oględzin stwierdzono, że kolejni pacjenci stali w bliskiej odległości od pacjenta obsługiwanego przez pracowników rejestracji. Obszar przebywania jednego pacjenta wyznaczono w trakcie kontroli NIK.

Brak klauzul informacyjnych dla pacjentów

Przy niektórych rejestracjach do poradni w dwóch szpitalach[38] nie zamieszczono klauzul informacyjnych, o których mowa w art. 13 ust. 1–2 RODO, zawierających m.in. dane personalne oraz adresy ADO i IOD, cele i podstawy przetwarzania danych oraz ich kategorie, a także okres przechowywania danych. W konsekwencji ADO, podczas pozyskiwania danych osobowych od pacjentów, nie wywiązywali się z obowiązku informacyjnego, nie zapewniając tym samym rzetelności i przejrzystości przetwarzania danych osobowych, do czego zobowiązują przepisy RODO.

Przykłady

W **Wojewódzkim Szpitalu dla Nerwowo i Psychicznie Chorych „Dziekanka" im. Aleksandra Piotrowskiego w Gnieźnie** na wspólnym stanowisku rejestracji do Poradni Geriatrycznej oraz Poradni Zdrowia Psychicznego nie udostępniono pacjentom rejestrującym się klauzuli informacyjnej, zawierającej m.in. dane ADO i IOD, cele i podstawy przetwarzania danych oraz ich kategorie, a także okres przechowywania danych, tj. informacje, o których mowa w art. 13 ust. 1–2 RODO. Zgodnie z tymi przepisami, jeżeli dane osobowe osoby, której dane dotyczą, są od niej zbierane, to administrator podczas pozyskiwania tych danych podaje jej te informacje. Dyrektor wskazał, że klauzula ta znajdowała się w pomieszczeniu poradni, lecz była niewidoczna dla pacjentów (w trakcie kontroli została wywieszona na tablicy ogłoszeń).

W **Powiatowym Centrum Zdrowia sp. z o.o. w Drezdenku** – z powodu niedopatrzenia – przy żadnej z rejestracji ani w ogólnodostępnym dla pacjentów miejscu nie umieszczono klauzul informacyjnych RODO. W trakcie kontroli NIK w budynku Szpitala klauzule informacyjne RODO zamieszczono na tablicach informacyjnych, w głównej rejestracja i w Izbie Przyjęć.

Wzywanie pacjenta do gabinetu lekarskiego z zachowaniem anonimowości

W żadnym ze skontrolowanych szpitali nie posługiwano się imionami i nazwiskami pacjentów podczas wywoływania ich na wizytę do gabinetów poradni specjalistycznych[39]. Stosowano różne rozwiązania: podanie

[38] Powiatowe Centrum Zdrowia Sp. z o.o. Szpital Powiatowy w Drezdenku, Wojewódzki Szpital dla Nerwowo i Psychicznie Chorych „Dziekanka" im. Aleksandra Piotrowskiego w Gnieźnie.

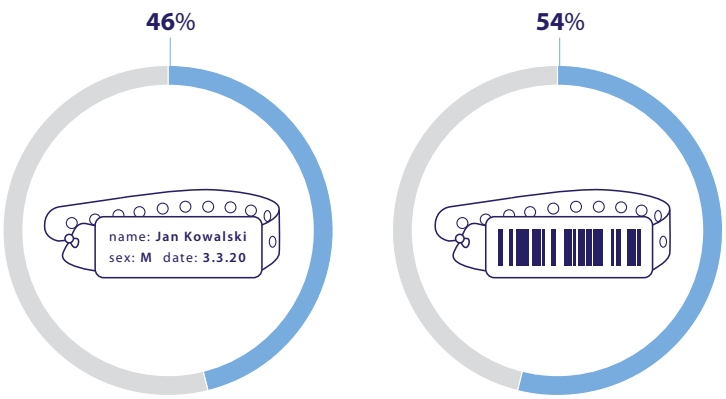
[39] W każdym skontrolowanym podmiocie leczniczym badaniem objęto trzy poradnie specjalistyczne, wybrane według osądu kontrolera.

imienia i godziny wizyty, numeru ustalonego przy rejestracji, ale często wzywano pacjentów do gabinetu bezosobowo, poprzez komunikat „proszę kolejną osobę". Oryginalne rozwiązanie stosowano w jednej z poradni **SP ZOZ w Radzyniu Podlaskim**. Wywieszano listę pacjentów do gabinetu, na której przy planowanej godzinie wizyty widniały pierwsze trzy litery imienia i cztery nazwiska pacjenta. Nieustalenie precyzyjnych zasad postępowania może w przyszłości nie zapewnić ochrony prywatności pacjentów o krótkich imionach i nazwiskach. Wpisanie w ten sposób osób nazywających się np. Jan Dec lub Ewa Król prowadziłoby do ujawnienia ich danych. Tymczasem ochrona prywatności pacjentów jest szczególnie ważna tam, gdzie ujawnienie danych może wiązać się ze stygmatyzacją związaną ze specjalizacją gabinetu, do którego pacjent udaje się na wizytę.

W 46% ZOZ na opaskach indentyfikacyjnych pacjentów zamieszczano dane osobowe

Wszystkie 24 skontrolowane szpitale wywiązały się z obowiązku zaopatrzenia pacjentów w znaki identyfikacyjne, określonego w art. 36 ust. 3 u.o.d.l. Jednak w 11[40] z nich obowiązek ten zrealizowano w sposób niewłaściwy. Opaski na nadgarstkach pacjentów zawierały bowiem – np. poza numerem księgi głównej bądź kodem kreskowym – imię i nazwisko, a w niektórych przypadkach nr PESEL[41]. Stanowiło to naruszenie art. 36 ust. 5 u.o.d.l., w myśl którego opaska zawierać powinna informacje zapisane w sposób uniemożliwiający identyfikację pacjenta przez osoby nieuprawnione.

Infografika nr 7
Udział szpitali pod względem sposobów umieszczania danych na opaskach identyfikacyjnych pacjentów



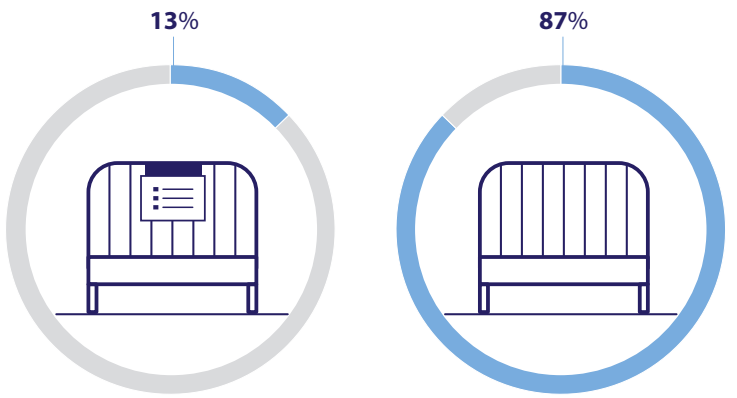
Źródło: Opracowanie własne NIK na podstawie wyników kontroli.

[40] Powiatowe Centrum Zdrowia sp. z o.o. Szpital Powiatowy w Drezdenku, Samodzielny Publiczny Wielospecjalistyczny Zakład Opieki Zdrowotnej w Stargardzie, SP ZOZ w Augustowie, SP ZOZ w Kole, Szpital im. E. Szczeklika w Tarnowie, Szpital Neuropsychiatryczny im. prof. Mieczysława Kaczyńskiego SP ZOZ w Lublinie, Szpital w Dębnie im. Świętej Matki Teresy z Kalkuty sp. z o. o., Szpital Wojewódzki im. Mikołaja Kopernika w Koszalinie, Wojewódzki Specjalistyczny Szpital Dziecięcy im. św. Ludwika w Krakowie, Wojewódzki Szpital Specjalistyczny im. Stefana Kardynała Wyszyńskiego SP ZOZ w Lublinie, Zachodniopomorskie Centrum Onkologii w Szczecinie.

[41] Badaniami objęto po trzy oddziały szpitalne w każdym skontrolowanym podmiocie leczniczym, wybrane według osądu kontrolera.

W trzech[42] podmiotach leczniczych (12,5%) wystąpiły także przypadki zamieszczania danych osobowych pacjentów na szpitalnych kartach przyłóżkowych, które nie zostały zasłonięte, mimo funkcjonujących na innych oddziałach tych jednostek rozwiązań polegających na zastosowaniu ramek na karty przyłóżkowe, zasłaniających dane medyczne pacjentów. Umieszczanie danych osobowych pacjentów w sposób umożliwiający odczytanie przez osoby postronne stanowi naruszenie art. 24 ust. 1 RODO. W myśl tego przepisu jednym z obowiązków ADO jest wdrożenie odpowiednich środków technicznych i organizacyjnych zapewniających ochronę danych osobowych. Jako powód takich działań kierownicy jednostek podawali najczęściej potrzebę właściwego zabezpieczenia usług medycznych i bezpieczeństwa osobowego przy udzielaniu świadczeń zdrowotnych, tj. częstą konieczność niezwłocznej identyfikacji pacjenta.

Infografika nr 8
Udział szpitali pod względem umieszczania kart gorączkowych przy łóżkach pacjentów



Źródło: Opracowanie własne NIK na podstawie wyników kontroli.

Przykłady

W **Specjalistycznym Szpitalu im. Edwarda Szczeklika w Tarnowie** wprowadzono regulacje wewnętrzne, w myśl których dane osobowe pacjentów powinny być umieszczane na opaskach identyfikacyjnych i w związku z tym pobierano zgody od każdego pacjenta na umieszczenie na nich imienia i nazwiska. Na opaskach identyfikacyjnych pacjentów wszystkich trzech oddziałów objętych oględzinami umieszczano imię i nazwisko oraz dodatkowo te same dane osobowe zamieszczano na łóżkach pacjentów. Dyrektor Szpitala wyjaśnił, że podstawą do dodatkowego wpisywania imienia i nazwiska pacjenta na opasce identyfikacyjnej jest jedno z zarządzeń wewnętrznych. Wskazał także, że każdy pacjent przy przyjęciu wyraża pisemną zgodę na umieszczenie swoich danych na opasce identyfikacyjnej, a wprowadzone rozwiązanie ma na celu zwiększenie bezpieczeństwa pacjenta w przypadku konieczności jego szybkiej identyfikacji. Stanowiło to naruszenie art. 36 ust. 3 i 5 u.o.d.l. Wątpliwa była też zdaniem NIK dobrowolność takiej zgody. W myśl motywu 43 RODO, aby zapewnić dobrowolność, zgoda nie powinna stanowić ważnej podstawy

[42] SP ZOZ w Radzyniu Podlaskim (stwierdzono jeden przypadek zamieszczenia danych pacjenta), Wojewódzki Szpital Specjalistyczny im. Stefana Kardynała Wyszyńskiego SP ZOZ w Lublinie i Zachodniopomorskie Centrum Onkologii w Szczecinie – dane pacjentów umieszczono na kartach przyłóżkowych trzech oddziałów objętych oględzinami.

prawnej przetwarzania danych osobowych, w szczególnej sytuacji, w której istnieje wyraźny brak równowagi między osobą, której dane dotyczą a administratorem, w szczególności, gdy jest on organem publicznym.

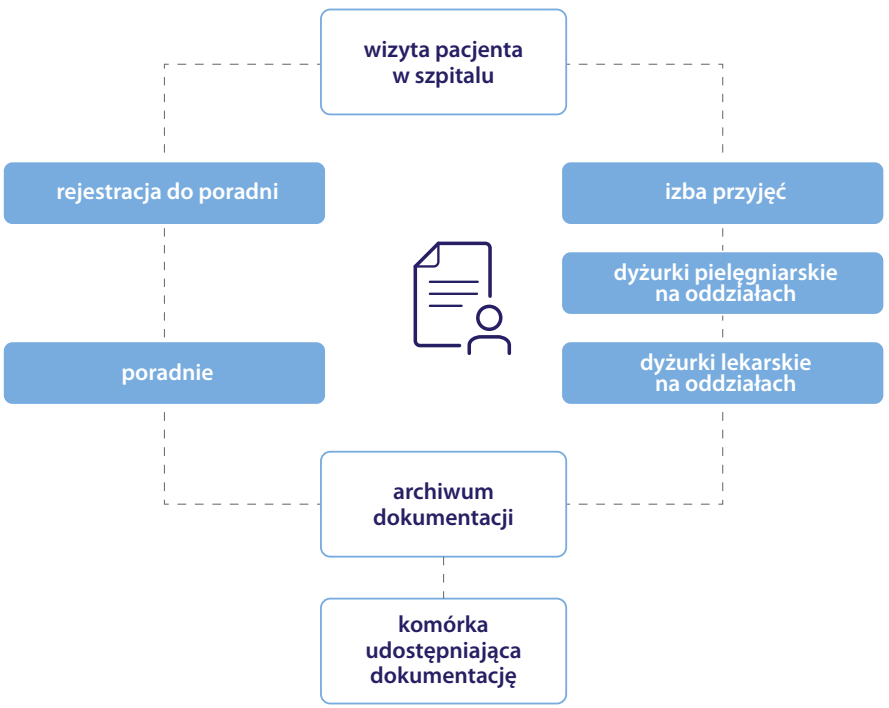
W **SP ZOZ w Radzyniu Podlaskim** pacjenci w momencie przyjęcia na oddział wyrażali pisemną zgodę na umieszczenie ich danych osobowych na kartach gorączkowych, które były zamieszczane na łóżkach oddziałowych, lecz w sposób uniemożliwiający odczytanie danych na nich zapisanych osobom postronnym. Jeżeli pacjent nie wyraził takiej zgody, jego karta nie była przechowywana przy łóżku.

W 37% jednostek niewłaściwie przechowywano papierową dokumentację medyczną pacjentów

Dokumentacja medyczna dotycząca pacjentów jest wytwarzana i przechowywana w różnych komórkach organizacyjnych podmiotów leczniczych.

Infografika nr 9

Miejsca wytworzenia i przechowywania dokumentów zawierających dane osobowe pacjenta



Źródło: Opracowanie własne NIK na postawie wyników kontroli.

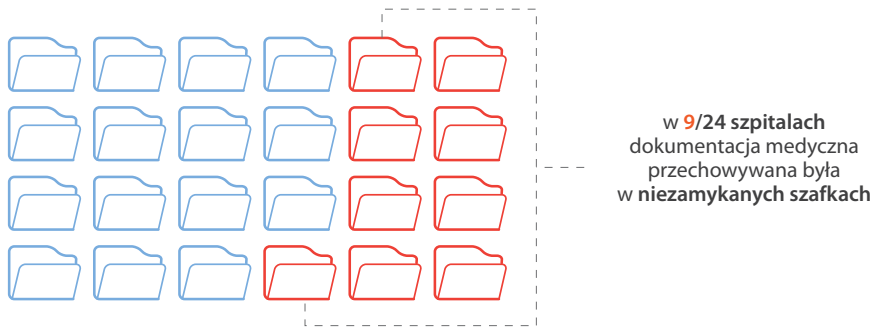
W dziewięciu[43] szpitalach (37,5%) nie zapewniono właściwego przechowywania papierowej dokumentacji medycznej pacjentów[44]. Podręczna papierowa dokumentacja pielęgniarska, zawierająca dane osobowe pacjentów, znajdowała się w niezamykanych szafkach usytuowanych w otwartych pomieszczeniach. Podobna sytuacja miała miejsce w dyżurkach lekarzy na oddziałach, gdzie często dokumentację medyczną przechowywano

[43] Białostockie Centrum Onkologii im. M. Skłodowskiej-Curie w Białymstoku, SP ZOZ w Augustowie, SP ZOZ w Kraśniku, SP ZOZ w Radzyniu Podlaskim, Specjalistyczny Psychiatryczny ZOZ w Suwałkach, Szpital Miejski Specjalistyczny im. Gabriela Narutowicza w Krakowie, Szpital Ogólny w Kolnie, Szpital Wojewódzki im. Mikołaja Kopernika w Koszalinie, Wojewódzki Szpital dla Nerwowo i Psychicznie Chorych „Dziekanka" im. Aleksandra Piotrowskiego w Gnieźnie.

[44] Badaniem objęto trzy oddziały szpitalne w każdym skontrolowanym podmiocie leczniczym, wybrane według osądu kontrolera.

na półkach nieposiadających możliwości zamknięcia. Naruszało to przepisy art. 23 ust. 2 u.o.p.p., w myśl których dane zawarte w dokumentacji medycznej podlegają ochronie, a często także naruszenie przejętych przez podmioty lecznicze regulacji wewnętrznych związanych z ochroną dokumentacji papierowej przed wglądem osób nieupoważnionych lub kradzieżą. Najczęstszymi przyczynami niezapewnienia właściwych warunków do przechowywania dokumentacji medycznej było przeświadczenie personelu, że wystarczą pokoje lekarskie i dyżurki pielęgniarskie zamykane na klucz lub oczekiwanie na remont pomieszczeń, który obejmie również meble na oddziałach, niedostosowane do przechowywania dokumentacji pacjentów w zamknięciu.

Infografika nr 10
Sposób przechowywania papierowej dokumentacji medycznej w dyżurkach pielęgniarskich oraz dyżurkach lekarskich



Źródło: Opracowanie własne NIK na podstawie wyników kontroli.

Przykłady

W **Białostockim Centrum Onkologii im. M. Skłodowskiej-Curie w Białymstoku** podręczna dokumentacja pielęgniarska, zawierająca dane osobowe pacjentów, w dwóch (z trzech) dyżurkach pielęgniarskich oddziałów[45] przechowywana była w niezamykanych pomieszczeniach, w których możliwości zamknięcia nie posiadały również szafki z danymi osobowymi pacjentów. Podobna sytuacja miała miejsce w Oddziale Radioterapii I, tj. w jednym z trzech poddanych oględzinom gabinetów lekarskich, w którym dokumentację medyczną przechowywano na półkach nieposiadających możliwości zamknięcia. Zgodnie z art. 23 ust. 2 u.o.p.p., dane zawarte w dokumentacji medycznej podlegają ochronie. Ponadto zgodnie z postanowieniami pkt 4 Regulaminu Ochrony Danych Osobowych, wprowadzonego w szpitalu, ochrona przed wglądem osób nieupoważnionych lub kradzieżą dokumentacji papierowej, zawierającej dane osobowe, polega m.in. na zabezpieczeniu (zamykaniu) dokumentów w szafach, biurkach i pomieszczeniach.

W dyżurce pielęgniarskiej oraz dwóch oddziałowych gabinetach lekarskich **Wojewódzkiego Szpitala dla Nerwowo i Psychicznie Chorych „Dziekanka" im. Aleksandra Piotrowskiego w Gnieźnie** dokumentacja medyczna pacjentów była przechowywana w szafach, które nie były zamykane na klucz. Stan ten stwarzał ryzyko ujawnienia tych danych osobom nieuprawnionym i był niezgodny z motywem 39. preambuły oraz art. 5 ust. 1 lit. f. RODO, w myśl których dane osobowe powinny być przetwarzane w sposób zapewniający im

[45] Oddziały Chirurgii Onkologicznej i Onkologii Klinicznej.

odpowiednie bezpieczeństwo i odpowiednią poufność, w tym ochronę przed nieuprawnionym dostępem do nich, niedozwolonym lub niezgodnym z prawem przetwarzaniem. Stan ten naruszał również postanowienia obowiązującej w szpitalu Polityki Bezpieczeństwa Ochrony Danych Osobowych, w której wskazano m.in. że niewłaściwe zabezpieczenie fizyczne pomieszczeń i dokumentów oraz niezamykanie szaf stanowi incydent w obszarze bezpieczeństwa danych, wymagający przeprowadzenia postępowania wyjaśniającego. W szpitalu tym stwierdzono także duże ryzyko nieuprawnionego zapoznania się z danymi zastrzeżonymi wyłącznie dla personelu medycznego. Rejestratorka Laboratorium opuściła bowiem pomieszczenie, w którym wykonywała swoje zadania, pozostawiając niezamknięte drzwi i włączony komputer, niezabezpieczony przed dostępem do systemu operacyjnego osób nieupoważnionych.

Monitoring bez podglądu dokumentów pacjentów

Monitoring wizyjny zamontowany był w 17[46] podmiotach leczniczych (71%). Umiejscowienie kamer było różne w zależności od szpitala. Nie stwierdzono, aby pozwalało ono na wgląd w dokumenty pacjentów na oddziałach szpitalnych lub w procesie rejestracji na wizytę.

Przykłady

W **Wielkopolskim Centrum Onkologii im. Marii Skłodowskiej-Curie w Poznaniu** monitoring rejestrował ruch osobowy na korytarzach prowadzących do sal chorych oraz pomieszczeniach, w których mogą przebywać tylko pracownicy szpitala lub personel medyczny razem z pacjentami, a także w salach intensywnego nadzoru i w sekretariatach. W widocznych miejscach umieszczone były komunikaty informujące o funkcjonowaniu monitoringu wizyjnego.

W **Białostockim Centrum Onkologii im. Marii Skłodowskiej-Curie w Białymstoku** kamery umiejscowiono w dwóch[47] z czterech poddanych oględzinom rejestracji szpitala. Informacja o funkcjonującym monitoringu (zawierające m.in. dane ADO, kontakt do IOD oraz podstawę prawną przetwarzania) znajdowała się na drzwiach wejściowych do pomieszczeń, w których odbywała się rejestracja.

W **Szpitalu Miejskim Specjalistycznym im. Gabriela Narutowicza w Krakowie** kamery monitoringu znajdowały się tylko na Szpitalnym Oddziale Ratunkowym.

Pracownikom działów administracyjnych szpitali ograniczono dostęp do danych pacjentów

Spośród 845 objętych analizą pracowników działów administracyjnych[48], 307 (36,3%) miało przyznany pełny lub częściowy dostęp do systemu HIS, w tym 305 (99,3%) osobom był on niezbędny do wykonywania obowiązków służbowych. Każdy z badanych pracowników z przyznanym dostępem

[46] Białostockie Centrum Onkologii im. M. Skłodowskiej-Curie w Białymstoku, Samodzielny Publiczny Szpital dla Nerwowo i Psychicznie Chorych w Międzyrzeczu, Samodzielny Publiczny Wielospecjalistyczny ZOZ w Stargardzie, SP ZOZ w Kole, SP ZOZ w Radzyniu Podlaskim, Specjalistyczny Psychiatryczny ZOZ w Suwałkach, Szpital im. E. Szczeklika w Tarnowie, Szpital Miejski Specjalistyczny im. Gabriela Narutowicza w Krakowie, Szpital Neuropsychiatryczny im. prof. Mieczysława Kaczyńskiego SP ZOZ w Lublinie, Szpital Ogólny w Kolnie, Szpital Specjalistyczny im. Ludwika Rydygiera w Krakowie sp. z o.o., Szpital Specjalistyczny im. Stanisława Staszica w Pile, Szpital Wojewódzki im. Mikołaja Kopernika w Koszalinie, Wielkopolskie Centrum Onkologii im. Marii Skłodowskiej-Curie w Poznaniu, Wojewódzki Specjalistyczny Szpital Dziecięcy im. św. Ludwika w Krakowie, Wojewódzki Szpital dla Nerwowo i Psychicznie Chorych „Dziekanka" im. Aleksandra Piotrowskiego w Gnieźnie, Zachodniopomorskie Centrum Onkologii w Szczecinie.

[47] W rejestracji głównej BCO i Rejestracji Pracowni Tomografii Komputerowej i Rezonansu Magnetycznego.

[48] Badaniem objęto wszystkich pracowników niemedycznych, nie więcej niż po 30 osób w każdym podmiocie leczniczym, wybranych w sposób losowy.

posiadał stosowne upoważnienie ADO. Jedynie w **Szpitalu Specjalistycznym im. Ludwika Rydygiera w Krakowie sp. z o.o.** dwóm osobom przyznano dostęp do systemu HIS, chociaż były one zatrudnione w Dziale Komercji, Marketingu i Komunikacji Korporacyjnej oraz Dziale Planowania i Analiz. Nie wykonywały one czynności pomocniczych przy udzielaniu świadczeń zdrowotnych, w rozumieniu art. 24 ust. 2 pkt 1 u.o.p.p.

Co 11 pielęgniarka posiadała przyznane w HIS zbyt szerokie uprawnienia do danych pacjentów szpitala

Spośród 712 pielęgniarek i położnych[49], których uprawnienia do systemu HIS poddano weryfikacji, 624 (87,6%) posiadały dostęp do tego systemu ograniczony do oddziału lub poradni, na których świadczyły pracę, a 64 (9%) zatrudnione w ośmiu[50] szpitalach miały przyznane w systemie HIS uprawnienia dostępu do danych pacjentów z oddziałów lub poradni szpitala, na których nie świadczyły pracy[51]. Tym samym nie zapewniono im dostępu do danych pacjentów adekwatnego do wykonywanych obowiązków. Stanowiło to naruszenie § 20 ust. 2 pkt 4 rozporządzenia KRI, zobowiązującego kierownika podmiotu publicznego do podejmowania działań zapewniających, że osoby zaangażowane w proces przetwarzania informacji mają stosowne uprawnienia i uczestniczą w tym procesie w stopniu adekwatnym do realizowanych przez nie zadań.

Przykłady

W **SP ZOZ w Augustowie** uprawnienia 22 pielęgniarkom i położnym w systemie HIS zostały nadane podczas wdrażania „Podlaskiego Systemu Informacyjnego e-Zdrowie" w 2015 r. Dyrektor szpitala nie wiedziała, że pielęgniarki mają nadane takie uprawnienia w systemie HIS i że prawdopodobnie od nadania im takich uprawnień nikt ich nie weryfikował. Dla przykładu pielęgniarka środowiskowa w gabinecie lekarza rodzinnego – oprócz dostępu w systemie HIS do pacjentów z tej komórki organizacyjnej – posiadała dostęp do danych pacjentów Oddziału Chirurgii Urazowo-Ortopedycznej, Oddziału Ginekologiczno-Położniczego, Oddziału Chorób Wewnętrznych, Poradni Ginekologiczno-Położniczej, Poradni Chirurgii Urazowo-Ortopedycznej, Poradni Położnej Środowiskowej, Pododdziału Neonatologicznego, w których nigdy nie świadczyła pracy.

W **Lubuskim Szpitalu Specjalistycznym Pulmonologiczno-Kardiologicznym w Torzymiu sp. z o. o.** uprawnienia 16 pielęgniarkom i położnym w systemie HIS zostały nadane przez niedopatrzenie, wynikające z braku bieżącej analizy adekwatności dostępu do danych tylko do tych modułów w HIS, które są niezbędne do wykonywania obowiązków służbowych. Dla przykładu pielęgniarka świadcząca pracę na Oddziale Rehabilitacji Pulmonologicznej posiadała dostęp do danych pacjentów z Oddziału Chorób Płuc, Oddziału Onkologii Pulmonologicznej i Chemioterapii oraz do Zakładu Opiekuńczo-Leczniczego.

---

[49] Badaniem objęto, wybraną w sposób losowy, próbę 20% pielęgniarek i położnych, nie więcej niż po 30 osób w każdym podmiocie leczniczym.

[50] SP ZOZ w Augustowie – 22 osoby, Lubuski Szpital Specjalistyczny Pulmonologiczno-Kardiologiczny w Torzymiu sp. z o.o. – 16 osób, Niepubliczny ZOZ Szpital im. prof. Z. Religi w Słubicach sp. z o.o. – 12 osób, Powiatowe Centrum Zdrowia sp. z o.o. Szpital Powiatowy w Drezdenku – pięć osób, Szpital Ogólny w Kolnie – cztery osoby, Szpital Specjalistyczny im. Ludwika Rydygiera w Krakowie sp. z o.o. i Samodzielny Publiczny Szpital dla Nerwowo i Psychicznie Chorych w Międzyrzeczu – po dwie osoby, SP ZOZ w Kole – jedna osoba.

[51] Kolejne 24 poddane analizie pielęgniarki i położne zatrudnione w Szpitalu im. E. Szczeklika w Tarnowie, Szpitalu Miejskim Specjalistycznym im. Gabriela Narutowicza w Krakowie i w Szpitalu Specjalistycznym im. Ludwika Rydygiera w Krakowie sp. z o.o. nie miały nadanych uprawnień w systemie HIS i nie wykonywały w tym programie żadnych operacji.

W **Niepublicznym ZOZ Szpitalu im. prof. Z. Religi w Słubicach Sp. z o.o.** administrator systemów informatycznych nadał w systemie HIS siedmiu pielęgniarkom lub położnym dostęp nie tylko do miejsca świadczenia przez nie pracy, lecz też do innych oddziałów lub poradni, co wynikało z niewłaściwej komunikacji administratora systemów informatycznych z komórką kadrową szpitala. Położna pracująca w Poradni w Słubicach posiadała uprawnienia do Poradni w Górzycy, trzy pielęgniarki wykonujące pracę na Oddziale Anestezjologii i Intensywnej Terapii posiadały uprawnienia także do Bloku Operacyjnego, a dwie pielęgniarki z Oddziału Chirurgii – do Oddziału Ginekologiczno-Położniczego.

Część personelu medycznego nie posiadała upoważnień do danych osobowych pacjentów lub nadano im je wadliwie

Wraz z przyznaniem uprawnień w systemie HIS pracownicy powinni otrzymać upoważnienia do przetwarzania danych osobowych (art. 32 ust. 4 RODO). W pięciu[52] szpitalach (21%) stwierdzono błędy zarówno podczas udzielania uprawnień do systemu HIS, jak też przy upoważnianiu pracowników:

Przykłady

W **SP ZOZ w Kraśniku** 69 pielęgniarek, cztery położne oraz 14 lekarzy nie posiadało udokumentowanego uprawnienia do przetwarzania danych w systemie HIS. Nie odpowiadało to wymogom art. 32 ust. 4 RODO, aby administrator podjął działania w celu zapewnienia, żeby każda osoba fizyczna, działająca z jego upoważnienia, która ma dostęp do danych osobowych, przetwarzała je wyłącznie na jego polecenie. W trakcie kontroli NIK stwierdzone braki w upoważnieniach zostały uzupełnione. Jednocześnie stwierdzono, że w 23 z 31 analizowanych przypadków, uprawnienia nadano, mimo złożenia wniosków przez nieuprawnione osoby, tj. przez pracowników, a nie przez bezpośrednich przełożonych osób upoważnianych, co było niezgodne z zapisami funkcjonującej w szpitalu Polityki Ochrony Danych.

W **Specjalistycznym Psychiatrycznym ZOZ w Suwałkach** dwóm pracownikom (z 30 objętych analizą) nadano uprawnienia do systemu HIS od siedmiu do 21 dni przed udzieleniem im upoważnienia do przetwarzania danych osobowych. Kolejnej osobie udzielono dostępu do systemu HIS, mimo że nie posiadała ona upoważnienia do przetwarzania danych osobowych, a następnej udzielenie dostępu nie zostało poprzedzone akceptacją IOD, co było wymagane wewnętrznymi przepisami szpitala.

W **Szpitalu Neuropsychiatrycznym im. prof. Mieczysława Kaczyńskiego SP ZOZ w Lublinie** pięciu pracownikom (z 30 objętych analizą) dostęp do programu HIS przyznany został na wniosek samego pracownika, zaakceptowany przez administratora systemu informatycznego, co było niezgodne z obowiązującą w szpitalu Polityką Bezpieczeństwa, zgodnie z którą dyrektor szpitala określa, kto z pracowników ma mieć konto w systemie informatycznym, określa uprawnienia użytkownika i wnioskuje o zmianę tych uprawnień. Jednej pielęgniarce przetwarzającej dane osobowe pacjentów (z 30 poddanych analizie) nie wydano zaś stosownego upoważnienia.

[52] Białostockie Centrum Onkologii im. M. Skłodowskiej-Curie w Białymstoku, SP ZOZ w Kraśniku, Specjalistyczny Psychiatryczny ZOZ w Suwałkach, Szpital Neuropsychiatryczny im. prof. Mieczysława Kaczyńskiego SP ZOZ w Lublinie, Szpital w Dębnie im. Świętej Matki Teresy z Kalkuty sp. z o.o.

Sanitariusze i salowe z upoważnieniami do przetwarzania danych osobowych

W siedmiu[53] skontrolowanych szpitalach (29,2%) praktykowano udzielanie upoważnień do przetwarzania danych osobowych, w tym medycznych, pracownikom obsługi: salowym i sanitariuszom[54]. Funkcje tych osób nie wiązały się jednak w sposób bezpośredni z udzielaniem świadczeń opieki zdrowotnej i nie powinny one mieć dostępu do danych medycznych pacjentów.

Główną przyczyną upoważniania pracowników obsługi do przetwarzania danych osobowych był sposób organizacji pracy podmiotów leczniczych. Upoważnienia te wydawano osobom transportującym pacjentów na badania lub zabiegi, wraz ze skierowaniem lub wynikami badań. Możliwe jest jednak organizacja transportu chorego i odbioru wyników badań, zapewniająca właściwą ochronę danych zawartych w dokumentacji medycznej pacjenta, bez konieczności dostępu do niej pracowników obsługi. Sprzątanie pomieszczeń, dbanie o czystość pacjentów, transport chorych i kierowanie pojazdem nie stanowi celu przetwarzania, uzasadniającego dostęp do danych z historii choroby pacjentów szpitali. Zgodnie z art. 5 ust. 1 i art. 6 ust. 1 RODO, przetwarzanie danych powinno być ograniczone do tego, co jest niezbędne do celów przetwarzania. W takim przypadku wystarczające byłoby zatem odbieranie od pracowników zobowiązania do zachowania w tajemnicy informacji, z którymi mogliby mieć kontakt w trakcie wykonywania obowiązków służbowych. Możliwe jest również wysyłanie skierowań i odbieranie wyników badań za pomocą systemów informatycznych, a w przypadku braku takiej funkcjonalności – w zamykanych kopertach. Nie ma również powodu udzielania pracownikom sprzątającym upoważnień do danych medycznych pacjentów. NIK nie kwestionuje natomiast dostępu do zwykłych danych osobowych pacjentów (jak imię i nazwisko) personelowi pomocniczemu i pracownikom obsługi, jeżeli jest to niezbędne do właściwej realizacji zadań.

Byłym pracownikom w 63% szpitali nie odbierano niezwłocznie uprawnień do systemów informatycznych

W 15[55] podmiotach leczniczych (62,5%) nie w pełni wywiązano się z obowiązku wynikającego z §20 ust. 2 pkt 5 rozporządzenia KRI, zgodnie z którym zarządzanie bezpieczeństwem informacji realizowane jest poprzez bezzwłoczną zmianę uprawnień w przypadku zmiany zadań osób zaangażowanych w proces przetwarzania informacji.

---

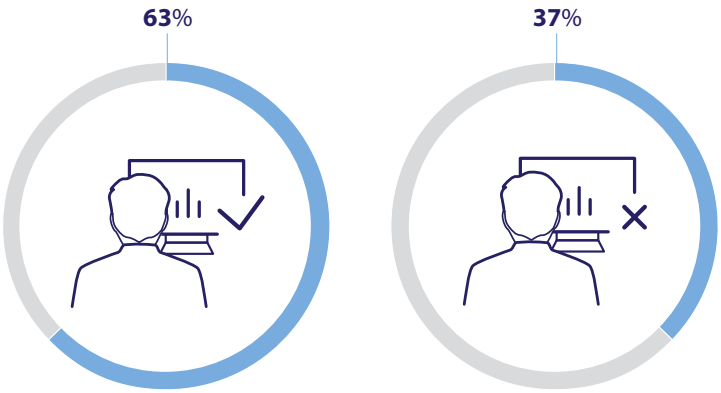
53 Niepubliczny ZOZ Szpital im. prof. Z. Religi w Słubicach sp. z o.o., SP ZOZ w Augustowie, SP ZOZ w Kraśniku, Specjalistyczny Psychiatryczny ZOZ w Suwałkach, Szpital im. E. Szczeklika w Tarnowie, Szpital Miejski Specjalistyczny im. Gabriela Narutowicza w Krakowie, Szpital Specjalistyczny im. Ludwika Rydygiera w Krakowie Sp. z o.o.

54 Badaniem objęto wszystkich pracowników obsługi.

55 Białostockie Centrum Onkologii im. M. Skłodowskiej-Curie w Białymstoku, Lubuski Szpital Specjalistyczny Pulmonologiczno-Kardiologiczny w Torzymiu sp. z o.o., Niepubliczny ZOZ Szpital im. prof. Z. Religi w Słubicach sp. z o.o., Powiatowe Centrum Zdrowia sp. z o.o. Szpital Powiatowy w Drezdenku, Samodzielny Publiczny Szpital dla Nerwowo i Psychicznie Chorych w Międzyrzeczu, Samodzielny Publiczny Wielospecjalistyczny ZOZ w Stargardzie, SP ZOZ w Kole, Specjalistyczny Psychiatryczny ZOZ w Suwałkach, Szpital im. E. Szczeklika w Tarnowie, Szpital Neuropsychiatryczny im. prof. Mieczysława Kaczyńskiego SP ZOZ w Lublinie, Szpital Specjalistyczny im. Ludwika Rydygiera w Krakowie sp. z o.o., Szpital w Dębnie im. Świętej Matki Teresy z Kalkuty sp. z o.o., Szpital Wojewódzki im. Mikołaja Kopernika w Koszalinie, Wojewódzki Specjalistyczny Szpital Dziecięcy im. św. Ludwika w Krakowie. W Wielkopolskim Centrum Onkologii im. Marii Skłodowskiej-Curie w Poznaniu pracownik, któremu nie odebrano dostępu nie miał możliwości logowania do sieci szpitala, gdyż logowanie następowało za pomocą karty dostępowej wraz z numerem PIN, którą pracownik zwrócił w dniu zakończenia zatrudnienia, ale nie zgłosił się z kartą obiegową do działu informatyki, gdzie blokowano dostęp do systemów informatycznych.

Infografika nr 11

Udział szpitali terminowo odbierających uprawnienia w systemach informatycznych pracownikom kończącym zatrudnienie



Źródło: Opracowanie własne NIK na podstawie wyników kontroli.

Spośród poddanych analizie 642 byłych pracowników skontrolowanych szpitali posiadających w trakcie zatrudnienia uprawnienia dostępu do danych zamieszczonych w systemach informatycznych[56], 107 (16,7%) nie odebrano ich niezwłocznie wraz z zakończeniem zatrudnienia, a 96 z 630 (15,2%) nie odebrano uprawnień do systemu HIS[57]. Części pracowników odebranie dostępu do systemu operacyjnego nie było możliwe, ponieważ nie posiadali oni indywidualnego loginu i hasła – stosowano jeden login i hasło dla grupy osób (najczęściej pracowników oddziału). Zagadnienie to szerzej opisano w dalszej części informacji.

Uprawnienia do systemów informatycznych pracownikom kończącym zatrudnienie w szpitalach odbierane były również z opóźnieniem, wynoszącym nawet 227 dni po zakończeniu pracy.

Przykłady

W **Samodzielnym Publicznym Wielospecjalistycznym ZOZ w Stargardzie** dopiero w trakcie kontroli NIK odebrany został dostęp do systemów informatycznych wszystkim 30 objętych badaniem byłym pracownikom szpitala. Osobom tym nie odebrano wcześniej uprawnień dostępowych, wychodząc błędnie z założenia, że wystarczająca była automatyczna blokada konta po 30 dniach.

W **Specjalistycznym Psychiatrycznym ZOZ w Suwałkach** 15 osobom uprawnienia w systemach informatycznych odebrano dopiero po upływie od dziewięciu do 227 dni od momentu zaprzestania przez te osoby świadczenia pracy, co wynikało z niewiedzy administratora systemów informatycznych o konieczności odebrania dostępu. Według dyrektor szpitala, w trakcie kontroli informatyk został dopisany do karty obiegowej, tj. dokumentu wypełnianego przed odejściem pracownika, w celu jego rozliczenia się z firmą. W efekcie będzie miał on wiedzę kto zaprzestał świadczenia pracy i możliwość stosownej reakcji.

[56] Poprzez sformułowanie „systemy informatyczne" należy rozumieć systemy operacyjne komputerów (Windows, Linux) i dziedzinowe systemy robocze (medyczne, księgowe).

[57] Badaniem objęto wszystkich pracowników, z którymi rozwiązano stosunek pracy po 25 maja 2018 r.

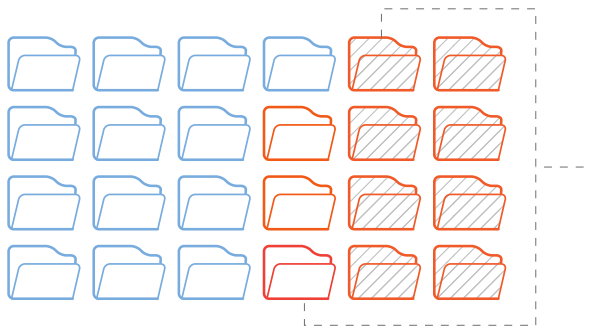
W **Szpitalu Wojewódzkim im. Mikołaja Kopernika w Koszalinie** stwierdzono przypadek logowania się byłego pracownika do systemu operacyjnego po dniu zakończenia przez niego pracy w szpitalu. Zakończenie zatrudnienia nastąpiło 30 września 2018 r., a logowanie miało miejsce 4 października 2018 r. Według pracowników służb informatycznych, konto użytkownika blokowane jest w dniu, w którym ten pracownik zgłasza się z kartą obiegową, lecz nie potrafili wyjaśnić przyczyny aktywności konta po dacie rozwiązania umowy o pracę tego pracownika.

W 46% szpitalach nie przestrzegano zasady adekwatności i minimalizacji danych podczas zgłaszana usterek w oprogramowaniu

W 11[58] skontrolowanych podmiotach leczniczych (46%) stwierdzono przesłanie do firm świadczących usługę helpdesk wraz ze zgłoszeniami serwisowymi danych osobowych 41 pacjentów, w tym danych medycznych 31 z nich[59]. Tym samym złamano zasadę adekwatności i minimalizacji danych (art. 5 pkt 1 lit. c RODO). Przesyłanie w zgłoszeniach serwisowych danych osobowych pacjentów wraz z ich numerami PESEL, a także zrzutów ekranu z historią leczenia, było bowiem działaniem niewspółmiernym do celu, którym był usunięcie usterki w oprogramowaniu HIS. Możliwe było natomiast posługiwanie się unikalnym numerem ID pacjenta jednoznacznie wskazującym osobę, której dane zgłoszenie dotyczyło.

Infografika nr 12

Proceder przesyłania danych osobowych i medycznych pacjentów w zgłoszeniach serwisowych dokonanych w okresie objętym kontrolą



w **11/24 szpitalach** w zgłoszeniach do serwisanta problemów technicznych z medycznymi systemami informatycznymi **przekazano na zewnątrz szpitala dane osobowe pacjenta**

w tym w **8/24 szpitalach** wśród przekazanych danych znalazły się **informacje medyczne o pacjentach**

Źródło: Opracowanie własne NIK na podstawie wyników kontroli.

Przykłady

W **Białostockim Centrum Onkologii im. M. Skłodowskiej-Curie w Białymstoku** przekazano dane osobowe dziewięciu pacjentów, w tym dane medyczne pięciu z nich. Odbiorcą tych danych była firma zewnętrzna, będąca podwykonawcą firmy świadczącej usługi serwisowe na rzecz szpitala. Podwykonawca ten nie został wymieniony w umowie serwisowej, a dodatkowo szpital nie miał z nim zawartej umowy powierzenia przetwarzania danych.

[58] Białostockie Centrum Onkologii im. M. Skłodowskiej-Curie w Białymstoku, Niepubliczny ZOZ Szpital im. prof. Z. Religi w Słubicach sp. z o.o., SP ZOZ w Augustowie, SP ZOZ w Kraśniku, SP ZOZ w Radzyniu Podlaskim, Specjalistyczny Psychiatryczny ZOZ w Suwałkach, Szpital im. E. Szczeklika w Tarnowie, Szpital Neuropsychiatryczny im. Prof. Mieczysława Kaczyńskiego SP ZOZ w Lublinie, Szpital Wojewódzki im. Mikołaja Kopernika w Koszalinie, Wojewódzki Specjalistyczny Szpital Dziecięcy im. św. Ludwika w Krakowie, Zachodniopomorskie Centrum Onkologii w Szczecinie.

[59] Badaniem objęto zgłoszenia serwisowe wysłane po 25 maja 2018 r., nie więcej niż po 50 zgłoszeń w każdym skontrolowanym podmiocie leczniczym, wybranych według osądu kontrolera.

W **Wojewódzkim Specjalistycznym Szpitalu Dziecięcym im. Św. Ludwika w Krakowie** przekazano zewnętrznej firmie serwisowej dane osobowe i medyczne dwóch pacjentów, w tym wyniki tomografii komputerowej i badania mikrobiologicznego.

NIK nie kwestionowała wprowadzonych przez szpitale zabezpieczeń systemów informatycznych (szyfrowanego kanału komunikacji z firmą świadczącą usługi helpdesk) ani możliwego dostępu serwisantów do danych osobowych i medycznych pacjentów w związku z zawartą umową powierzenia przetwarzania danych i wystawionymi upoważnieniami dostępu do tych danych. Nie było jednak powodu podawania danych osobowych i historii leczenia w treści zgłoszeń serwisowych. Wprawdzie odsetek zgłoszeń serwisowych, w których stwierdzono przekazywanie danych osobowych i medycznych pacjentów nie był wysoki – stanowił odpowiednio 3,7% i 2,8% zgłoszeń serwisowych zbadanych przez NIK – to jednak należy mieć na uwadze ewentualne skutki w przypadku ujawnienia tych danych. Przykładem tego mogą być, opisywany przez portale internetowe[60], przypadek wycieku w 2017 r. danych zawartych z zgłoszeniach serwisowych. Dane przesyłane na system helpdesk gromadzone były na zewnętrznym serwerze. Do ich ujawnienia doszło na skutek błędu podczas migracji danych na nowy serwer. Zasadnym jest zatem takie działanie, aby treści zgłoszeń serwisowych nie zawierały danych osobowych i medycznych pacjentów szpitali.

Właściwie dokumentowano i reagowano na incydenty związane z naruszeniem ochrony danych osobowych

W 13[61] skontrolowanych szpitalach (54%) doszło do naruszeń ochrony danych osobowych[62], w tym w sześciu z nich wynikała potrzeba powiadomienia Prezesa Urzędu, co w każdym przypadku uczyniono. W pozostałych szpitalach incydenty związane z bezpieczeństwem danych osobowych nie wiązały się z ryzykiem naruszenia praw lub wolności osób fizycznych.

Przykłady

W **Szpitalu Specjalistycznym im. Ludwika Rydygiera w Krakowie sp. z o.o.** doszło do nieumyślnego zabrania dokumentacji medycznej pacjenta przez innego pacjenta jednej z poradni. Przyczyną zdarzenia było naruszenie „zasady czystego biurka" przez personel medyczny.

60 https://niebezpiecznik.pl/post/dane-pacjentow-i-szpitali-wyciekly-z-helpdesku-eskulapa-szpitale-powinny-zmienic-hasla/
[dostęp z 24 maja 2019 r.].
https://zaufanatrzeciastrona.pl/post/wyciek-danych-wrazliwych-50-tysiecy-pacjentow-polskiego-szpitala/
[dostęp z 24 maja 2019 r.].

61 Białostockie Centrum Onkologii im. M. Skłodowskiej-Curie w Białymstoku, Samodzielny Publiczny Szpital dla Nerwowo i Psychicznie Chorych w Międzyrzeczu, SP ZOZ w Augustowie, SP ZOZ w Radzyniu Podlaskim, Szpital im. E. Szczeklika w Tarnowie, Szpital Neuropsychiatryczny im. prof. Mieczysława Kaczyńskiego SP ZOZ w Lublinie, Szpital Ogólny w Kolnie, Szpital Specjalistyczny im. Ludwika Rydygiera w Krakowie sp. z o.o., Szpital Specjalistyczny im. Stanisława Staszica w Pile, Szpital Wojewódzki im. Mikołaja Kopernika w Koszalinie, Wojewódzki Specjalistyczny Szpital Dziecięcy im. św. Ludwika w Krakowie, Wojewódzki Szpital dla Nerwowo i Psychicznie Chorych „Dziekanka" im. Aleksandra Piotrowskiego w Gnieźnie, Wojewódzki Szpital Specjalistyczny im. Stefana Kardynała Wyszyńskiego SP ZOZ w Lublinie.

62 Art. 4 pkt 12 RODO definiuje naruszenie ochrony danych osobowych jako „naruszenie bezpieczeństwa prowadzące do przypadkowego lub niezgodnego z prawem zniszczenia, utracenia, zmodyfikowania, nieuprawnionego ujawnienia lub nieuprawnionego dostępu do danych osobowych przesyłanych, przechowywanych lub w inny sposób przetwarzanych".

W **Wojewódzkim Specjalistycznym Szpitalu Dziecięcym im. Św. Ludwika w Krakowie** niezrównoważony psychicznie mężczyzna ukradł z pomieszczenia rejestracji trzy kartoteki pacjentów. Dwóch z nich nie odnaleziono, a sprawa została zgłoszona organom ścigania.

W **Samodzielnym Publicznym Szpitalu dla Nerwowo i Psychicznie Chorych w Międzyrzeczu** naruszenie polegało na dokonaniu przez pracownika szpitala przywłaszczenia dokumentacji medycznej pacjenta i wyniesienia jej poza obszar szpitala.

Przykłady dotyczące ujawnienia dokumentacji medycznej świadczą o złym jej zabezpieczeniu i przechowywaniu, często wynikającymi z rutyny personelu medycznego. Odpowiednio zabezpieczone dokumenty nie zostałyby nieumyślnie zabrane przez innego pacjenta lub osobę z zaburzeniami psychicznymi.

W dwóch szpitalach wydano kopię dokumentacji medycznej osobie nieupoważnionej

Zgodnie z przepisami u.o.p.p., pacjent ma prawo do zachowania w tajemnicy przez osoby wykonujące zawód medyczny, w tym udzielające mu świadczeń zdrowotnych, informacji z nim związanych, uzyskanych w związku z wykonywaniem zawodu medycznego (art. 13). Dokumentacja medyczna winna być udostępniana osobie upoważnionej przez pacjenta lub jego przedstawicielowi ustawowemu (art. 26 ust. 1).

W czterech[63] szpitalach (16,7%) stwierdzono przypadki niewłaściwego udostępniania dokumentacji medycznej[64]. W dwóch z nich udostępniono ją innym osobom niż pacjent, chociaż nie posiadały one stosownego upoważnienia.

Przykłady

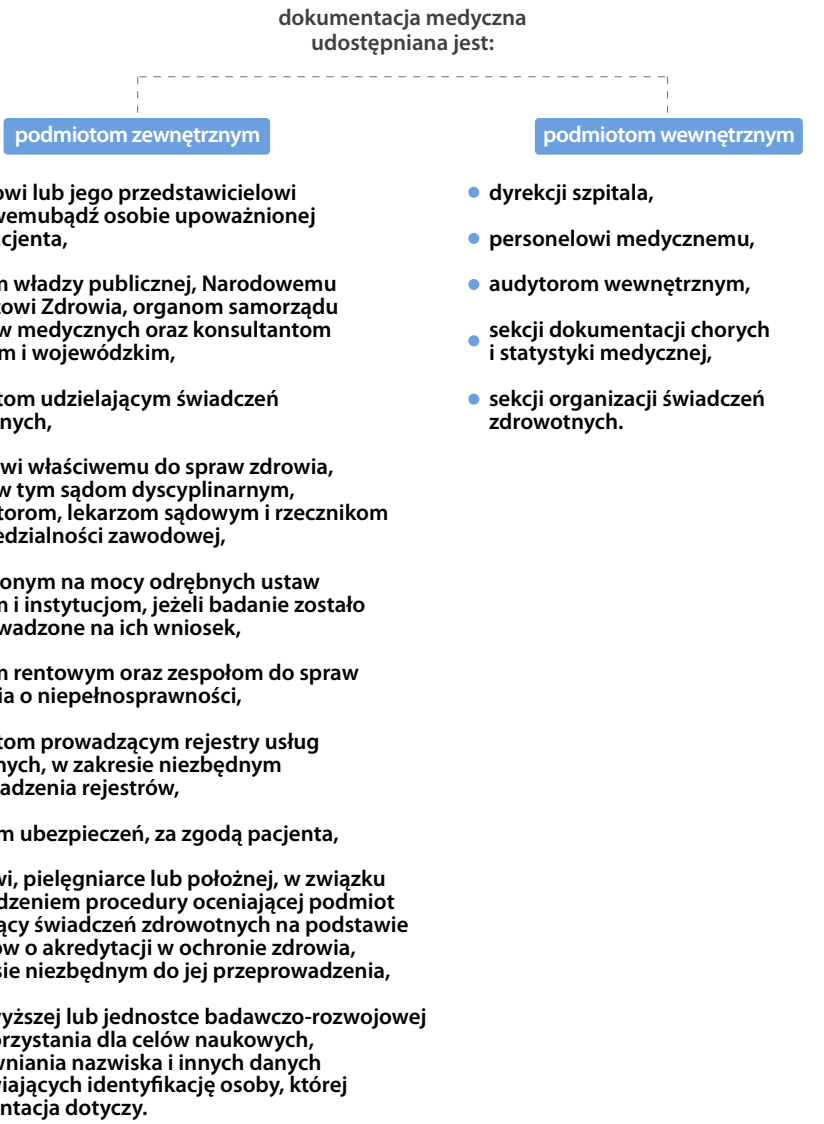
W **SP ZOZ w Augustowie** w trzech przypadkach (z 49 badanych) dokumentacja medyczna została udostępniona osobom nieupoważnionym przez pacjentów, wbrew art. 26 ust. 1 u.o.p.p., a w kolejnym przypadku nie zweryfikowano tożsamości osoby, której udostępniono dokumentację medyczną. Dokumentacja została udostępniona pocztą elektroniczną (e-mail) na wniosek złożony tą samą drogą, podczas gdy – zgodnie z obowiązującą w szpitalu procedurą udostępniania dokumentacji medycznej – powinna być udostępniana za okazaniem dokumentu potwierdzającego tożsamość.
Jednocześnie w szpitalu nie był prowadzony wykaz zawierający informacje dotyczące udostępnianej dokumentacji medycznej dla pacjentów lub osób upoważnionych przez pacjentów, wymagany art. 27 ust. 4 u.o.p.p., a na złożonych wnioskach nie było danych (imienia i nazwiska) oraz podpisu pracownika, który udostępnił dokumentację medyczną.

W **Białostockim Centrum Onkologii im. M. Skłodowskiej-Curie w Białymstoku** dokumentację medyczną pełnoletniego pacjenta (z 28 analizowanych) udostępniono na podstawie listu otrzymanego przez szpital od osoby podającej się za matkę pacjenta, która nie przedstawiła stosownego upoważnienia w tym zakresie.

[63] Białostockie Centrum Onkologii im. M. Skłodowskiej-Curie w Białymstoku, SP ZOZ w Augustowie, Szpital Miejski Specjalistyczny im. Gabriela Narutowicza w Krakowie, Zachodniopomorskie Centrum Onkologii w Szczecinie.

[64] W każdym skontrolowanym podmiocie leczniczym badaniem objęto po 30 spraw (lub wszystkie jeśli było ich mniej) związanych z udostępnieniem dokumentacji medycznej innej osobie niż pacjent, którego ta dokumentacja dotyczy oraz po 30 spraw (lub wszystkie jeśli było ich mniej) związanych z udostępnieniem dokumentacji medycznej firmom ubezpieczeniowym – wybranych według osądu kontrolera.

Infografika nr 13
Podmioty, którym szpital udostępnia dokumentację medyczną



Źródło: Opracowanie własne NIK na podstawie u.o.p.p.

Niewiele było skarg związanych z ochroną danych osobowych

W dwóch szpitalach pacjenci złożyli skargi związane z niewłaściwą ochroną danych osobowych.

Przykłady

W **Szpitalu Neuropsychiatrycznym im. prof. Mieczysława Kaczyńskiego SP ZOZ w Lublinie** pacjentka skarżyła się na używanie jej nazwiska przez pracownika szpitala, podczas wzywania jej na zabieg.

W **Szpitalu im. E. Szczeklika w Tarnowie** przedmiotem skargi dotyczącej niewłaściwej ochrony danych osobowych było niepoinformowanie skarżącego (członka rodziny) o wypisie pacjenta ze szpitala. Powodem nieudzielenia takiej informacji był brak upoważnienia do udzielenia informacji o stanie zdrowia pacjenta.

Tylko w sześciu szpitalach podstawowe zabezpieczenia danych w postaci elektronicznej były właściwe

Tylko w sześciu[65] skontrolowanych szpitalach (25%) zastosowano właściwe środki techniczne do zabezpieczenia danych osobowych pacjentów. W pozostałych poszczególne elementy wpływające na bezpieczeństwo elektroniczne zostały bądź niewłaściwie zaplanowane, bądź były niewłaściwie użytkowane. Tymczasem właściwe podejście do zagadnień ochrony danych osobowych związane jest z zapewnieniem odpowiedniego poziomu ochrony danych przechowywanych w postaci elektronicznej. Elektroniczna dokumentacja medyczna nie jest jeszcze upowszechniona we wszystkich podmiotach leczniczych, niemniej każdy z nich sprawozdaje elektronicznie do oddziału wojewódzkiego Narodowego Funduszu Zdrowia dane o charakterze statystycznym i rozliczeniowym. Zawierają one syntezę informacji o pacjencie, jednostce chorobowej, na którą był leczony w szpitalu, wykonanych badaniach, zabiegach i procedurach leczniczych. Stanowią zatem kompendium wiedzy o pobycie pacjenta w podmiocie leczniczym, co sprawia, że wymagają szczególnej ochrony. W myśl art. 5 ust. 1 lit. f RODO, dane osobowe muszą być przetwarzane w sposób zapewniający odpowiednie bezpieczeństwo danych osobowych, w tym ochronę przed niedozwolonym lub niezgodnym z prawem przetwarzaniem oraz przypadkową utratą, zniszczeniem lub uszkodzeniem, za pomocą odpowiednich środków technicznych lub organizacyjnych („integralność i poufność").

Pracownikom nadawano zbyt wysokie uprawnienia w systemach operacyjnych

W dziesięciu[66] podmiotach leczniczych (42%) nie przestrzegano wymogu ustalonego w § 20 ust. 2 pkt 4 rozporządzenia KRI, zgodnie z którym kierownictwo podmiotu publicznego jest obowiązane do podejmowania działań zapewniających, że osoby zaangażowane w proces przetwarzania informacji posiadają stosowne uprawnienia i uczestniczą w tym procesie w stopniu adekwatnym do realizowanych zadań. Z 720 pracowników objętych analizą NIK[67], 167 (23,2%) posiadało uprawnienia administratora systemów operacyjnych, chociaż nie posiadali oni w swych zakresach obowiązków zadań związanych z administrowaniem systemami. Dawało im to nieograniczoną możliwość instalacji dowolnego oprogramowania na użytkowanych komputerach, wyłączenia ochrony antywirusowej i ingerowania w inne ustawienia systemów informatycznych. Taka sytuacja stwarzała ryzyko obniżenia skuteczności ochrony przetwarzanych danych i zainstalowania na komputerze złośliwego oprogramowania, umożliwiającego penetrację systemu informatycznego.

---

65 SP ZOZ w Kraśniku, SP ZOZ w Radzyniu Podlaskim, Szpital Specjalistyczny im. Stanisława Staszica w Pile, Wielkopolskie Centrum Onkologii im. Marii Skłodowskiej-Curie w Poznaniu, Wojewódzki Specjalistyczny Szpital Dziecięcy im. św. Ludwika w Krakowie, Wojewódzki Szpital dla Nerwowo i Psychicznie Chorych „Dziekanka" im. Aleksandra Piotrowskiego w Gnieźnie.

66 Szpital Miejski Specjalistyczny im. Gabriela Narutowicza w Krakowie, Szpital im. E. Szczeklika w Tarnowie, Powiatowe Centrum Zdrowia sp. z o.o. Szpital Powiatowy w Drezdenku – po 30 osób z uprawnieniami administratora, Niepubliczny ZOZ Szpital im. prof. Z. Religi w Słubicach sp. z o.o. – 27 osób, Samodzielny Publiczny Wielospecjalistyczny ZOZ w Stargardzie – 20 osób, SP ZOZ w Augustowie – 11 osób, Samodzielny Publiczny Szpital dla Nerwowo i Psychicznie Chorych w Międzyrzeczu – dziewięć osób, Szpital Wojewódzki im. Mikołaja Kopernika w Koszalinie – pięć osób, Specjalistyczny Psychiatryczny ZOZ w Suwałkach – trzy osoby, Szpital Neuropsychiatryczny im. Prof. Mieczysława Kaczyńskiego SP ZOZ w Lublinie – dwie osoby.

67 W badaniach dotyczących bezpieczeństwa danych w postaci elektronicznej, w każdym skontrolowanym podmiocie leczniczym kontrolą objęto po 10 komputerów użytkowanych przez lekarzy, pielęgniarki i personel administracyjny – wybranych według osądu kontrolera.

Nie każdy komputer chroniony był programem antywirusowym

W trzech[68] szpitalach (12,5%) część komputerów nie posiadała zainstalowanego oprogramowania antywirusowego, a w czterech[69] baza sygnatur wirusów na części komputerów była nieaktualna (np. w **SP ZOZ w Augustowie** ostatnia aktualizacja miała miejsce ponad 16 miesięcy przed oględzinami NIK). Niezapewnienie aktualnej bazy sygnatur w oprogramowaniu antywirusowym były niezgodne z § 20 ust. 2 pkt 7 i 9 rozporządzenia KRI, zgodnie z którymi kierownictwo podmiotu publicznego jest obowiązane do podejmowania działań zapewniających ochronę przetwarzanych informacji przed ich kradzieżą, nieuprawnionym dostępem, uszkodzeniami lub zakłóceniami, a także zabezpieczenia przetwarzanych informacji w sposób uniemożliwiający nieuprawnionemu jej ujawnienie, modyfikację, usunięcie lub zniszczenie. Zgodnie zaś z przepisem § 20 ust. 2 pkt 12 tego rozporządzenia, zapewnienie odpowiedniego poziomu bezpieczeństwa w systemach teleinformatycznych polega w szczególności na dbałości o aktualizację oprogramowania, minimalizowaniu ryzyka utraty informacji w wyniku awarii oraz ochronie przed błędami, utratą, nieuprawnioną modyfikacją.

W części szpitali komputery były dostępne dla wszystkich, bez potrzeby autoryzacji lub z loginem i hasłem wspólnym dla kilku osób

W trzech[70] szpitalach (12,5%) część komputerów można było uruchomić bez uwierzytelniania hasłem, a w dwunastu[71] – login i hasło przyznawano grupie osób, zamiast dla każdego użytkownika. Dotyczyło to 188 komputerów z 720 zbadanych (26,1%). Obowiązkiem kierownictwa jednostki jest zaś zapewnienie ochrony przetwarzanych informacji przed ich kradzieżą, nieuprawnionym dostępem, uszkodzeniami lub zakłóceniami, poprzez zapewnienie środków uniemożliwiających nieautoryzowany dostęp na poziomie systemów operacyjnych, usług sieciowych i aplikacji (§ 20 ust. 7 lit. c rozporządzenia KRI). Praktyka wprowadzona w części podmiotów leczniczych oznacza jednocześnie niemożliwość ustalenia pracownika, który dokonywał operacji w systemie operacyjnym (rozliczalność danych, o której mowa w § 21 rozporządzenia KRI). Jest to szczególne ważne w przypadku wycieku danych poza szpital, gdyż uniemożliwia przypisanie odpowiedzialności konkretnemu użytkownikowi (w zapisach w dziennikach systemów – logach – odnotowane zostanie logowanie do systemu operacyjnego nieokreślonej osoby). Wspólny login dostępu do komputera uniemożliwia również odebranie dostępu do systemu operacyjnego osobie kończącej zatrudnienie. Login i hasło do systemu używane jest bowiem przez pozostałych pracowników tej komórki organizacyjnej.

---

68 SP ZOZ w Augustowie oraz Niepubliczny ZOZ Szpital im. prof. Z. Religi w Słubicach sp. z o.o. – po trzy komputery, Zachodniopomorskie Centrum Onkologii w Szczecinie – dwa komputery.

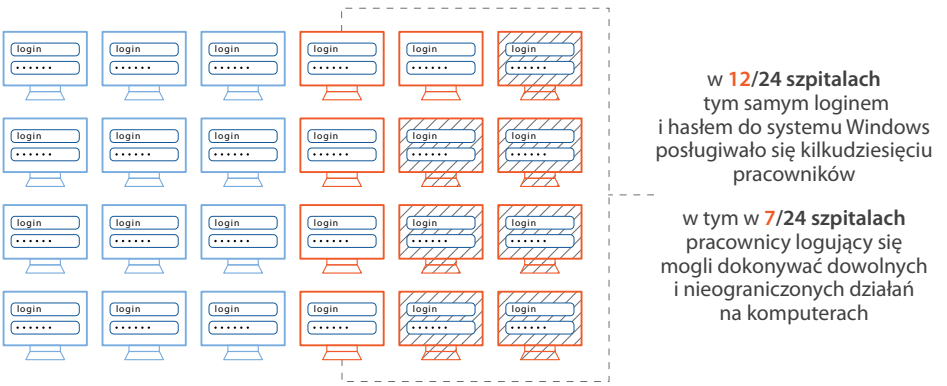
69 Szpital Specjalistyczny im. Ludwika Rydygiera w Krakowie sp. z o.o. – dziewięć komputerów z nieaktualną bazą wirusów, Specjalistyczny Psychiatryczny ZOZ w Suwałkach, SP ZOZ w Augustowie, Szpital Wojewódzki im. Mikołaja Kopernika w Koszalinie – po jednym komputerze.

70 SP ZOZ w Augustowie oraz Szpital Neuropsychiatryczny im. Prof. Mieczysława Kaczyńskiego SP ZOZ w Lublinie – po cztery komputery, Samodzielny Publiczny Szpital dla Nerwowo i Psychicznie Chorych w Międzyrzeczu – jeden komputer.

71 Szpital Miejski Specjalistyczny im. Gabriela Narutowicza w Krakowie – 30 komputerów, Szpital im. E. Szczeklika w Tarnowie, SP ZOZ w Kole, Szpital w Dębnie im. Świętej Matki Teresy z Kalkuty sp. z o.o., Samodzielny Publiczny Wielospecjalistyczny ZOZ w Stargardzie, Powiatowe Centrum Zdrowia sp. z o.o. Szpital Powiatowy w Drezdenku – po 20, Niepubliczny ZOZ Szpital im. prof. Z. Religi w Słubicach sp. z o.o. –16, Białostockie Centrum Onkologii im. M. Skłodowskiej-Curie w Białymstoku – 12, Szpital Specjalistyczny im. Ludwika Rydygiera w Krakowie sp. z o.o. – 11, Szpital Neuropsychiatryczny im. prof. Mieczysława Kaczyńskiego SP ZOZ w Lublinie, Lubuski Szpital Specjalistyczny Pulmonologiczno-Kardiologiczny w Torzymiu sp. z o.o. – po dziewięć, Samodzielny Publiczny Szpital dla Nerwowo i Psychicznie Chorych w Międzyrzeczu – jeden.

Infografika nr 14

Posługiwanie się tym samym loginem i hasłem do systemu operacyjnego



Źródło: Opracowanie własne NIK na podstawie wyników kontroli.

Hasła do logowania nie spełniały wewnętrznych wymagań, stanowiących o ich sile

W siedmiu[72] szpitalach (29,2%) na 114 komputerach (15,8% objętych badaniem NIK) stosowano hasła, które nie spełniały wewnętrznie ustalonych wymogów złożoności. Zazwyczaj wymagano stosowanie w haśle dużych i małych liter, cyfr i znaków specjalnych. Pracownicy nie respektowali jednak wewnętrznych ustaleń w tym zakresie. Obniżało to skuteczność ochrony dostępu do sytemu operacyjnego.

Przykład

W **Lubuskim Szpitalu Specjalistycznym Pulmonologiczno-Kardiologicznym w Torzymiu sp. z o. o.** hasła nie podlegały okresowej zmianie (w regulacjach wewnętrznych określony był wymóg zmiany hasła do systemu HIS co 30 dni, faktycznie wymuszanie zmiany hasła ustawiono na 180 dni, ważność hasła do systemu operacyjnego ustawiona bezterminowo – system nie wymuszał zmiany hasała), a trzykrotne błędne wpisanie hasła do sytemu operacyjnego Windows nie skutkowało zablokowaniem dostępu do systemu. Administrator systemów informatycznych szpitala tłumaczył takie działanie względami praktycznymi. Jego zdaniem częsta zmiana haseł stwarza pracownikom dodatkowe obowiązki i może utrudniać bieżące wykonywanie podstawowych zadań, jakimi jest świadczenie usług zdrowotnych.

Użytkowano systemy operacyjne pozbawione wsparcia technicznego

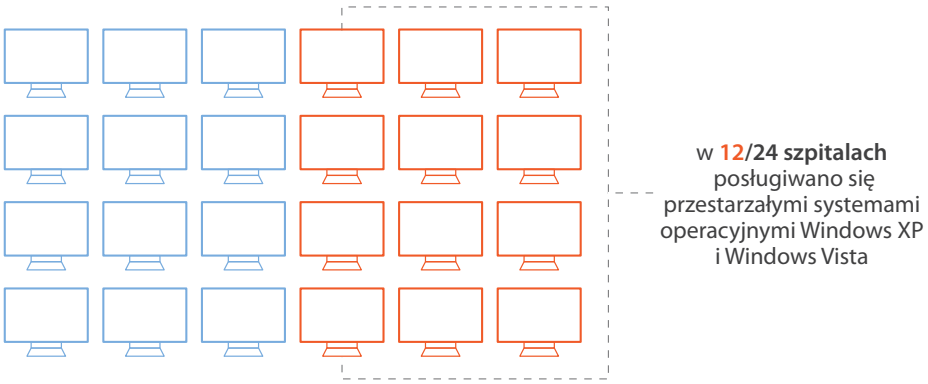
W dwunastu[73] szpitalach (50%) na 119 komputerach (16,5%) zainstalowany był system operacyjny Windows XP lub Vista, mimo że dla tych systemów producent oprogramowania zakończył wsparcie techniczne odpowiednio 8 kwietnia 2014 r. i 11 kwietnia 2017 r. Przestał zatem dostarczać aktualizacje zabezpieczeń, poprawki niezwiązane z zabezpie-

72 Szpital Miejski Specjalistyczny im. Gabriela Narutowicza w Krakowie – 30 komputerów, Samodzielny Publiczny Wielospecjalistyczny ZOZ w Stargardzie – 20, Samodzielny Publiczny Szpital dla Nerwowo i Psychicznie Chorych w Międzyrzeczu – 17, Niepubliczny ZOZ Szpital im. prof. Z. Religi w Słubicach sp. z o.o. – 15, Szpital Specjalistyczny im. Ludwika Rydygiera w Krakowie sp. z o.o. – 14, Białostockie Centrum Onkologii im. M. Skłodowskiej-Curie w Białymstoku – 12, Lubuski Szpital Specjalistyczny Pulmonologiczno-Kardiologiczny w Torzymiu sp. z o.o. – sześć.

73 Samodzielny Publiczny Szpital dla Nerwowo i Psychicznie Chorych w Międzyrzeczu – 26 komputerów, Lubuski Szpital Specjalistyczny Pulmonologiczno-Kardiologiczny w Torzymiu sp. z o.o. – 19, SP ZOZ w Kole – 17, Szpital Neuropsychiatryczny im. prof. Mieczysława Kaczyńskiego SP ZOZ w Lublinie – 16, Wojewódzki Szpital Specjalistyczny im. Stefana Kardynała Wyszyńskiego SP ZOZ w Lublinie i Szpital w Dębnie im. Świętej Matki Teresy z Kalkuty sp. z o.o. – po 10, Szpital Specjalistyczny im. Ludwika Rydygiera w Krakowie sp. z o.o. – dziewięć, Niepubliczny ZOZ Szpital im. prof. Z. Religi w Słubicach sp. z o.o. – cztery, Szpital im. E. Szczeklika w Tarnowie i Szpital Wojewódzki im. Mikołaja Kopernika w Koszalinie – po trzy, SP ZOZ w Augustowie i Powiatowe Centrum Zdrowia sp. z o.o. Szpital Powiatowy w Drezdenku – po jednym.

czeniami, bezpłatne lub płatne opcje asystowanej pomocy technicznej i aktualizacje zawartości technicznej online, co znacznie wpływało na bezpieczeństwo tych systemów operacyjnych. Na pozostałych komputerach stosowano systemy Windows 7, Windows 8 lub Windows 10.

Infografika nr 15
Użytkowanie systemów operacyjnych bez wsparcia producenta



Źródło: Opracowanie własne NIK na podstawie wyników kontroli.

Na dyskach twardych przechowywano dane osobowe i medyczne pacjentów

W czterech[74] szpitalach (16,7%) na dyskach twardych 14 komputerów (1,9%) przechowywano, w podręcznych folderach, pliki z danymi osobowymi i medycznymi wybranych pacjentów. Jednocześnie w dwóch z tych szpitali dostęp do siedmiu z tych komputerów nie wymagał uwierzytelnienia loginem i hasłem (**SP ZOZ w Augustowie**[75]) lub przyznany był wspólny login i hasło dla grupy osób (**SP ZOZ w Kole**). Nie przestrzegano zatem prawa pacjenta do zachowania w tajemnicy przez osoby wykonujące zawód medyczny, w tym udzielające mu świadczeń zdrowotnych, informacji z nim związanych, uzyskanych w związku z wykonywaniem zawodu medycznego (art. 13 u.o.p.p.).

Zadbano o zabezpieczenie szpitalnych serwerowni

W 22 szpitalach (92%) serwerownie były właściwie zabezpieczone. Zastosowano w nich m.in. drzwi przeciwpożarowe, podłogę techniczną, czujniki dymu, czujniki alarmowe. Wyposażone zostały w klimatyzację, gaśnice, system monitoringu. Tylko w dwóch skontrolowanych podmiotach leczniczych stwierdzono niedostateczne zabezpieczenie serwerowni.

Przykłady

W **Samodzielnym Publicznym Wielospecjalistycznym ZOZ w Stargardzie** okna serwerowni nie posiadały żadnych zabezpieczeń. Nie było systemu alarmowego/monitoringu dostępu do pomieszczeń. W trakcie kontroli zamontowano system monitoringu i trwały prace nad zamontowaniem żaluzji okiennych i alarmu przeciwpożarowego.

W **Lubuskim Szpitalu Specjalistycznym Pulmonologiczno-Kardiologicznym w Torzymiu sp. z o. o.** serwerownia nie posiadała gaśnicy oraz systemów ostrzegania pożarowego.

[74] Samodzielny Publiczny Szpital dla Nerwowo i Psychicznie Chorych w Międzyrzeczu i SP ZOZ w Kole – po sześć komputerów, Zachodniopomorskie Centrum Onkologii w Szczecinie i SP ZOZ w Augustowie – po jednym komputerze.

[75] Oznaczało to, że każdy, kto włączył komputer, mógł zapoznać się z opisem stanu zdrowia wybranych pacjentów.

W trzech serwerowniach przechowywano łatwopalne materiały. Z uwagi na prawdopodobieństwo wystąpienia przegrzania macierzy dyskowych lub przepięcia elektrycznego, serwerownia nie powinna być miejscem do składowania jakichkolwiek materiałów lub urządzeń.

Przykłady

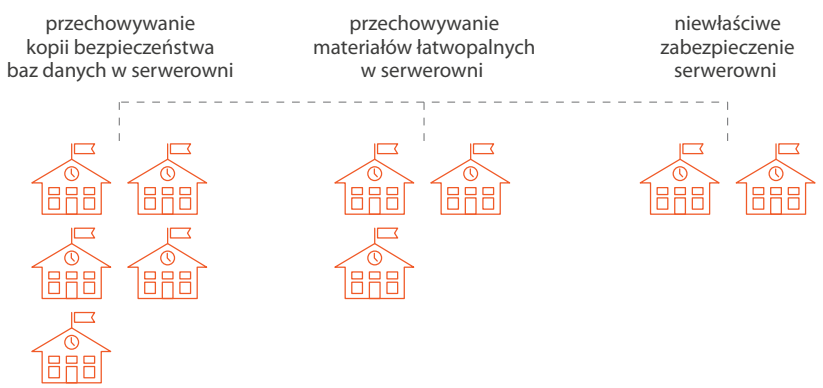
W **Białostockim Centrum Onkologii im. M. Skłodowskiej-Curie w Białymstoku** oraz w **Szpitalu Neuropsychiatrycznym im. prof. Mieczysława Kaczyńskiego SP ZOZ w Lublinie** w pomieszczeniach serwerowni oraz w miejscu, w którym przechowywano kopie zapasowe baz danych szpitala, znajdowały się kartonowe pudła oraz urządzenia informatyczne niepodłączone do infrastruktury. Część z tych przedmiotów była łatwopalna. Usunięto je w trakcie kontroli NIK.

W **SP ZOZ w Augustowie** w pomieszczeniu serwerowni znajdowały się kartonowe opakowania po sprzęcie informatycznym, które usunięto w trakcie kontroli NIK.

Kopie zapasowe danych w 21% szpitali nie były właściwie przechowywane

W celu zabezpieczenia danych przed utratą, sporządza się ich kopie zapasowe (backup). Każdy z podmiotów sam, na podstawie analizy ilości generowanych dziennych danych i podatności systemu na awarie, ustala, jak często należy wykonywać kopie zapasowe danych. Stosuje się przy tym popularną metodę 3–2–1. Zgodnie z nią powinno tworzyć się trzy kopie danych: jedną używaną do pracy, a dwie pozostałe przechowywane na dwóch różnych urządzeniach (chmura, pendrive, zewnętrzny dysk twardy, taśma). Jedno z tych urządzeń powinno być umieszczone poza miejscem przechowywania danych, czyli poza serwerownią główną, na wypadek jej pożaru, zalania lub innego zdarzenia, które zniszczyłoby macierze danych. W pięciu[76] szpitalach (21%) kopie bezpieczeństwa były przechowywane w tym samym miejscu, co dane poddane backupowi. Sytuacja taka naruszała przepisy § 20 ust. 2 pkt 12 lit. b rozporządzenia KRI, zgodnie z którym zapewnienie odpowiedniego poziomu bezpieczeństwa w systemach teleinformatycznych polega w szczególności na minimalizowaniu ryzyka utraty informacji w wyniku awarii oraz była często sprzeczna z regulacjami wewnętrznymi podmiotów leczniczych w tym zakresie.

Infografika nr 16
Przechowywanie kopii bezpieczeństwa baz danych



Źródło: opracowanie własne NIK na podstawie wyników kontroli.

[76] Samodzielny Publiczny Wielospecjalistyczny ZOZ w Stargardzie, SP ZOZ w Augustowie (do 23 lutego 2019 r.), SP ZOZ w Kole, Szpital Ogólny w Kolnie, Zachodniopomorskie Centrum Onkologii w Szczecinie.

6. ZAŁĄCZNIKI

6.1. Metodyka kontroli i informacje dodatkowe

Cel główny kontroli

Celem głównym kontroli było ustalenie, czy dane osobowe w podmiotach leczniczych są prawidłowo chronione i przetwarzane.

Cele szczegółowe

Celami szczegółowymi w jednostkach objętych kontrolą było ustalenie, czy:

- prawidłowo opracowano wymaganą dokumentację i procedury związane z ochroną przetwarzanych danych osobowych,
- wdrożone rozwiązania zapewniają prawidłowe przetwarzanie i ochronę danych osobowych.

Zakres podmiotowy

Kontrolą objęte zostały 24 podmioty lecznicze z sześciu województw: lubelskiego, lubuskiego, małopolskiego, podlaskiego, wielkopolskiego, zachodniopomorskiego.

W każdym z województw do kontroli zostały wybrane dwa szpitale, dla których organem tworzącym jest marszałek województwa oraz dwa powiatowe lub miejskie. Podmioty lecznicze zostały wybrane w sposób celowy, uwzględniający m.in. informacje uzyskane od Rzecznika Praw Pacjenta oraz Prezesa Urzędu, dotyczące skarg lub zawiadomień związanych z nieprzestrzeganiem przez podmioty lecznicze przepisów dotyczących ochrony danych osobowych, a także fakt wdrożenia przez te jednostki zintegrowanych systemów informatycznych.

Kryteria kontroli

Kontrolę przeprowadzono na podstawie art. 2 ust. 2 ustawy o NIK, pod względem legalności i rzetelności, tj. kryteriów określonych w art. 5 ust. 2 ustawy o NIK.

Okres objęty kontrolą

Kontrolą objęto okres od 25 maja 2018 r. (data wejścia w życie przepisów RODO) do dnia zakończenia czynności kontrolnych (w ostatniej jednostce zakończono je 23 kwietnia 2019 r.). Badania kontrolne mogły dotyczyć działań sprzed tego okresu, jeśli miały związek z zagadnieniami będącymi przedmiotem kontroli. Kontrole rozpoczęto 8 stycznia 2019 r., a zakończono 23 kwietnia 2019 r.

Wnioski pokontrolne

Wyniki kontroli przedstawiono w 24 wystąpieniach pokontrolnych, w których sformułowano 132 wnioski pokontrolne. Według stanu na 16 lipca 2019 r. 76 z nich zostało zrealizowanych, 31 było w trakcie realizacji, a 25 nie zrealizowano.

W wystąpieniach do kierowników podmiotów leczniczych objętych kontrolą wnioskowano głównie o:

- zapewnienie w procesie rejestracji i leczenia właściwych środków technicznych i organizacyjnych zapewniających ochronę danych osobowych leczonych pacjentów,
- objęcie pracowników szpitali szkoleniami z zakresu ochrony danych osobowych i zapewnienia bezpieczeństwa danych elektronicznych,
- niezwłoczne odbieranie uprawnień byłym pracownikom szpitali,
- niepodawanie w zgłoszeniach serwisowych danych osobowych pacjentów,
- stosowanie bezpiecznych rozwiązań informatycznych m.in. związanych z nadanymi uprawnieniami w systemie operacyjnym.

Do wystąpienia pokontrolnego skierowanego do Samodzielnego Publicznego Zakładu Opieki Zdrowotnej w Radzyniu Podlaskim złożonych zostało dziesięć zastrzeżeń. Zespół Orzekający Komisji Rozstrzygającej w Najwyższej Izbie Kontroli uwzględnił dwa z tych zastrzeżeń, pozostałe oddalił. Zastrzeżenia dotyczyły głównie interpretacji, czy stwierdzony stan faktyczny jest sytuacją nieprawidłową.

Pozostałe informacje

Kontrola „Wdrożenie przez podmioty lecznicze regulacji dotyczących ochrony danych osobowych" została przeprowadzona w związku z propozycją Komisji Zdrowia Sejmu RP. Kontrolę poprzedziła kontrola rozpoznawcza R/18/002/LBI „Ochrona danych osobowych pacjentów w Samodzielnym Publicznym Zakładzie Opieki Zdrowotnej w Hajnówce".

Wykaz jednostek kontrolowanych

Lp.	Jednostka organizacyjna NIK przeprowadzająca kontrolę	Nazwa jednostki kontrolowanej	Imię i nazwisko kierownika jednostki kontrolowanej
1.	Delegatura NIK w Białymstoku	Białostockie Centrum Onkologii im. M. Skłodowskiej-Curie w Białymstoku	Magdalena Joanna Borkowska
2.		Specjalistyczny Psychiatryczny Zakład Opieki Zdrowotnej w Suwałkach	Bożena Łapińska
3.		Szpital Ogólny w Kolnie	Krystyna Marianna Dobrołowicz
4.		Samodzielny Publiczny Zakład Opieki Zdrowotnej w Augustowie	Danuta Zawadzka
5.	Delegatura NIK w Krakowie	Szpital Specjalistyczny im. Ludwika Rydygiera w Krakowie sp. z o.o.	Wojciech Szafrański
6.		Wojewódzki Specjalistyczny Szpital Dziecięcy im. św. Ludwika w Krakowie	Stanisław Stępniewski
7.		Szpital Miejski Specjalistyczny im. Gabriela Narutowicza w Krakowie	Renata Godyń-Swędzioł
8.		Szpital im. E. Szczeklika w Tarnowie	Marcin Kuta
9.	Delegatura NIK w Lublinie	Wojewódzki Szpital Specjalistyczny im. Stefana Kardynała Wyszyńskiego Samodzielny Publiczny Zakład Opieki Zdrowotnej w Lublinie	Gabriel Maj
10.		Szpital Neuropsychiatryczny im. Prof. Mieczysława Kaczyńskiego Samodzielny Publiczny Zakład Opieki Zdrowotnej w Lublinie	Piotr Dreher
11.		Samodzielny Publiczny Zakład Opieki Zdrowotnej w Radzyniu Podlaskim	Marek Zawada
12.		Samodzielny Publiczny Zakład Opieki Zdrowotnej w Kraśniku	Marek Kos
13.	Delegatura NIK w Poznaniu	Wojewódzki Szpital dla Nerwowo i Psychicznie Chorych „Dziekanka" im. Aleksandra Piotrowskiego w Gnieźnie	Marek Czaplicki
14.		Wielkopolskie Centrum Onkologii im. Marii Skłodowskiej-Curie w Poznaniu	Julian Malicki
15.		Szpital Specjalistyczny im. Stanisława Staszica w Pile	Rafał Szuca
16.		Samodzielny Publiczny Zakład Opieki Zdrowotnej w Kole	Cezary Chmielecki

Lp.	Jednostka organizacyjna NIK przeprowadzająca kontrolę	Nazwa jednostki kontrolowanej	Imię i nazwisko kierownika jednostki kontrolowanej
17.	Delegatura NIK w Szczecinie	Zachodniopomorskie Centrum Onkologii w Szczecinie	Krystyna Pieczyńska
18.		Szpital Wojewódzki im. Mikołaja Kopernika w Koszalinie	Andrzej Kondaszewski
19.		Szpital w Dębnie im. Świętej Matki Teresy z Kalkuty sp. z o.o.	Krzysztof Prętnicki
20.		Samodzielny Publiczny Wielospecjalistyczny Zakład Opieki Zdrowotnej w Stargardzie	Krzysztof Kowalczyk
21.	Delegatura NIK w Zielonej Górze	Lubuski Szpital Specjalistyczny Pulmonologiczno-Kardiologiczny w Torzymiu sp. z o.o.	Katarzyna Lebiotkowska
22.		Samodzielny Publiczny Szpital dla Nerwowo i Psychicznie Chorych w Międzyrzeczu	Ewa Nowak-Lewicka
23.		Powiatowe Centrum Zdrowia Sp. z o.o. Szpital Powiatowy w Drezdenku	Wanda Szumna
24.		Niepubliczny Zakład Opieki Zdrowotnej Szpital im. prof. Z. Religi w Słubicach sp. z o.o.	Łukasz Kaczmarek

Wykaz ocen kontrolowanych jednostek

Lp.	Nazwa jednostki kontrolowanej	Ocena kontrolowanej działalności	Stany mające wpływ na wydaną ocenę:	
			prawidłowe	nieprawidłowe
1.	Białostockie Centrum Onkologii im. M. Skłodowskiej-Curie w Białymstoku	Negatywna	Wyznaczono IOD oraz umożliwiono mu wykonywanie obowiązków w sposób niezależny.	Przekazanie podmiotowi serwisującemu – z naruszeniem art. 24 ust. 2 u.o.p.p. – danych 29 pacjentów szpitala, w tym danych medycznych, zawierających wyniki badań pięciu pacjentów oraz niewłaściwe określenie w umowie powierzenia przetwarzania zakresu danych, który będzie przetwarzał podmiot zewnętrzny. Udostępnienie dokumentacji medycznej pacjenta z naruszeniem procedur wewnętrznych. Odbieranie byłym pracownikom uprawnień w systemie informatycznym z opóźnieniem, wbrew przepisom § 20 ust. 2 pkt 5 rozporządzenia KRI oraz nieprzestrzeganie przez personel regulacji wewnętrznych dotyczących korzystania z komputerów wykorzystywanych do przetwarzania danych medycznych. Niedostosowanie wewnętrznych regulacji do przepisów RODO, mimo wymogu wynikającego z art. 24 tego rozporządzenia, w tym niewprowadzenie środków zapewniających właściwą ochronę danych osobowych oraz minimalizację ryzyka ujawnienia informacji osobom postronnym w procesie rejestracji pacjentów. Dopuszczanie czterech (z 30) objętych badaniem pielęgniarek i położnych do przetwarzania danych osobowych pacjentów, mimo nieudzielenia im upoważnień do przetwarzania danych osobowych, wymaganego art. 32 ust. 4 RODO. Nieterminowe zgłoszenie Prezesowi Urzędu jednego (z 11) incydentu związanego z bezpieczeństwem danych osobowych, co stanowiło naruszenie art. 33 ust. 1 RODO. Przechowywanie m.in. materiałów łatwopalnych w serwerowni oraz pomieszczeniu, w którym znajdowały się kopie bezpieczeństwa baz danych. Niezabezpieczenie miejsc przechowywania podręcznej dokumentacji pielęgniarskiej z danymi osobowymi pacjentów, w dwóch (z trzech) objętych badaniem dyżurkach pielęgniarskich oraz dokumentacji medycznej w jednym (z trzech) poddanych oględzinom gabinecie lekarskim, co naruszało art. 24 ust. 1 RODO.

Lp.	Nazwa jednostki kontrolowanej	Ocena kontrolowanej działalności	Stany mające wpływ na wydaną ocenę:	
			prawidłowe	nieprawidłowe
2.	Samodzielny Publiczny Zakład Opieki Zdrowotnej w Augustowie	Negatywna	Wyznaczono IOD oraz umożliwiono mu wykonywanie obowiązków w sposób niezależny.	Podmiotowi świadczącemu usługi serwisowe przekazano – z naruszeniem art. 5 ust. 1 lit. c RODO – dane osobowe ośmiu pacjentów szpitala, w tym dane medyczne czterech z nich, co nie było konieczne do obsługi zgłoszenia serwisowego. Dokumentacja medyczna czterech pacjentów była udostępniona z naruszeniem art. 26 ust. 1 u.o.p.p oraz procedur wewnętrznych. Regulacje wewnętrzne nie zostały dostosowane do przepisów RODO (naruszenie art. 24 ust. 1 RODO), a pracowników szpitala do czasu kontroli NIK nie przeszkolono z zakresu ochrony danych osobowych i danych medycznych (naruszenie § 20 ust. 2 pkt 6 rozporządzenia KRI). 22 (z 30) objętych badaniem pielęgniarek i położnych dopuszczono do przetwarzania danych osobowych pacjentów z oddziałów lub poradni, na których nie świadczyły pracy, co było niezgodne z art. 5 pkt 1 lit. c RODO. Nie zostały wprowadzone odpowiednie środki techniczne i organizacyjne zapewniające właściwą ochronę danych osobowych oraz minimalizację ryzyka ujawnienia informacji osobom postronnym w procesie rejestracji i leczenia pacjentów. Stanowiło to naruszenie art. 24 ust. 1 RODO. Miejsca przechowywania podręcznej dokumentacji pielęgniarskiej, zawierającej dane osobowe pacjentów, w trzech objętych badaniem dyżurkach pielęgniarskich oraz dokumentacji medycznej w trzech poddanych oględzinom gabinetach lekarskich (za wyjątkiem nielicznych zamykanych szuflad), były niezabezpieczone, co było niezgodne z art. 24 ust. 1 RODO. 11 (z 30 zbadanych) pracownikom przyznano zbyt duże uprawnienia w systemach operacyjnych komputerów, w czterech z 30 komputerów nie zapewniono ochrony antywirusowej i nie zastosowano środków uwierzytelniających podczas rozpoczynania pracy (loginu i hasła), co naruszało § 20 ust. 2 pkt 4, pkt 7 lit. a i pkt 12 rozporządzenia KRI.

Lp.	Nazwa jednostki kontrolowanej	Ocena kontrolowanej działalności	Stany mające wpływ na wydaną ocenę:	
			prawidłowe	nieprawidłowe
3.	Specjalistyczny Psychiatryczny Zakład Opieki Zdrowotnej w Suwałkach	Ocena w formie opisowej	Szpital wprowadził rozwiązania organizacyjne i techniczne zmierzające do zapewnienia prawidłowej ochrony i przetwarzania danych osobowych. Szpital zaktualizował dokumentację i procedury dotyczące ochrony danych osobowych przed wejściem w życie przepisów RODO. Wywiązał się z obowiązku powołania IOD i zgłoszenia tego faktu Prezesowi Urzędu. Przeprowadził także wymaganą analizę ryzyka procesów przetwarzania tych danych. Prawidłowo chroniono i przetwarzano dane osobowe pacjentów w procesie rejestracji i udzielania świadczeń w objętych oględzinami poradniach specjalistycznych oraz w Izbie Przyjęć. Właściwie udostępniano również dokumentację medyczną upoważnionym podmiotom i osobom fizycznym. Personel administracyjny oraz objęte analizą 30 pielęgniarek posiadało uprawnienia w systemie HIS adekwatne do wykonywanych zadań. Wprowadzono odpowiednie zabezpieczenia fizyczne serwerowni szpitala i pomieszczenia pracy informatyka, w których przechowywano dane osobowe przetwarzane w formie elektronicznej.	Podmiotowi świadczącemu usługi serwisowe przekazano dane osobowe pacjenta, co stanowiło naruszenie art. 5 pkt. 1 lit. c RODO. Trzem (z 30 analizowanych) pracownikom nadano uprawnienia w systemie operacyjnym komputerów w zakresie nieadekwatnym do realizowanych zadań i obowiązków. Stanowiło to naruszenie § 20 ust. 2 pkt 4 rozporządzenia KRI. Nie był prowadzony rejestr przetwarzania danych osobowych, wbrew wymogom art. 30 RODO. Personelowi szpitala nie zapewniono szkoleń związanych z wejściem w życie RODO (obligował do tego art. 39 ust. 1 lit. b RODO) oraz z zagadnieniami dotyczącymi ochrony i bezpieczeństwa danych osobowych (§ 20 ust. 2 pkt 6 rozporządzenia KRI). Na trzech objętych oględzinami oddziałach i w trzech gabinetach lekarskich nie przestrzegano regulacji wewnętrznych dotyczących sposobu zabezpieczania papierowej dokumentacji medycznej. Nie był prowadzony rejestr identyfikatorów przyznanych użytkownikom poszczególnych komputerów oraz nie wykonywano kwartalnych kontroli antywirusowych, mimo takiego wymogu wynikającego z regulacji wewnętrznych. Dwóm pracownikom (z 30 analizowanych) nadano uprawnienia w systemie HIS szpitala przed udzieleniem im upoważnienia do przeważania danych osobowych. Było to niezgodne z procedurami wewnętrznymi oraz art. 32 ust. 4 RODO. Jednej osobie udzielono dostępu do systemu HIS bez upoważnienia jej do przetwarzania danych osobowych (naruszenie art. 32 ust. 4 RODO), a kolejnej – bez akceptacji IOD, wymaganej przepisami Polityki Bezpieczeństwa Ochrony Danych Osobowych. Uprawnienia 15 pracownikom posiadającym dostęp do systemów informatycznych szpitala (z 26 analizowanych) odebrano od dziewięciu do 227 dni od zaprzestania przez te osoby świadczenia pracy. Naruszało to § 20 ust. 2 pkt 4 i 5 rozporządzenia KRI.

Lp.	Nazwa jednostki kontrolowanej	Ocena kontrolowanej działalności	Stany mające wpływ na wydaną ocenę:	
			prawidłowe	nieprawidłowe
4.	Szpital Ogólny w Kolnie	Ocena w formie opisowej	Szpital wywiązał się z obowiązku powołania IOD i zgłoszenia tego faktu Prezesowi Urzędu. Przeprowadzono wymaganą analizę ryzyka procesów przetwarzania danych osobowych oraz opracowano rejestr czynności przetwarzania tych danych. Pracowników szpitala zapoznawano zaś z regulacjami dotyczącymi ochrony danych osobowych. W szpitalu prawidłowo chroniono i przetwarzano dane osobowe w skontrolowanych trzech oddziałach szpitalnych, dwóch (z trzech) poradniach specjalistycznych oraz w rejestracji ogólnej do poradni specjalistycznych. Personel administracyjny szpitala przetwarzał dane osobowe w systemie HIS adekwatnie do realizowanych zadań, a byłym pracownikom szpitala zablokowano dostęp do tego systemu. W pięciu analizowanych umowach powierzenia przetwarzania danych osobowych zamieszczono postanowienia wymagane art. 28 RODO. Dokumentację medyczną pacjentów we wszystkich 33 skontrolowanych sprawach udostępniono zaś wyłącznie uprawnionym podmiotom. Zastosowano fizyczne zabezpieczenia serwerowni szpitala, w której przechowywano dane osobowe przetwarzane w formie elektronicznej oraz zminimalizowano ryzyko ich utraty lub nieuprawnionej modyfikacji za pośrednictwem wszystkich 30 objętych kontrolą komputerów.	Dopiero po upływie ponad ośmiu miesięcy od wejścia w życie RODO dostosowano regulacje wewnętrzne szpitala do tego rozporządzenia, co stanowiło naruszenie art. 24 ust. 1 RODO. Nie była prowadzona ewidencja osób upoważnionych do przetwarzania danych osobowych, co było wbrew regulacjom wewnętrznym szpitala. Personel jednej poradni specjalistycznej (z trzech skontrolowanych) nie przestrzegał regulacji wewnętrznych dotyczących sposobu zabezpieczania papierowej dokumentacji medycznej. Czterem (z 30 objętych analizą) pracownikom nadano uprawnienia w systemach informatycznych szpitala w zakresie nieadekwatnym do realizowanych przez nich zadań. Było to niezgodne z § 20 ust. 2 pkt 4 rozporządzenia KRI. Kopie zapasowe elektronicznych baz danych szpitala przechowywano w tym samym pomieszczeniu, w którym przechowywano dane produkcyjne, co było naruszeniem § 20 ust. 2 pkt 12 lit. b rozporządzenia KRI.
5.	Szpital im. E. Szczeklika w Tarnowie	Ocena w formie opisowej	Szpital wywiązał się z obowiązku terminowego sporządzenia procedur dotyczących ochrony danych osobowych, uwzględniając przepisy RODO. Przeprowadzone zostały analizy ryzyka procesów przetwarzania danych. Właściwie wywiązano się z obowiązku powołania IOD i terminowego zgłoszenia tego faktu Prezesowi Urzędu oraz zagwarantowano IOD niezależność w sprawowaniu tej funkcji. Personelowi szpitala zapewniono odpowiedni dostęp do danych medycznych. Podejmowano właściwe działania w celu minimalizacji ryzyka utraty danych osobowych w wyniku awarii, błędów lub nieuprawnionej modyfikacji. Nie stwierdzono przypadków ujawnienia i przekazywania takich danych osobom lub podmiotom nieuprawnionym.	Statut szpitala i regulamin organizacyjny nie zostały dostosowane do zmian wynikających z wejścia w życie RODO. Stanowiło to naruszenie art. 24 ust. 1 RODO. Od 25 maja do 10 lipca 2018 r. nie prowadzono rejestru czynności przetwarzania danych (wbrew art. 30 ust. 1 RODO), a do 4 września 2018 r. nie zostały zaktualizowane: Polityka Bezpieczeństwa i Instrukcja Zarządzania Systemami Informatycznymi (niezgodnie z art. 24 ust. 1 RODO). Pracownikom szpitala nie zorganizowano szkoleń związanych z wejściem w życie przepisów RODO (przeszkolono tylko 5,7% personelu). Stanowiło to naruszenie art. 39 ust. 1 lit. b RODO i § 20 ust. 2 pkt 6 rozporządzenia KRI.

Lp.	Nazwa jednostki kontrolowanej	Ocena kontrolowanej działalności	Stany mające wpływ na wydaną ocenę:	
			prawidłowe	nieprawidłowe
				W celu identyfikacji pacjentów stosowano opaski zawierające dane osobowe, czym naruszono art. 36 ust. 5 u.o.d.l. Dane te umieszczano też na łóżkach chorych, wbrew art. 24 ust. 1 RODO. W dwóch z 50 zgłoszeń usterek oprogramowania przekazanych dostawcy oprogramowania zamieszczono dane osobowe pacjentów, czym złamano zasadę „adekwatności i minimalizacji", wskazaną w art. 5 pkt. 1 lit. c RODO. Ośmiu (z 23) pracownikom szpitala, z którymi rozwiązano stosunek pracy, nie odbierano niezwłocznie dostępu do systemów informatycznych. Było to niezgodne z § 20 ust. 2 pkt 5 rozporządzenia KRI. Dostęp do systemu operacyjnego zainstalowanego na wszystkich 20 poddanych analizie komputerach, użytkowanych przez personel medyczny, wymagał podania tego samego loginu i hasła. Dodatkowo każdy z 30 objętych badaniem użytkowników komputerów posiadał uprawnienia administratora w systemie operacyjnym, chociaż nie realizowali oni zadań związanych z utrzymaniem prawidłowego działania sieci komputerowej i administrowaniem systemami informatycznymi. Naruszało to § 20 ust. 2 pkt 7 lit. a i § 20 ust. 2 pkt 4 rozporządzenia KRI.
6.	Szpital Miejski Specjalistyczny im. Gabriela Narutowicza w Krakowie	Ocena w formie opisowej	W szpitalu prawidłowo sporządzono dokumentację związaną z ochroną danych osobowych oraz dokonywano jej przeglądów i aktualizacji. Wyznaczono IOD i zagwarantowano mu niezależność w sprawowaniu tej funkcji. Zgodnie z wymogiem, określonym w art. 37 ust. 7 RODO, dane IOD oraz sposób i formę kontaktu z nim udostępniono na tablicach informacyjnych, umieszczonych w sąsiedztwie rejestracji. W sposób prawidłowy prowadzono rejestr czynności przetwarzania danych osobowych, przeprowadzano analizy ryzyka procesów przetwarzania danych osobowych, zawarto wymagane umowy powierzenia przetwarzania danych osobowych oraz udostępniano dokumentację medyczną pacjentów.	Danych personalnych i sposobu kontaktu z IOD nie zamieszczono na stronie internetowej szpitala, pomimo takiego obowiązku wynikającego z art. 11 u.o.d.o. Logowanie do stacji roboczych możliwe było przy użyciu jednego konta użytkownika przez wielu pracowników, co wymagało przekazywania pomiędzy nimi haseł do autoryzacji w systemach operacyjnych, uniemożliwiając tym samym ich jednoznaczne rozróżnienie. Hasła te nie spełniały wewnętrznie ustalonych zasad złożoności i nie podlegały okresowej zmianie. Stanowiło to naruszenie § 20 ust. 2 pkt 7 lit. a rozporządzenia KRI. Użytkownikom komputerów przypisywano zbyt wysokie uprawnienia w systemach operacyjnych, co było niezgodne z § 20 ust. 2 pkt 4 rozporządzenia KRI. Nieprawidłowym było nieszyfrowanie dysków twardych komputerów przenośnych, co naruszało § 20 ust. 2 pkt 8 i pkt 9 rozporządzenia KRI.

Lp.	Nazwa jednostki kontrolowanej	Ocena kontrolowanej działalności	Stany mające wpływ na wydaną ocenę:	
			prawidłowe	nieprawidłowe
7.	Szpital Specjalistyczny im. Ludwika Rydygiera w Krakowie sp. z o.o.	Ocena w formie opisowej	W szpitalu prawidłowo sporządzono dokumentację związaną z ochroną danych osobowych oraz dokonywano wymaganych przeglądów i aktualizacji opracowanej dokumentacji. Wyznaczono IOD i zagwarantowano mu niezależność w sprawowaniu tej funkcji. W sposób prawidłowy prowadzono rejestr czynności przetwarzania danych osobowych, przeprowadzano analizy ryzyka procesów przetwarzania danych osobowych, zawarto wymagane umowy powierzenia przetwarzania danych osobowych oraz udostępniano dokumentację medyczną pacjentów. Szpital dokonał jednego zgłoszenia do Prezesa Urzędu stwierdzonego naruszenia ochrony danych osobowych. Należycie dokumentowano też pozostałe naruszenia ochrony takich danych (niewymagające zgłoszenia). W szpitalu podejmowano właściwe działania w celu minimalizacji ryzyka utraty danych osobowych w wyniku awarii, błędów lub nieuprawnionej modyfikacji. Nie stwierdzono przypadków ujawnienia i przekazywania takich danych podmiotom nieuprawnionym.	Szpital nie przesłał w terminie do Prezesa Urzędu informacji o powołaniu IOD, co stanowiło naruszenie art. 10 u.o.d.o. Nie zorganizowano szkoleń związanych z wejściem w życie przepisów RODO w tym dotyczących bezpieczeństwa danych dla całego personelu szpitala uczestniczącego w procesie przetwarzania danych osobowych (naruszenie art. 39 ust. 1 lit. b RODO i § 20 ust. 2 pkt 6 rozporządzenia KRI). Dwóm pracownikom administracji (z 30 skontrolowanych) nadano – nieuzasadniony wykonywanym zakresem obowiązków – dostęp do danych medycznych (posiadali oni pełny dostęp do systemu HIS, tj. do wszystkich informacji z oddziałów, na których komercyjnie leczono pacjentów). W systemie HIS dwie, z 39 osób objętych kontrolą, będących personelem medycznym, posiadały uprawnienia do więcej niż jednej poradni i oddziału o różnej specjalizacji medycznej, tj. niezgodnie z art. 5 pkt 1 lit. c RODO. Uprawnienia dostępu do systemu HIS posiadały dwie osoby, z 30 objętych kontrolą, które przestały być pracownikami szpitala po 25 maja 2018 r. Stanowiło to naruszenie § 20 ust. 2 pkt 4 i 5 rozporządzenia KRI. Na dziewięciu (z 30 skontrolowanych) komputerach stwierdzono niezaktualizowanie baz sygnatur wirusów, co było niezgodne z § 20 ust. 2 pkt 12 rozporządzenia KRI. W 11 z 30 zbadanych przypadków, do systemów operacyjnych komputerów personel szpitala logował się przy jednoczesnym użyciu tych samych: loginu i hasła. Stwierdzono też praktykę stosowania tego samego loginu przez personel medyczny różnych oddziałów, różną złożoność haseł oraz stosowanie loginów w postaci ciągu cyfr, co było niezgodne z § 20 ust. 2 pkt 7 lit. a rozporządzenia KRI oraz dokumentami wewnętrznymi.

Lp.	Nazwa jednostki kontrolowanej	Ocena kontrolowanej działalności	Stany mające wpływ na wydaną ocenę:	
			prawidłowe	nieprawidłowe
8.	Wojewódzki Specjalistyczny Szpital Dziecięcy im. św. Ludwika w Krakowie	Ocena w formie opisowej	W szpitalu prawidłowo sporządzono dokumentację związaną z ochroną danych osobowych oraz dokonywano wymaganych przeglądów i aktualizacji opracowanej dokumentacji. Wprowadzono kompleksowy system zarządzania bezpieczeństwem informacji, zgodnie z § 20 ust. 1 rozporządzenia KRI. Wyznaczono IOD i zagwarantowano mu niezależność w sprawowaniu tej funkcji. Szpital właściwie zrealizował obowiązki związane z przeprowadzeniem analizy ryzyka procesów przetwarzania danych, dokonaniem oceny skutków przetwarzania danych osobowych i prowadzeniem rejestru czynności przetwarzania. Wprowadzone rozwiązania organizacyjne, zmierzające do zapewnienia ochrony danych osobowych pacjentów, gwarantowały poszanowanie ich prywatności. Personelowi szpitala zapewniono odpowiedni dostęp do danych medycznych.	Czterem byłym pracownikom (na 21 objętych analizą) nie odebrano bezzwłocznie możliwości dostępu do systemów informatycznych, co było niezgodne z § 20 ust. 2 pkt 4 i 5 rozporządzenia KRI. Na opaskach identyfikacyjnych pacjentów zamieszczano imię i nazwisko pacjenta, co było sprzeczne z art. 36 ust. 2 i 5 u.o.d.l. W dwóch przypadkach (z 60 analizowanych) szpital przekazał firmie serwisowej, w celu naprawy błędu systemowego, dane medyczne i identyfikacyjne pacjentów, co naruszyło art. 5 pkt 1 lit. c RODO. Nie zaszyfrowano dysków twardych trzech komputerów przenośnych, co było niezgodne z § 20 ust. 2 pkt 12 lit. d rozporządzenia KRI.
9.	Samodzielny Publiczny Zakład Opieki Zdrowotnej w Kraśniku	Ocena w formie opisowej	Szpital opracował i wdrożył dokumentację oraz procedury ochrony danych osobowych. Wyznaczono IOD i terminowo zgłoszono ten fakt Prezesowi Urzędu. Przeprowadzono także analizę ryzyka procesów przetwarzania danych oraz wykonano oceny skutków ich przetwarzania. Dokumentację medyczną pacjentów udostępniano jedynie uprawnionym podmiotom, a analizowane umowy powierzenia przetwarzania danych osobowych spełniały wymagania określone w art. 28 RODO. Szpital zapewnił odpowiednie zabezpieczenia serwerowni, w której przechowywano dane osobowe (przetwarzane elektronicznie). Szpital zminimalizował ryzyko utraty danych medycznych oraz nieuprawnionego dostępu i nieuprawnionej modyfikacji systemu informatycznego poprzez zainstalowanie na wszystkich 30 komputerach programu antywirusowego i ograniczenie uprawnień do wprowadzania zamian w konfiguracji tych urządzeń. Dostęp do systemu operacyjnego wymagał podania hasła i loginu.	Dostawcy oprogramowania – wbrew art. 5 pkt 1 lit. c RODO – w celu usunięcia usterki przekazano dane medyczne pacjentów. W związku z wejściem w życie RODO tylko 52,5% pracowników przeszkolono z ochrony danych osobowych, co stanowiło naruszenie art. 39 ust. 1 lit. b RODO. Nie wszystkich pracowników szpitala zapoznano również z regulacjami dotyczącymi ochrony danych osobowych oraz z zagadnieniami dotyczącymi bezpieczeństwa, co było niezgodne z i § 20 ust. 2 pkt 6 rozporządzenia KRI. Na dwóch oddziałach szpitalnych niewłaściwe zabezpieczono dokumentację medyczną. Pozostawiono też komputer bez odpowiedniego zabezpieczenia, co naruszyło art. 24 ust. 1 RODO. Umożliwiono dostęp do systemów informatycznych szpitala pracownikom, którym nie nadano upoważnień do przetwarzania danych osobowych. Stanowiło to naruszenie art. 32 ust. 4 RODO. Stwierdzono przypadki nieuprawnionego wydania upoważnień do przetwarzania danych medycznych dla personelu pomocniczego szpitala (sanitariusze szpitalni, personel gospodarczy, kierowcy) – naruszenie art. 9 ust. 1 i 2 RODO.

Lp.	Nazwa jednostki kontrolowanej	Ocena kontrolowanej działalności	Stany mające wpływ na wydaną ocenę:	
			prawidłowe	nieprawidłowe
10.	Samodzielny Publiczny Zakład Opieki Zdrowotnej w Radzyniu Podlaskim	Negatywna	W szpitalu powołany został IOD, któremu zapewniono wykonywanie obowiązków w sposób niezależny. Opracował on rejestr czynności przetwarzania danych, przeprowadził analizę przetwarzania danych osobowych w szpitalu i ocenił stopień zapewnienia ich bezpieczeństwa w stosunku do stwierdzonych ryzyk. Przyjęte rozwiązania podczas rejestracji pacjentów, wizyt w gabinetach specjalistycznych oraz hospitalizacji zapewniały ochronę danych osobowych i medycznych pacjentów. Właściwie udostępniano dokumentację medyczną pacjentów oraz zawierano wymagane umowy powierzenia przetwarzania danych osobowych. Szpitalna serwerownia była zabezpieczona przed fizycznym dostępem, a jej wyposażenie zapewniało tworzenie kopii bezpieczeństwa baz danych i ochronę wewnętrznej sieci podmiotu leczniczego.	Podczas zdalnego zgłaszania usterek programów informatycznych, w 10% przypadkach firmom serwisowym przekazano dane medyczne pacjentów, wbrew art. 5 ust. 1 lit. c RODO. Szpital nie zaktualizował wewnętrznych regulacji dotyczących przetwarzania danych osobowych w związku z wejściem w życie RODO, czym naruszył art. 24 ust. 1 RODO. Prezesa Urzędu we właściwej formie zawiadomiono o wyznaczeniu IOD ze studziewięciodniowym opóźnieniem, co było niezgodne z art. 10 ust. 1 u.o.d.o. Szkoleniem z zakresu ochrony danych osobowych objęto jedynie 60,3% personelu, tj. wbrew obowiązkowi wskazanemu w art. 39 ust. 1 lit. b RODO i § 20 ust. 2 pkt 6 rozporządzenia KRI. Na dwóch oddziałach niewłaściwie przechowywano dokumentację medyczną. Było to niezgodne z art. 24 ust. 1 RODO.
11.	Szpital Neuropsychiatryczny im. Prof. Mieczysława Kaczyńskiego Samodzielny Publiczny Zakład Opieki Zdrowotnej w Lublinie	Negatywna	Wyznaczono IOD oraz umożliwiono mu wykonywanie obowiązków w sposób niezależny.	Podmiotowi świadczącemu usługi serwisowe, z naruszeniem art. 5 ust. 1 lit. c RODO, przekazano dane osobowe dwóch pacjentów, w tym dane medyczne jednego z nich. Regulacji wewnętrznych nie dostosowano do RODO (naruszenie art. 24 ust. 1 RODO), a ponad połowy pracowników nie przeszkolono z ochrony danych osobowych i medycznych (wbrew art. 39 ust. 1 lit. b RODO i § 20 ust. 2 pkt 6 rozporządzenia KRI). Jednej osobie (z 30 analizowanych) przyznano uprawnienia w systemach operacyjnych niewiążące się z wykonywanymi zadaniami, tj. wbrew § 20 ust. 2 pkt 4 rozporządzenia KRI. Na czterech (z 30 analizowanych) komputerach nie zastosowano środków uwierzytelniających (loginu i hasła) podczas rozpoczynania pracy, czym naruszono § 20 ust. 2 pkt 4, pkt 7 lit. a i pkt 12 rozporządzenia KRI. Byłym pracownikom z opóźnieniem odebrano uprawnienia w systemie HIS (wbrew § 20 ust. 2 pkt 5 rozporządzenia KRI). Materiały łatwopalne i niewykorzystywany sprzęt komputerowy przechowywano w serwerowni i pomieszczeniu, w którym znajdowały się kopie bezpieczeństwa baz danych, co ograniczało ich bezpieczeństwo.

Lp.	Nazwa jednostki kontrolowanej	Ocena kontrolowanej działalności	Stany mające wpływ na wydaną ocenę:	
			prawidłowe	nieprawidłowe
12.	Wojewódzki Szpital Specjalistyczny im. Stefana Kardynała Wyszyńskiego Samodzielny Publiczny Zakład Opieki Zdrowotnej w Lublinie	Pozytywna	Szpital wywiązał się z obowiązku opracowania, zatwierdzenia i wdrożenia dokumentacji oraz procedur dotyczących ochrony danych osobowych. Personel został właściwie poinformowany o przepisach RODO i regulacjach wewnętrznych. Rzetelnie przeprowadzono analizę ryzyka procesów przetwarzania danych oraz ocenę skutków dla ochrony danych osobowych. Prowadzony rejestr czynności przetwarzania zawierał wszystkie wymagane elementy. Personelowi szpitala zapewniono szkolenia związane z wejściem w życie RODO oraz zagadnieniami dotyczącymi bezpieczeństwa danych, a także zapewniono dostęp do danych medycznych oraz nadano uprawnienia w systemach informatycznych adekwatne do wykonywanych zadań. Rzetelnie wywiązano się z obowiązku zawarcia umów powierzenia przetwarzania danych. Udostępnianie dokumentacji medycznej pacjentów odbywało się zgodnie z obowiązującymi przepisami prawa oraz regulacjami wewnętrznymi. Podejmowano właściwe działania w celu minimalizacji ryzyka utraty danych osobowych w wyniku awarii, błędów lub nieuprawnionej modyfikacji.	Przyjęty w szpitalu sposób oznaczania opasek identyfikacyjnych pacjentów oraz stosowania ramek na karty przyłóżkowe był niezgodny z obowiązującymi w tym zakresie przepisami (odpowiednio art. 36 ust. 5 u.o.d.l. i art. 24 ust. 1 RODO). W jednym z gabinetów w poradni specjalistycznej nie zastosowano odpowiednich środków ochrony podczas nieobecności lekarza, co stwarzało niebezpieczeństwo dostępu do danych osobowych i medycznych pacjentów przez osoby nieuprawnione. Nieterminowo poinformowano również Prezesa Urzędu o wyznaczeniu IOD.
13.	Samodzielny Publiczny Zakład Opieki Zdrowotnej w Kole	Ocena w formie opisowej	Szpital wdrożył Politykę Bezpieczeństwa Informacji, służącą zapewnieniu realizacji celów i zadań z zakresu ochrony danych osobowych. Realizacja tych zadań następowała w sposób zgodny z prawem i skuteczny, przy zapewnieniu odpowiedniego stopnia ochrony praw i wolności osób fizycznych w związku z przetwarzaniem ich danych osobowych. Szpital prawidłowo wyznaczył IOD oraz zapewnił przeszkolenie personelu z przepisów o ochronie danych osobowych. Prowadzono rejestr czynności przetwarzania tych danych oraz dokonano analizy ryzyka procesów ich przetwarzania. Personel posiadał, adekwatne do wykonywanych obowiązków, prawo dostępu do zbioru danych osobowych w systemie informatycznym. Właściwie udostępniano dokumentację medyczną pacjentów i zawierano wymagane umowy powierzenia przetwarzania danych osobowych. Podejmowano też odpowiednie działania w celu minimalizacji ryzyka utraty tych danych.	W szpitalu nie wdrożono logowania do systemów operacyjnych komputerów za pomocą indywidualnych loginów i haseł, przyznając je grupom osób, co naruszało § 20 ust. 2 pkt 7 lit. a i c rozporządzenia KRI. Stwierdzono przypadki przechowywania na komputerach dokumentacji medycznej pacjentów bez uzasadnionego powodu, co w sytuacji niewdrożenia zindywidualizowanego sposobu logowania do systemów operacyjnych komputerów, wymaganego wewnętrznymi regulacjami, mogło zagrażać bezpieczeństwu takich danych i wiązało się z ryzykiem ich ujawnienia osobom nieuprawnionym. Ruch chorych w dyżurkach pielęgniarek prowadzony był w ogólnodostępnym miejscu, co również stwarzało ryzyko ujawnienia tych danych osobom postronnym i było niezgodne z art. 24 ust. 1 RODO. Nie zapewniono odrębnego pomieszczenia dla serwera kopii zapasowej przechowując ją razem z danymi produkcyjnymi, co stanowiło naruszenie § 20 ust. 2 pkt 12 lit. b rozporządzenia KRI. Pięciu byłym pracownikom nie odebrano uprawnień w systemach.

Lp.	Nazwa jednostki kontrolowanej	Ocena kontrolowanej działalności	Stany mające wpływ na wydaną ocenę:	
			prawidłowe	nieprawidłowe
14.	Szpital Specjalistyczny im. Stanisława Staszica w Pile	Ocena w formie opisowej	Wprowadzone rozwiązania organizacyjne, zmierzające do zapewnienia ochrony danych osobowych pacjentów, gwarantowały poszanowanie ich prywatności. Przyjęty w szpitalu system zarządzania bezpieczeństwem informacji odpowiadał wymogom § 20 ust. 1 rozporządzenia KRI. Rzetelnie przeprowadzono analizę ryzyka procesów przetwarzania danych osobowych i oceniono ich skutki oraz właściwie prowadzono związane z tym rejestry. Szkoleniami z zakresu znajomości przepisów RODO oraz zagadnień bezpieczeństwa danych objęto 98% personelu szpitala. Personel szpitala posiadał dostęp do danych medycznych, adekwatny do zakresu wykonywanych przez poszczególne osoby czynności. Byłym pracownikom niezwłocznie odbierano uprawnienia do systemów informatycznych, w których przetwarzano dane osobowe. Prawidłowo zabezpieczano stacje robocze i stanowiska pracy podczas nieobecności pracowników oraz zgodnie z regulacjami wewnętrznymi uwierzytelniano poszczególnych użytkowników systemów informatycznych. Usługa opieki serwisowej nad tymi systemami była zlecona umową, w której zawarto odpowiednie postanowienia zabezpieczające przetwarzanie danych osobowych, a stosowane przy takim przetwarzaniu środki techniczne i organizacyjne zapewniały stopień bezpieczeństwa adekwatny do ryzyk związanych m.in. ze skalą i rodzajem takiego przetwarzania.	Z opóźnieniem zawiadomiono Prezesa Urzędu o powołaniu na stanowisko IOD dotychczasowego administratora bezpieczeństwa informacji, co stanowiło naruszenie art. 158 ust. 2 u.o.d.o. Politykę bezpieczeństwa informatycznego z opóźnieniem dostosowano do obowiązujących od 25 maja 2018 r. przepisów RODO i zawarto 20 umów dotyczących powierzenia podmiotom zewnętrznym przetwarzania danych. Stanowiło to naruszenie art. 24 ust. 1 i art. 28 ust. 3 RODO. Przez kilkanaście miesięcy w szpitalu nie wykorzystywano sprzętu służącego do drukowania znaków identyfikacyjnych, zakupionego za 23,3 tys. zł, co było działaniem niegospodarnym i nie sprzyjało efektywnemu wykorzystaniu tych środków publicznych.
15.	Wielkopolskie Centrum Onkologii im. Marii Skłodowskiej-Curie w Poznaniu	Pozytywna	Regulacje wewnętrzne szpitala związane z ochroną i przetwarzaniem danych osobowych były sporządzone profesjonalnie i kompleksowo. Rzetelnie przeprowadzono analizę ryzyka procesów przetwarzania danych osobowych oraz ocenę skutków ich przetwarzania, jak również prawidłowo prowadzono rejestry dotyczące tych kwestii. Personelowi szpitala zapewniono odpowiedni, zgodny z zakresem wykonywanych czynności, dostęp do danych pacjentów oraz właściwie udostępniano ich dokumentację medyczną. Pracowników zapoznano z przepisami RODO oraz zagadnieniami dotyczącymi bezpieczeństwa danych. Zastosowane środki organizacyjne i techniczne skutecznie przeciwdziałały ujawnieniu danych pacjentów osobom nieuprawnionym oraz ich utracie w wyniku awarii, błędów lub nieuprawnionej modyfikacji. Środki te zapewniały stopień bezpieczeństwa adekwatny do ryzyk związanych m.in. ze skalą i rodzajem przetwarzanych danych osobowych.	Funkcję IOD i Kierownika Działu Informatyki pełniła ta sama osoba, która była jednocześnie zaangażowana w proces określania sposobów i celów przetwarzania danych osobowych, co powodowało konflikt interesów, o którym mowa w art. 38 ust. 6 RODO.

Lp.	Nazwa jednostki kontrolowanej	Ocena kontrolowanej działalności	Stany mające wpływ na wydaną ocenę:	
			prawidłowe	nieprawidłowe
16.	Wojewódzki Szpital dla Nerwowo i Psychicznie Chorych „Dziekanka” im. Aleksandra Piotrowskiego w Gnieźnie	Ocena w formie opisowej	W związku z rozpoczęciem stosowania przepisów RODO w szpitalu opracowano Politykę Bezpieczeństwa Ochrony Danych Osobowych i wdrożono procedury dotyczące ochrony takich danych, tworząc kompleksowy system zarządzania bezpieczeństwem informacji. Realizowano obowiązki związane z analizą ryzyka procesów przetwarzania danych, a wprowadzone rozwiązania zmierzające do zapewnienia ochrony danych osobowych pacjentów gwarantowały poszanowanie ich prywatności. Personelowi szpitala zapewniono dostęp do danych osobowych w zakresie adekwatnym do potrzeb oraz niezwłocznie odbierano go pracownikom, którzy przestali być zatrudniani. Szpitalne komputery były wykorzystywane zgodnie z przeznaczeniem wynikającym z zakresu dostępu personelu do systemów i były odpowiednio zabezpieczone. Prawidłowo udostępniano dokumentację medyczną pacjentów, a w umowach powierzenia przetwarzania danych osobowych zawierano warunki wymagane przez RODO. Pomieszczenie serwerowni było prawidłowo użytkowane, monitorowane i zabezpieczone.	Stwierdzono przypadki wskazujące na możliwość nieuprawnionego ujawnienia danych osobowych pacjentów przy ich rejestrowaniu, prowadzeniu ruchu chorych i przechowywaniu dokumentacji medycznej, co naruszało art. 24 ust. 1 RODO. Przeszkolenie jedynie niewielkiej części pracowników szpitala z przepisów RODO (naruszenie art. 39 ust. 1 lit. b RODO i § 20 ust. 2 pkt 6 rozporządzenia KRI) oraz brak przy jednym ze stanowisk rejestracyjnych klauzuli informacyjnej, o której mowa w art. 13 ust. 1–2 tego rozporządzenia, nie sprzyjały zapewnieniu optymalnego poziomu ochrony danych osobowych w szpitalu. Stwierdzono nieprawidłowości dotyczące: nieaktualizowania regulaminu organizacyjnego (naruszenie art. 24 ust. 1 pkt 3 u.o.d.l.), zamieszczania na stronie internetowej niepełnej informacji o powołaniu IOD (naruszenie art. 11 w zw. z art. 10 ust. 1 u.o.d.o.) oraz nieprowadzenia rejestru podmiotów, którym w drodze umowy powierzono przetwarzanie danych osobowych – taki obowiązek wynikał z dokumentów wewnętrznych szpitala.
17.	Samodzielny Publiczny Wielospecjalistyczny Zakład Opieki Zdrowotnej w Stargardzie	Ocena w formie opisowej	Szpital wywiązał się z obowiązku powołania IOD i zgłoszenia tego faktu Prezesowi Urzędu. Przeprowadzono wymaganą analizę ryzyka procesów przetwarzania danych osobowych oraz opracowano rejestr czynności przetwarzania tych danych. Pracowników szpitala zapoznano z regulacjami dotyczącymi ochrony danych osobowych. 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 adekwatnie do realizowanych zadań i obowiązków. W pięciu analizowanych umowach powierzenia przetwarzania danych osobowych zamieszczono postanowienia wymagane art. 28 RODO. 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.	Pracownikom, z którymi szpital rozwiązał stosunek pracy, nie odbierano uprawnień w systemie HIS, co stanowiło naruszenie § 20 ust. 2 pkt 4 i 5 rozporządzenia KRI. Nie stosowano indywidualnych identyfikatorów i haseł dostępu do systemów operacyjnych na oddziałach szpitala, co było niezgodne z § 20 ust. 2 pkt 7 lit. a i c rozporządzenia KRI. Personel medyczny posiadał pełne uprawnienia administracyjne w systemach operacyjnych, co stanowiło naruszenie § 20 ust. 2 pkt 4 rozporządzenia KRI. Kopie zapasowe elektronicznych baz danych szpitala przechowywano w tym samym pomieszczeniu, w którym przechowywano dane produkcyjne. Było to niezgodne z § 20 ust. 2 pkt 12 lit. b rozporządzenia KRI.

Lp.	Nazwa jednostki kontrolowanej	Ocena kontrolowanej działalności	Stany mające wpływ na wydaną ocenę:	
			prawidłowe	nieprawidłowe
18.	Szpital w Dębnie im. Świętej Matki Teresy z Kalkuty Sp. z o. o.	Ocena w formie opisowej	Szpital wdrożył dokumentację oraz procedury dotyczące ochrony danych osobowych z dniem wejścia w życie RODO. Wdrożył również kompleksowy system zarządzania bezpieczeństwem informacji, określony w § 20 ust. 1 rozporządzenia KRI. Jednak nie wszystkie wytyczne tego systemu były realizowane. Szpital właściwie zrealizował swoje obowiązki związane z przeprowadzeniem analizy ryzyka procesów przetwarzania danych, dokonaniem oceny skutków przetwarzania danych osobowych i prowadzeniem rejestru czynności przetwarzania. Personelowi szpitala zapewniono odpowiedni dostęp do danych medycznych.	Jedynie części personelu szpitala zapewniono szkolenia związane z wejściem w życie RODO oraz zagadnieniami dotyczącymi bezpieczeństwa danych, naruszając tym samym przepisy art. 39 ust. 1 lit. b RODO i § 20 ust. 2 pkt 6 rozporządzenia KRI. Byłym pracownikom szpitala nie odbierano uprawnień do systemów informatycznych. Sześciu pracownikom nadano uprawnienia administratora systemów informatycznych, mimo że nie realizowali oni takich zadań. Stanowiło to naruszenie § 20 ust. 2 pkt 4 i 5 rozporządzenia KRI. Cześć personelu do systemu operacyjnego szpitala logowała się za pomocą loginu i hasła przypisanego dla oddziału lub całego szpitala, co stanowiło to naruszenie § 20 ust. 2 pkt 7 lit. a i § 21 ust. 2 pkt 3, w zw. z § 20 ust. 1 rozporządzenia KRI.
19.	Szpital Wojewódzki im. Mikołaja Kopernika w Koszalinie	Ocena w formie opisowej	Szpital wywiązał się z obowiązku powołania IOD i zgłoszenia tego faktu Prezesowi Urzędu. Zagwarantowano niezależność IOD w sprawowaniu tej funkcji. Przeprowadzono wymaganą analizę ryzyka procesów przetwarzania danych osobowych. Zapewniono całemu personelowi szpitala szkolenia związane z wejściem w życie RODO, a części pracowników szkolenia związane z bezpieczeństwem danych. Założono rejestr czynności przetwarzania, lecz prowadzono go tylko w formie pisemnej. Wprowadzone rozwiązania organizacyjne, zmierzające do zapewnienia ochrony danych osobowych pacjentów, z wyjątkiem Przychodni Onkologicznej, gwarantowały poszanowanie ich prywatności. Personelowi szpitala zapewniono dostęp do danych medycznych adekwatny do realizowanych zadań i obowiązków.	Szpital nie opracował dokumentacji i procedur dotyczących ochrony danych osobowych w oparciu o RODO i u.o.d.o. Do zakończenia kontroli NIK, powołany przez dyrektora szpitala zespół do opracowania projektu Polityki Ochrony Danych Osobowych, nadal pracował nad jego treścią. Było to niezgodne z art. 24 ust. 1 RODO. Wystąpiły przypadki nadania zbyt dużych uprawnień użytkownikom komputerów, braku skutecznej ochrony antywirusowej oraz logowanie do sieci szpitala przez byłego pracownika, co stanowiło naruszenie art. 5 pkt 1 lit. f RODO oraz § 20 ust. 2 pkt 7 i 12 rozporządzenia KRI. Dostawcy oprogramowania w zgłoszeniu serwisowym wysłano dane pacjenta, które nie były konieczne do naprawy usterki. Było to niezgodne z art. 5 pkt. 1 lit. c RODO. Podczas rejestracji do Przychodni Onkologicznej nie w pełni zapewniono pacjentom prawo do zachowania w tajemnicy informacji z nimi związanymi, czym naruszono art. 13 u.o.p.p. i art. 24 ust. 1 RODO. Nie przestrzegano zasad przechowywania dokumentacji medycznej pacjentów w gabinecie lekarskim jednego z oddziałów (naruszenie art. 24 ust. 1 RODO). Pacjentów zaopatrywano w opaski z danymi osobowymi, wbrew art. 36 ust. 5 u.o.d.l.

Lp.	Nazwa jednostki kontrolowanej	Ocena kontrolowanej działalności	Stany mające wpływ na wydaną ocenę:	
			prawidłowe	nieprawidłowe
20.	Zachodniopomorskie Centrum Onkologii w Szczecinie	Ocena w formie opisowej	Szpital wdrożył Politykę Bezpieczeństwa Ochrony Danych Osobowych, służącą zapewnieniu realizacji celów i zadań z zakresu ochrony danych osobowych, które uwzględniały przepisy RODO. Ich aktualizacja i dostosowanie do tych regulacji nastąpiło przed wejściem w życie RODO. Wywiązano się z obowiązku powołania IOD i terminowego zgłoszenia tego faktu Prezesowi Urzędu. Przeprowadzono analizę ryzyka procesów przetwarzania danych osobowych oraz ocenę skutków przetwarzania takich danych, mimo że nie była ona obligatoryjna. Pracowników szpitala zapoznano z regulacjami dotyczącymi ochrony danych osobowych i zagadnieniami dotyczącymi ich bezpieczeństwa. Wszystkie nowo zatrudnione osoby obejmowano szkoleniami indywidualnymi bądź grupowymi. Rejestr czynności przetwarzania zawierał wszystkie wymagane elementy oraz został opracowany przed wejściem w życie RODO. Personel posiadał dostęp do zbioru danych osobowych w zintegrowanym systemie informatycznym w stopniu adekwatnym do wykonywanych obowiązków. W systemie tym zablokowano konta byłych pracowników. Na bieżąco aktualizowano zakresy pisemnych upoważnień do przetwarzania danych osobowych oraz podejmowano odpowiednie działania w celu zminimalizowania ryzyka utraty tych danych.	Wystąpił jeden przypadek przekazania w zgłoszeniu serwisowym danych pacjenta, które nie były konieczne do naprawy usterki. Było to niezgodne z art. 5 pkt. 1 lit. c RODO. Na opaskach nadgarstkowych i kartach przyłóżkowych zamieszczono dane osobowe pacjentów, co stanowiło naruszenie art. 36 ust. 5 u.o.d.l. Nie zawsze przestrzegano przepisów § 20 ust. 2 pkt 12 lit. b rozporządzenia KRI i procedur wewnętrznych podczas udostępniania dokumentacji medycznej pacjentów, zawierania umów powierzenia przetwarzania danych osobowych oraz przechowywania kopii bezpieczeństwa baz danych elektronicznych baz danych szpitala w tym samym pomieszczeniu, w którym przechowywano dane produkcyjne. Nie zaktualizowano rejestru umów powierzenia przetwarzania danych osobowych, do którego prowadzenia obligowały wewnętrzne regulacje szpitala. Stwierdzono przypadek przechowywania na komputerze służbowym dokumentacji medycznej pacjentów, lecz była ona odpowiednio zabezpieczona przed dostępem osób niepowołanych.
21.	Lubuski Szpital Specjalistyczny Pulmonologiczno-Kardiologiczny w Torzymiu Sp. z o.o.	Ocena w formie opisowej	Szpital wywiązał się z obowiązku wdrożenia dokumentacji oraz procedur dotyczących ochrony danych osobowych, a także powołał na stanowisko IOD osobę posiadającą odpowiednie przygotowanie i kwalifikacje zawodowe, a fakt ten zgłosił Prezesowi Urzędu. Opracowany terminowo rejestr czynności przetwarzania danych zawierał wymagane elementy. Rzetelnie przeprowadzono i udokumentowano analizę ryzyka procesów przetwarzania danych. Szpital zawierał umowy powierzenia przetwarzania danych w sytuacjach tego wymagających, a w pięciu analizowanych umowach zamieścił postanowienia wymagane art. 28 RODO. Prawidłowo udostępniano uprawnionym podmiotom dokumentację medyczną pacjentów. Prawidłowo zastosowano też fizyczne zabezpieczenia serwerowni szpitala.	Blisko 60% pracowników szpitala uczestniczących w procesie przetwarzania danych osobowych nie zapoznano z regulacjami dotyczącymi ochrony danych osobowych. Stanowiło to naruszenie art. 39 ust. 1 lit. b RODO i § 20 ust. 2 pkt 6 rozporządzenia KRI. W jednym z oddziałów na łóżkach pacjentów zamieszczano dane osobowe (imię i nazwisko) pacjentów, a w procesie rejestracji na wizyty nie zapewniono pełnej ochrony tych danych. Było to niezgodne z art. 24 ust. 1 RODO. Na skutek nieprowadzenia bieżącej analizy uprawnień personelu szpitala do dostępu do danych medycznych pacjentów, 16 pielęgniarkom (z 30 analizowanych) nadano zbyt szerokie uprawnienia w systemie informatycznym. Stanowiło to naruszenie art. 5 pkt 1 lit. c RODO. Ze znacznym opóźnieniem (od 60 do 274 dni od daty rozwiązania stosunku pracy) byłym pracownikom szpitala odbierano możliwości dostępu do tych systemów. Było to niezgodne z § 20 ust. 2 pkt 4 i 5 rozporządzenia KRI.

Lp.	Nazwa jednostki kontrolowanej	Ocena kontrolowanej działalności	Stany mające wpływ na wydaną ocenę:	
			prawidłowe	nieprawidłowe
				Sposób użytkowania i zabezpieczenia wykorzystywanych w szpitalu komputerów stacjonarnych (badaniami objęto 30 komputerów) nie gwarantował pełnej ochrony danych osobowych pacjentów przetwarzanych na tych komputerach. Nie przestrzegano bowiem wymogów dotyczących haseł oraz wprowadzono praktykę logowania się do systemu operacyjnego z użyciem loginu i hasła wspólnego dla kilku pracowników. Nie odbierano też uprawnień do systemów informatycznych byłym pracownikom. Było to niezgodne z § 20 ust. 2 pkt 7 lit. a i c oraz § 20 ust. 2 pkt 4 rozporządzenia KRI. W pomieszczeniu do przechowywania kopii bezpieczeństwa baz danych nie zapewniono pełnego bezpieczeństwa przechowywanym danym. Stanowiło to naruszenie § 20 ust. 2 pkt 12 lit. b rozporządzenia KRI.
22.	Niepubliczny Zakład Opieki Zdrowotnej Szpital im. prof. Z. Religi w Słubicach sp. z o.o.	Ocena w formie opisowej	Szpital wywiązał się z obowiązku powołania na stanowisko IOD osoby posiadającej odpowiednie przygotowanie i kwalifikacje zawodowe oraz terminowo zawiadomił o tym fakcie Prezesa Urzędu. Wdrożono rozwiązania organizacyjne i techniczne zmierzające do zapewnienia prawidłowej ochrony i przetwarzania danych osobowych. Prawidłowo chroniono i przetwarzano dane osobowe w skontrolowanych trzech oddziałach szpitalnych, trzech poradniach specjalistycznych, a także w punktach rejestracji do poradni szpitalnych oraz szpitalnej izbie przyjęć. Szpital prawidłowo udostępniał uprawnionym podmiotom dokumentację medyczną pacjentów, a prowadzony wykaz udostępniania tych danych był zgodny z obowiązującymi wymogami.	Analiza ryzyka procesów przetwarzania danych osobowych nie objęła wszystkich operacji przetwarzania danych, a zatem nie była kompletna. Niespełna 15% pracowników uczestniczących w procesie przetwarzania danych osobowych zostało przeszkolonych z zagadnień dotyczących bezpieczeństwa danych oraz obowiązywania przepisów RODO. Stanowiło to naruszenie art. 39 ust. 1 lit. b RODO i § 20 ust. 2 pkt 6 rozporządzenia KRI. Personelowi szpitala nadawano zbyt szerokie uprawnienia dostępu do danych w systemach informatycznych oraz upoważniano go do tego dostępu, chociaż część z nich nie realizowała zadań związanych z przetwarzaniem danych osobowych. Stanowiło to naruszenie art. 32 ust. 4 i art. 5 pkt 1 lit. c RODO. Byłym pracownikom możliwość dostępu do systemów informatycznych odbierano zaś ze znacznym opóźnieniem (naruszenie § 20 ust. 2 pkt 4 i 5 rozporządzenia KRI). Nie we wszystkich wymaganych przypadkach szpital zawierał umowy powierzenia przetwarzania danych (wymóg art. 28 RODO), a prowadzony wykaz podmiotów, z którymi zawarto takie umowy był niekompletny. Sposób użytkowania i zabezpieczenia komputerów nie gwarantował – wskutek m.in. nieprzestrzegania wymogów dotyczących haseł oraz możliwości instalowania dowolnego oprogramowania – pełnej ochrony przetwarzanych na tych komputerach danych osobowych pacjentów. Stanowiło to jednocześnie naruszenie § 20 ust. 2 pkt 4 rozporządzenia KRI.

Lp.	Nazwa jednostki kontrolowanej	Ocena kontrolowanej działalności	Stany mające wpływ na wydaną ocenę:	
			prawidłowe	nieprawidłowe
23.	Powiatowe Centrum Zdrowia sp. z o.o. Szpital Powiatowy w Drezdenku	Ocena w formie opisowej	Szpital terminowo opracował dokumentację oraz procedury związane z ochroną przetwarzanych danych osobowych, a także powołał na stanowisko IOD osobę posiadającą odpowiednie przygotowanie i kwalifikacje zawodowe oraz zgłosił ten fakt Prezesowi Urzędu. Opracowany terminowo rejestr czynności przetwarzania zawierał wszystkie wymagane elementy. Przeprowadzono także analizę ryzyka procesów przetwarzania danych oraz ocenę skutków przetwarzania danych osobowych. Personel szpitala uczestniczący w procesie przetwarzania danych osobowych został przeszkolony z zagadnień dotyczących bezpieczeństwa danych oraz obowiązywania przepisów RODO. Wprowadzone rozwiązania organizacyjne, zmierzające do zapewnienia ochrony danych osobowych pacjentów, gwarantowały poszanowanie ich prywatności. Prawidłowo chroniono i przetwarzano dane osobowe w skontrolowanych trzech poradniach specjalistycznych, a także w trzech rejestracjach. Personelowi administracyjnemu szpitala ograniczono dostęp do danych medycznych. Szpital zawierał umowy powierzenia przetwarzania danych w sytuacjach tego wymagających, a w pięciu analizowanych umowach zamieszczono postanowienia wymagane art. 28 RODO. Prawidłowo udostępniano również uprawnionym podmiotom dokumentację medyczną pacjentów. Zastosowano właściwe fizyczne zabezpieczenia serwerowni szpitala, w których przechowywano dane osobowe przetwarzane w formie elektronicznej.	Przy rejestracjach do poradni specjalistycznych nie zamieszczono klauzul informacyjnych RODO (wymóg wynikający z art. 13 RODO), a na oddziałach stosowano opaski dla pacjentów ze znakami identyfikacyjnymi, zapisywanymi w sposób umożliwiający ustalenie tożsamości pacjentów przez osoby nieuprawnione, co było niezgodne z art. 36 ust. 5 u.o.d.l. Pięć (na 30 zbadanych) pielęgniarek miało nadane zbyt szerokie uprawnienia w systemie HIS (naruszenie art. 5 pkt 1 lit. c RODO), a byłym pracowników szpitala ze znacznym opóźnieniem odbierano możliwość dostępu do tego systemu (naruszenie § 20 ust. 2 pkt 4 i 5 rozporządzenia KRI). Sposób użytkowania i zabezpieczenia wykorzystywanych w szpitalu komputerów stacjonarnych (badaniami objęto 30 komputerów) nie gwarantował pełnej ochrony przetwarzanych na tych komputerach danych osobowych pacjentów. Istniała bowiem możliwość instalowania przez użytkowników komputerów oprogramowania, a także praktyka logowania się do systemu operacyjnego z użyciem loginu i hasła wspólnego kilku pracownikom. Stanowiło to naruszenie § 20 ust. 2 pkt 4 i § 20 ust. 2 pkt 7 lit. a i c rozporządzenia KRI.
24.	Samodzielny Publiczny Szpital dla Nerwowo i Psychicznie Chorych w Międzyrzeczu	Ocena w formie opisowej	W szpitalu wywiązano się z obowiązku wdrożenia dokumentacji i procedur dotyczących ochrony danych osobowych, a także powołano na stanowisko IOD osobę posiadającą odpowiednie przygotowanie i kwalifikacje zawodowe oraz zgłoszono ten fakt Prezesowi Urzędu. Opracowany terminowo rejestr czynności przetwarzania zawierał wszystkie wymagane elementy. Przeprowadzono także analizę ryzyka procesów przetwarzania danych oraz ocenę skutków przetwarzania danych osobowych. Prawidłowo chroniono i przetwarzano dane osobowe w skontrolowanych trzech oddziałach szpitalnych, trzech poradniach specjalistycznych, a także – za wyjątkiem usytuowania dwóch okienek rejestracyjnych bezpośrednio obok siebie – w rejestracji ogólnej do poradni specjalistycznych. Personelowi szpitala zapewniono odpowiedni dostęp do danych medycznych i prawidłowo udostępniano uprawnionym podmiotom dokumentację medyczną pacjentów. Prawidłowo zastosowano fizyczne zabezpieczenia serwerowni szpitala oraz pomieszczenia wykorzystywanego do przechowywania danych osobowych przetwarzanych w formie elektronicznej. We wszystkich 30 badanych komputerach zainstalowany był program antywirusowy, aktualny na dzień przeprowadzenia oględzin.	Blisko 30% pracowników szpitala uczestniczących w procesie przetwarzania danych osobowych nie zapoznano z regulacjami dotyczącymi ochrony danych osobowych. Było to niezgodne z art. 39 ust. 1 lit. b RODO i § 20 ust. 2 pkt 6 rozporządzenia KRI. Wystąpiły dwa przypadki pozostawienia zbyt szerokich uprawnień pracownikom nierealizujących zadań związanych z administrowaniem i utrzymaniem sieci komputerowej szpitala. Byłym pracownikom ze znacznym opóźnieniem odbierano możliwość dostępu do systemów informatycznych. Stanowiło to naruszenie art. 5 pkt 1 lit. c RODO, § 20 ust. 2 pkt 4 i 5 rozporządzenia KRI. Sposób użytkowania i zabezpieczenia wykorzystywanych w szpitalu komputerów stacjonarnych nie gwarantował – wskutek m.in. nieprzestrzegania wymogów dotyczących obowiązujących haseł oraz możliwości instalowania dowolnego oprogramowania – pełnej ochrony przetwarzanych na tych komputerach danych osobowych pacjentów. Było to niezgodne z § 20 ust. 2 pkt 4 rozporządzenia KRI.

6.2. Analiza stanu prawnego

Przepisy RODO są bezpośrednio stosowane w Polsce od 25 maja 2018 r. Podlegają im wszystkie placówki medyczne, zarówno publiczne, jak i niepubliczne (prywatne). Regulacje RODO dotyczą zarówno dużych szpitali, zatrudniających liczny personel medyczny, jak i gabinetów lekarskich z jednym tylko lekarzem.

Podstawowe zasady przetwarzania danych osobowych

Przepisy art. 5 RODO określają podstawowe zasady dotyczące przetwarzania danych osobowych. Zgodnie z nimi dane osobowe muszą być:

- przetwarzane zgodnie z prawem, rzetelnie i w sposób przejrzysty dla osoby, której dane dotyczą;
- zbierane w konkretnych, wyraźnych oraz prawnie uzasadnionych celach i nieprzetwarzane dalej w sposób niezgodny z tymi celami;
- adekwatne, stosowne oraz ograniczone do tego, co niezbędne do celów, w których są przetwarzane (tzw. „minimalizacja danych");
- prawidłowe i w razie potrzeby uaktualniane – należy podjąć wszelkie rozsądne działania, aby dane osobowe, które są nieprawidłowe w świetle celów ich przetwarzania, zostały niezwłocznie usunięte lub sprostowane;
- przechowywane w formie umożliwiającej identyfikację osoby, której dane dotyczą, przez okres nie dłuższy, niż jest to niezbędne do celów, w których dane są przetwarzane;
- przetwarzane w sposób zapewniający odpowiednie bezpieczeństwo danych osobowych, w tym ochronę przed niedozwolonym lub niezgodnym z prawem przetwarzaniem oraz przypadkową utratą, zniszczeniem lub uszkodzeniem, za pomocą odpowiednich środków technicznych lub organizacyjnych;
- ADO musi być w stanie wykazać przestrzeganie wszystkich ww. zasad, tzw. „rozliczalność".

Dane osobowe o stanie zdrowia

Art. 4 pkt 15 RODO wskazuje, że dane dotyczące stanu zdrowia oznaczają dane osobowe o zdrowiu fizycznym lub psychicznym osoby fizycznej – w tym o korzystaniu z usług opieki zdrowotnej – ujawniające informacje o stanie jej zdrowia. Natomiast art. 9 ust. 1 RODO zabrania przetwarzania danych dotyczących zdrowia, poza 10 przypadkami, podanymi w art. 9 ust. 2 RODO, w tym gdy jest ono niezbędne do celów zapewnienia opieki zdrowotnej, leczenia lub zarządzania systemami i usługami opieki zdrowotnej.

Zgodnie z art. 4 pkt 12 RODO, naruszenie ochrony danych osobowych oznacza naruszenie bezpieczeństwa, prowadzące do przypadkowego lub niezgodnego z prawem zniszczenia, utracenia, zmodyfikowania, nieuprawnionego ujawnienia lub nieuprawnionego dostępu do danych osobowych przesyłanych, przechowywanych lub w inny sposób przetwarzanych.

Obowiązki administratora

Obowiązki ADO (zdefiniowanego w art. 4 pkt 7 RODO) określa art. 24 RODO. Zgodnie z tym przepisem ADO, uwzględniając charakter, zakres, kontekst i cele przetwarzania oraz ryzyko naruszenia praw lub wolności osób fizycznych o różnym prawdopodobieństwie i wadze zagrożenia, wdraża odpowiednie środki techniczne i organizacyjne, aby przetwarza-

nie odbywało się zgodnie przepisami RODO i aby móc to wykazać. Środki te są w razie potrzeby poddawane przeglądom i uaktualniane (art. 24 ust. 1). W przypadku, gdy jest to proporcjonalne w stosunku do czynności przetwarzania, środki, o których mowa w ust. 1, obejmują wdrożenie przez ADO odpowiednich polityk ochrony danych (art. 24 ust. 2). Stosowanie zatwierdzonych kodeksów postępowania, określonych w art. 40 RODO lub zatwierdzonego mechanizmu certyfikacji, o którym mowa w art. 42 tego rozporządzenia, może być wykorzystane jako element dla stwierdzenia przestrzegania przez ADO ciążących na nim obowiązków (art. 24 ust. 3 RODO).

Przepisy art. 29 oraz art. 32 ust. 4 RODO, wskazują że ADO podejmuje działania w celu zapewnienia, aby każda osoba fizyczna mająca dostęp do danych osobowych, przetwarzała je wyłącznie na podstawie upoważniania ADO i na jego polecenie.

Regulacje art. 28 RODO wprowadzają obowiązek zawierania pisemnych umów powierzenia przetwarzania (dopuszczają także elektroniczną formę takiej umowy). Zgodnie z tym przepisem, umowa taka winna stanowić w szczególności, że podmiot, któremu powierzone zostało przetwarzanie danych m.in.:

dokonuje tego wyłącznie na udokumentowane polecenie ADO oraz zapewnia, by osoby upoważnione do przetwarzania danych osobowych zobowiązały się do zachowania tajemnicy lub by podlegały odpowiedniemu ustawowemu obowiązkowi zachowania tajemnicy,

podejmuje wszelkie niezbędne środki bezpieczeństwa dla ochrony przetwarzanych danych oraz przestrzega warunków korzystania z usług innego podmiotu przetwarzającego, o ile dysponuje szczegółową i pisemną zgodą ADO na dalsze powierzenie,

w miarę możliwości wspiera ADO w wywiązywaniu się przez niego z obowiązków związanych z ochroną danych osobowych, nałożonych treścią rozporządzenia, a także udostępnia ADO wszelkie informacje niezbędne do wykazania spełnienia powyższych obowiązków,

po zakończeniu świadczenia usług związanych z przetwarzaniem, zależnie od decyzji, ADO usuwa lub zwraca wszelkie dane osobowe oraz usuwa wszelkie ich istniejące kopie, chyba że prawo nakazują przechowywanie danych osobowych.

Rejestr czynności przetwarzania

Zgodnie z art. 30 ust. 1 RODO, każdy ADO, przetwarzający dane wrażliwe (szczególne kategorie danych osobowych, o których mowa w art. 9 ust. 1 rozporządzenia), jest zobowiązany do prowadzenia rejestru czynności przetwarzania danych osobowych, za które odpowiada. W rejestrze tym należy zamieścić informacje takie, jak m.in.: [1] nazwę i dane kontaktowe ADO oraz IOD, [2] cele przetwarzania, [3] opis kategorii osób, których dane dotyczą oraz kategorii danych osobowych, [4] kategorie odbiorców, którym dane osobowe zostały lub zostaną ujawnione. Rejestr czynności powinien mieć formę pisemną, w ramach której ustawodawca unijny przewiduje również formę elektroniczną (art. 30 ust. 3 RODO).

Szacowanie ryzyka

W myśl motywu 83 RODO, w celu zachowania bezpieczeństwa i zapobiegania przetwarzaniu niezgodnemu z tym rozporządzeniem, ADO lub podmiot przetwarzający powinien oszacować ryzyko właściwe dla przetwarzania oraz wdrożyć środki minimalizujące to ryzyko. Środki takie powinny zapewnić odpowiedni poziom bezpieczeństwa, w tym poufność, oraz uwzględniać stan wiedzy technicznej i koszty ich wdrożenia w stosunku do ryzyka oraz charakteru danych osobowych podlegających ochronie. Oceniając ryzyko dotyczące bezpieczeństwa danych, należy wziąć pod uwagę ryzyko związane z przetwarzaniem danych osobowych, np. dotyczące przypadkowego lub niezgodnego z prawem zniszczenia, utracenia, zmodyfikowania, nieuprawnionego ujawnienia lub nieuprawnionego dostępu do danych osobowych przesyłanych, przechowywanych lub w inny sposób przetwarzanych, które mogą w szczególności prowadzić do uszczerbku fizycznego, szkód majątkowych lub niemajątkowych.

Zagadnienia związane z bezpieczeństwem przetwarzania danych osobowych reguluje art. 32 RODO. W myśl przepisu tego artykułu, uwzględniając stan wiedzy technicznej, koszt wdrażania oraz charakter, zakres, kontekst i cele przetwarzania oraz ryzyko naruszenia praw lub wolności osób fizycznych o różnym prawdopodobieństwie wystąpienia i wadze zagrożenia, ADO i podmiot przetwarzający mają obowiązek wdrożyć odpowiednie środki techniczne i organizacyjne, aby zapewnić stopień bezpieczeństwa odpowiadający temu ryzyku, w tym m.in. w stosownym przypadku: [1] pseudonimizację i szyfrowanie danych osobowych; [2] zdolność do ciągłego zapewnienia poufności, integralności, dostępności oraz odporności systemów i usług przetwarzania; [3] zdolność do szybkiego przywrócenia dostępności danych osobowych i dostępu do nich w razie incydentu fizycznego lub technicznego; [4] regularne testowanie, mierzenie i ocenianie skuteczności środków technicznych oraz organizacyjnych mających zapewnić bezpieczeństwo przetwarzania (art. 32 ust. 1). Dokonując oceny czy stopień bezpieczeństwa jest odpowiedni, uwzględnia się w szczególności ryzyko wiążące się z przetwarzaniem, w szczególności wynikające z przypadkowego lub niezgodnego z prawem zniszczenia, utraty, modyfikacji, nieuprawnionego ujawnienia lub nieuprawnionego dostępu do danych osobowych przesyłanych, przechowywanych lub w inny sposób przetwarzanych (art. 32 ust. 2). W myśl art. 32 ust. 3, wywiązywanie się przez ADO i podmiot przetwarzający z obowiązków, o których mowa w ust. 1, można wykazać m.in. przez stosowanie zatwierdzonego kodeksu postępowania lub zatwierdzonego mechanizmu certyfikacji, o których mowa w art. 40 i 42 RODO.

Zgłaszanie naruszeń Prezesowi Urzędu

Przepisy art. 33 ust. 1 RODO zobowiązują ADO, aby zgłaszał Prezesowi Urzędu naruszenia ochrony danych osobowych bez zbędnej zwłoki, nie później niż w terminie 72 godzin po ich stwierdzeniu, chyba że jest mało prawdopodobne, by naruszenie skutkowało ryzykiem naruszenia praw lub wolności osób fizycznych. Dodatkowo art. 33 ust. 5 RODO nakłada na ADO obowiązek dokumentowania wszelkich naruszeń ochrony danych osobowych, w tym okoliczności tych naruszeń, ich skutki oraz podjęte działania zaradcze.

Obowiązkiem ADO, określonym w art. 35 RODO, jest dokonanie oceny skutków planowanych operacji przetwarzania dla ochrony danych osobowych, a w przypadku przetwarzania na dużą skalę szczególnych kategorii danych osobowych.

Wyznaczenie IOD

Zgodnie z art. 37 ust. 1 RODO, każdy podmiot publiczny (z wyjątkiem sądów w zakresie sprawowania przez nie wymiaru sprawiedliwości) zobowiązany jest do wyznaczenia IOD. Natomiast art. 37 ust. 5 RODO stanowi, że IOD jest wyznaczany na podstawie kwalifikacji zawodowych, a w szczególności wiedzy fachowej na temat prawa i praktyk w dziedzinie ochrony danych oraz umiejętności wypełnienia zadań, o których mowa w art. 39 RODO. W myśl z art. 38 ust. 3 RODO, należy zapewnić, aby IOD podlegał bezpośrednio najwyższemu kierownictwu, co zapewnić ma mu niezależność. Nie powinien on otrzymywać instrukcji dotyczących sposobu wykonywania swoich obowiązków, ani być odwoływany bądź karany przez ADO za wypełnianie swoich zadań. IOD wprawdzie może wykonywać inne obowiązki, jednak najwyższe kierownictwo zapewnia, aby takie obowiązki nie powodowały konfliktu interesów (art. 38 ust. 6 RODO). Szczegółowe zadania IOD zostały określone w art. 39 RODO.

Kodeksy postępowania

Zgodnie z art. 40 RODO państwa członkowskie i organy nadzorcze zachęcają do sporządzania kodeksów postępowania mających pomóc we właściwym stosowaniu tego rozporządzenia. Jednocześnie wskazano możliwość opracowania lub zmiany kodeksów postępowania albo rozszerzania ich zakresu przez podmioty reprezentujące określone kategorie administratorów (np. szpitale), celem doprecyzowania sposobu stosowania rozporządzenia RODO. Pożądanym stanem jest zatem kierowanie się określonymi standardami pracy, opisanymi w kodeksie dobrych praktyk, medycznym kodeksie branżowym lub innym dokumencie.

Dostęp do danych medycznych

Podkreślić należy, że art. 24 ust. 2 u.o.p.p. ogranicza dostęp do dokumentacji medycznej jedynie do wąskiego grona osób, wykonujących zawód medyczny lub czynności pomocnicze przy udzielaniu świadczeń zdrowotnych, a także czynności związane z utrzymaniem systemu teleinformatycznego, w którym przetwarzana jest dokumentacja medyczna oraz z zapewnieniem bezpieczeństwa tego systemu. Ponadto osoby wykonujące czynności pomocnicze lub dotyczące systemu teleinformatycznego muszą posiadać upoważnienia wydane przez ADO. Zgodnie zaś z art.13 u.o.p.p. każdy pacjent ma prawo do zachowania w tajemnicy przez osoby wykonujące zawód medyczny informacji z nim związanych, uzyskanych w związku z wykonywaniem zawodu medycznego. Zarazem art. 14 u.o.p.p. zobowiązuje osoby wykonujące zawód medyczny do zachowania w tajemnicy informacji związanych z pacjentem, w szczególności ze stanem jego zdrowia.

Zarządzenie bezpieczeństwem informacji

Kluczowe uwarunkowania w odniesieniu do urządzeń i systemów informatycznych wykorzystywanych do przetwarzania danych zostały określone w rozporządzeniu KRI i w rozporządzeniu w sprawie dokumentacji oraz warunków technicznych. Rozporządzenie KRI wskazuje m.in. wymogi dotyczące zarządzania bezpieczeństwem informacji. Przepisy tego rozporządzenia zobowiązują podmioty realizujące zadania publiczne do opracowania, ustanowienia, wdrożenia, monitorowania i dokonywania przeglądów

systemu zarządzania bezpieczeństwem informacji. Zgodnie z § 23 rozporządzenia KRI, systemy teleinformatyczne podmiotów realizujących zadania publiczne funkcjonujące w dniu wejścia w życie tego rozporządzenia, tj. 31 maja 2012 r., należało dostosować w powyższym zakresie, nie później niż w dniu ich pierwszej istotnej modernizacji. Systemy informatyczne nabywane po tej dacie obligatoryjnie podlegają wymogom rozporządzenia KRI.

W myśl § 20 ust 1 rozporządzenia KRI, jednostka realizująca zadania publiczne opracowuje i ustanawia, wdraża i eksploatuje, monitoruje i przegląda oraz utrzymuje i doskonali system zarządzania bezpieczeństwem informacji zapewniający poufność, dostępność i integralność informacji z uwzględnieniem takich atrybutów, jak autentyczność, rozliczalność, niezaprzeczalność i niezawodność. Zarządzanie bezpieczeństwem informacji, zgodnie z § 20 ust. 2 rozporządzenia KRI, realizowane jest w szczególności przez zapewnienie przez kierownictwo podmiotu publicznego warunków umożliwiających realizację i egzekwowanie m.in. następujących działań: [1] zapewnienia aktualizacji regulacji wewnętrznych w zakresie dotyczącym zmieniającego się otoczenia; [2] podejmowania działań zapewniających, że osoby zaangażowane w proces przetwarzania informacji mają stosowne uprawnienia i uczestniczą w tym procesie w stopniu adekwatnym do realizowanych przez nie zadań oraz obowiązków mających na celu zapewnienie bezpieczeństwa informacji; [3] bezzwłocznej zmiany uprawnień, w przypadku zmiany zadań osób zaangażowanych w proces przetwarzania informacji, [4] zapewnienia szkolenia osób zaangażowanych w proces przetwarzania informacji ze szczególnym uwzględnieniem takich zagadnień, jak: zagrożenia bezpieczeństwa informacji, skutki naruszenia zasad bezpieczeństwa informacji, w tym odpowiedzialność prawna, stosowanie środków zapewniających bezpieczeństwo informacji, w tym urządzenia i oprogramowanie minimalizujące ryzyko błędów ludzkich; [5] zabezpieczenia informacji w sposób uniemożliwiający nieuprawnionemu jej ujawnienie, modyfikacje, usunięcie lub zniszczenie; [6] zapewnienia odpowiedniego poziomu bezpieczeństwa w systemach teleinformatycznych, polegającego w szczególności na: dbałości o aktualizację oprogramowania, minimalizowaniu ryzyka utraty informacji w wyniku awarii, ochronie przed błędami, utratą, nieuprawnioną modyfikacją, kontroli zgodności systemów teleinformatycznych z odpowiednimi normami i politykami bezpieczeństwa; [7] bezzwłocznego zgłaszania incydentów naruszenia bezpieczeństwa informacji w określony i z góry ustalony sposób, umożliwiający szybkie podjęcie działań korygujących.

Nowelizacja 168 ustaw

W dniu 4 maja 2019 r. weszła w życie ustawa z dnia 21 lutego 2019 r. o zmianie niektórych ustaw w związku z zapewnieniem stosowania 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)[77], wprowadzająca zmiany w 162 innych usta-

[77] Dz. U. poz. 730.

wach. W obszarze szeroko rozumianej opieki zdrowotnej wprowadzono m.in. zmianę w art. 28 ust. 2a u.o.p.p., zgodnie z którą pacjentowi udostępnia się dokumentację medyczną, otrzymywaną po raz pierwszy, bez opłaty. Po 25 maja 2018 r. funkcjonowały w tym zakresie dwa sprzeczne poglądy. Rzecznik Praw Pacjenta był zdania, że na mocy art. 15 ust. 3 RODO[78] pierwsza kopia dokumentacji medycznej jest bezpłatna. Innego zdania był Prezes Urzędu, według którego udostępnienie kopii danych zawartych w dokumentacji medycznej, nie było równoznaczne z obowiązkiem udostępnienia danych w formie i strukturze właściwych dla dokumentacji medycznej – czyli że wspomniany art. 15 ust. 3 nie dotyczył danych z dokumentacji medycznej. Ustawodawca krajowy doprecyzował więc, że pierwsza kopia dokumentacji medycznej jest bezpłatna.

[78] Administrator dostarcza osobie, której dane dotyczą, kopię danych osobowych podlegających przetwarzaniu. Za wszelkie kolejne kopie, o które zwróci się osoba, której dane dotyczą, administrator może pobrać opłatę w rozsądnej wysokości, wynikającej z kosztów administracyjnych. Jeżeli osoba, której dane dotyczą, zwraca się o kopię drogą elektroniczną i jeżeli nie zaznaczy inaczej, informacji udziela się w powszechnie stosowanej formie elektronicznej.

6.3. Wykaz aktów prawnych dotyczących kontrolowanej działalności

1. Ustawa z dnia 15 kwietnia 2011 r. *o działalności leczniczej* (Dz.U z 2018 r. poz. 2190, ze zm.).
2. Ustawa z dnia 27 sierpnia 2004 r. *o świadczeniach opieki zdrowotnej finansowanych ze środków publicznych* (Dz. U. z 2018 r. poz. 1510, ze zm.).
3. 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 4.05.2016 r., s. 1 ze zm.
4. Ustawa z dnia 10 maja 2018 r. *o ochronie danych osobowych* (Dz. U. poz. 1000, ze zm.).
5. Ustawa z dnia 23 grudnia 1994 r. *o Najwyższej Izbie Kontroli* (Dz. U. z 2019 r. poz. 489).
6. Ustawa z dnia 5 lipca 2018 r. *o krajowym systemie cyberbezpieczeństwa* (Dz. U. poz. 1560).
7. Ustawa z dnia 6 listopada 2008 r. *o prawach pacjenta i Rzeczniku Praw Pacjenta* (Dz. U. z 2017 r. poz. 1318, ze zm.).
8. Ustawa z dnia 17 lutego 2005 r. *o informatyzacji działalności podmiotów realizujących zadania publiczne* (Dz. U. z 2019 r. poz. 700, ze zm.).
9. Rozporządzenie Rady Ministrów z dnia 12 kwietnia 2012 r. *w sprawie Krajowych Ram Interoperacyjności, minimalnych wymagań dla rejestrów publicznych i wymiany informacji w postaci elektronicznej oraz minimalnych wymagań dla systemów teleinformatycznych* (Dz. U. z 2017 r. poz. 2247).

6.4. Wykaz podmiotów, którym przekazano informację o wynikach kontroli

1. Prezydent Rzeczypospolitej Polskiej
2. Marszałek Sejmu Rzeczypospolitej Polskiej
3. Marszałek Senatu Rzeczypospolitej Polskiej
4. Prezes Rady Ministrów
5. Prezes Trybunału Konstytucyjnego
6. Rzecznik Praw Obywatelskich
7. Sejmowa Komisja do Spraw Kontroli Państwowej
8. Sejmowa Komisja Zdrowia
9. Sejmowa Komisja Cyfryzacji, Innowacyjności i Nowoczesnych Technologii
10. Sejmowa Komisja Administracji i Spraw Wewnętrznych
11. Sejmowa Komisja Sprawiedliwości i Praw Człowieka
12. Senacka Komisja Zdrowia
13. Senacka Komisja Praw Człowieka, Praworządności i Petycji
14. Prezes Urzędu Ochrony Danych Osobowych
15. Minister Cyfryzacji
16. Minister Spraw Wewnętrznych i Administracji
17. Minister Zdrowia
18. Rzecznik Praw Pacjenta
19. Marszałkowie województw
20. Wójtowie gmin, burmistrzowie i prezydenci miast
21. Starostowie powiatów
22. Publiczne podmioty lecznicze

Informację o wynikach kontroli opublikowano na stronie internetowej:
http://bip.nik.gov.pl/kontrole/wyniki-kontroli-nik/

6.5. Stanowisko Prezesa Urzędu Ochrony Danych Osobowych

PREZES
URZĘDU OCHRONY
DANYCH OSOBOWYCH
Jan Nowak

Warszawa, dnia 9 września 2019 r.

ZSZZS.023.387.2019.NS/MP

Pani
Ewa Polkowska
Wiceprezes
Najwyższej Izby Kontroli
ul. Filtrowa 57
02-056 Warszawa
Adres skrytki na ePUAP:
/NIK/SkrytkaESP

Szanowna Pani Prezes,

w odpowiedzi na pismo z 20 sierpnia 2019 r. (znak: LBI.430.004.2019), które wpłynęło do Urzędu Ochrony Danych Osobowych 26 sierpnia br., dotyczące informacji o wynikach kontroli P/19/063 Wdrożenie przez podmioty lecznicze regulacji dotyczących ochrony danych osobowych oraz w związku z przysługującym - na mocy art. 64 ust. 2 ustawy z dnia 23 grudnia 1994 r. o Najwyższej Izbie Kontroli (Dz. U. z 2019 r. poz. 489) - uprawnieniem proszę o przyjęcie poniższego stanowiska.

W treści informacji o wynikach kontroli Prezes Najwyższej Izby Kontroli (Prezes NIK) w części dotyczącej wniosków sformułował dla Prezesa Urzędu Ochrony Danych Osobowych (Prezesa Urzędu) dwa zadania, tj. przeprowadzenie systemowych kontroli przestrzegania zasad ochrony danych osobowych w jednostkach z sektora ochrony zdrowia (pkt 1), a także niezwłoczne zakończenie działań związanych z przyjęciem Kodeksu postępowania dla sektora ochrony zdrowia oraz wprowadzenie regulacji dotyczących certyfikacji, o której mowa w art. 42 RODO (pkt 2).

Odnosząc się do zadania dotyczącego przeprowadzenia systemowych kontroli, zgodnie z art. 78 ustawy z dnia 10 maja 2018 r. o ochronie danych osobowych (Dz. U. z 2018 r. poz. 1000 z późn. zm.) Prezes Urzędu przeprowadza kontrolę przestrzegania przepisów o ochronie danych osobowych (ust. 1), którą prowadzi się zgodnie z zatwierdzonym przez Prezesa Urzędu planem kontroli lub na podstawie uzyskanych przez Prezesa Urzędu informacji lub w ramach monitorowania przestrzegania stosowania rozporządzenia 2016/679 (ust. 2). Plan kontroli, o którym mowa powyżej został opublikowany na stronie internetowej urzędu pn. Roczny plan kontroli sektorowych na 2019

rok. W części dotyczącej sektora zdrowia w 2019 roku zaplanowano przeprowadzenie kontroli w podmiotach udzielających świadczeń zdrowotnych dotyczących przetwarzania danych osobowych w związku z udostępnianiem dokumentacji medycznej w ramach realizacji praw pacjenta do dostępu do dokumentacji medycznej dotyczącej jego stanu zdrowia oraz udzielonych mu świadczeń zdrowotnych. Mając na uwadze powyższe, zakres planowanych przez Prezesa Urzędu kontroli sektorowych dotyczy zgodności przestrzegania zasad ochrony danych osobowych w jednostkach z sektora ochrony zdrowia, co jest zbieżne z wnioskami sformułowanymi przez Prezesa NIK. Na marginesie należy wskazać, że Prezes Urzędu podejmuje również działania w powyższym zakresie poprzez prowadzenie skargowych postępowań administracyjnych.

W odniesieniu do kwestii niezwłocznego zakończenia działań związanych z przyjęciem Kodeksu postępowania dla sektora ochrony zdrowia należy wskazać, że obecnie trwają prace związane z analizą i oceną przedłożonych do zatwierdzenia Prezesowi Urzędu dwóch projektów kodeksów postępowań z zakresu sektora zdrowia (Kodeks postępowania dotyczący ochrony danych osobowych przetwarzanych w małych placówkach medycznych przedłożony w dniu 5.09.2018 r. oraz Kodeks postepowania dla sektora ochrony zdrowia wydany zgodnie z art. 40 RODO dotyczący podmiotów wykonujących działalność leczniczą i podmiotów przetwarzających przedłożony w dniu 13.11.2018 r.). Oba projekty kodeksów mają na celu umożliwienie łatwiejszego i skuteczniejszego wdrożenia i stosowania przepisów RODO czego skutkiem będzie podniesienie poziomu ochrony danych osobowych pacjentów oraz doprecyzowanie praw i obowiązków pacjentów i podmiotów leczniczych we wzajemnych relacjach w kontekście przetwarzanych danych osobowych.

Zważywszy na poruszaną w kodeksach materię, tj. przetwarzanie danych wrażliwych pacjentów, którymi są dane o ich stanie zdrowia oraz spoczywający na organie nadzorczym obowiązek wyważenia prawa do ochrony danych osobowych względem innych praw podstawowych w myśl zasady proporcjonalności, nie można, na obecnym etapie prac nad przedmiotowymi kodeksami, wskazać terminu ich zakończenia. Tym bardziej próba niezwłocznego zakończenia prac nad nimi mogłaby prowadzić do pozostawienia w kodeksach postanowień skutkujących ich nadinterpretacją, a w konsekwencji ich błędnym stosowaniem obniżającym znacząco poziom ochrony danych osobowych pacjentów. Taki stan rzeczy zaprzeczałby idei przyświecającej sporządzaniu kodeksów, które mają pomóc we właściwym stosowaniu RODO, jako instrumentów zapewniających wykazywanie zgodności z RODO.

W odniesieniu do treści merytorycznej kodeksów należy wskazać, że aktualnie trwają intensywne konsultacje między organem nadzorczym a wnioskodawcami zmierzające do uspójnienia stanowisk w kwestii stosowania m.in. monitoringu w podmiotach leczniczych, badań jakości wykonywanych usług przez te podmioty, stosowania profilaktyki z wykorzystaniem środków teleinformatycznych oraz ich działalnością marketingową. W tym kontekście niepokojące dla Prezesa Urzędu jest stwierdzenie w informacji o wynikach kontroli, że część skontrolowanych podmiotów leczniczych stosowało już kodeks przedłożony Prezesowi Urzędu w dniu 13 listopada 2018 r. dopiero do zatwierdzenia, w sytuacji której część poruszonych w nim kwestii nie zostało jeszcze wyjaśnionych i uzgodnionych między organem nadzorczym a wnioskodawcami kodeksu.

Podsumowując powyższe, należy wskazać, że Prezes UODO wyda opinię o zgodności projektów kodeksów, z RODO i zatwierdzi je, jeżeli uzna, że będą one stanowić odpowiednie zabezpieczenie dla ochrony danych osobowych.

W części dotyczącej wprowadzenia regulacji dotyczących certyfikacji należy wskazać, że w 2018 i 2019 roku Urząd wraz z Europejską Radą Ochrony Danych prowadził konsultacje dotyczące wytycznych w sprawie certyfikacji i identyfikacji kryteriów certyfikacji zgodnie z art. 42 i 43 Rozporządzenia 2016/67 oraz wytycznych w sprawie akredytacji jednostek certyfikujących na podstawie art. 43 ogólnego rozporządzenia o ochronie danych (2016/679), które zostały przyjęte w dniu 4 czerwca br., a obecnie prowadzone są prace nad tłumaczeniem ostatecznych wersji na język polski. Przyjęcie przez Europejską Radę Ochrony Danych, po konsultacjach publicznych, ostatecznej wersji powyższych dokumentów umożliwi przygotowanie przez Urząd Ochrony Danych Osobowych projektu wymogów akredytacji podmiotów certyfikujących, o których mowa w art. 43 ust. 3 rozporządzenia 2016/679, a następnie przekazanie go Europejskiej Radzie Ochrony Danych do zaopiniowania w ramach procedury spójności określonej w art. 63 RODO.

Mając na uwadze powyższe, zadania sformułowane przez Prezesa NIK dotyczące działań, które powinny zostać podjęte przez Prezesa Urzędu, pozostają spójne z obecnie prowadzonymi działaniami organu na nadzorczego.

Z poważaniem,

Prezesa Urzędu
Ochrony Danych Osobowych
Jan Nowak

6.6. Opinia Prezesa NIK do stanowiska Prezesa Urzędu

PREZES
NAJWYŻSZEJ IZBY KONTROLI
MARIAN BANAŚ

LBI.430.004.2019
P/19/063

Warszawa, dnia 16 września 2019 r.

Opinia
Prezesa Najwyższej Izby Kontroli
do Stanowiska Prezesa Urzędu Ochrony Danych Osobowych w sprawie informacji o wynikach kontroli
Wdrożenie przez podmioty lecznicze regulacji dotyczących ochrony danych osobowych

Stosownie do art. 64 ust. 2 ustawy z dnia 23 grudnia 1994 r. o Najwyższej Izbie Kontroli[1], przedstawiam opinię do Stanowiska Prezesa Urzędu Ochrony Danych Osobowych, zawartego w piśmie z 9 września 2019 r. (znak: ZSZZS.023.387.2019.NS/MP).

Najwyższa Izba Kontroli z satysfakcją przyjmuje do wiadomości fakt niezgłaszania przez Prezesa Urzędu Ochrony Danych Osobowych uwag do wniosków zawartych w *Informacji*.

Ze szczególnym zadowoleniem przyjmuję stanowisko, w którym Pan Prezes podkreśla potrzebę kontroli podmiotów leczniczych oraz informuje o pracach nad opracowaniem ostatecznej treści *Kodeksu postępowania dla sektora ochrony zdrowia*. Ze względu na niezapewnienie przez prawie wszystkie skontrolowane szpitale prawidłowej ochrony i przetwarzania danych osobowych pacjentów oraz wagę problemu, jakim jest ochrona ich prywatności, Najwyższa Izba Kontroli uważa, że istotne jest jak najszybsze zakończenie prac nad przyjęciem tego dokumentu. Może być on bowiem narzędziem skutecznie wspomagającym podmioty lecznicze we wdrażaniu rozwiązań organizacyjnych i technicznych zapewniających odpowiednią ochronę danych osobowych pacjentów.

PREZES
Najwyższej Izby Kontroli
Marian Banaś

[1] Dz. U. z 2019 r. poz. 489, ze zm.