Wdrażanie RODO przez podmioty lecznicze

Ochrona danych osobowych pacjentów

PAWEŁ TOŁWIŃSKI

Regulacje wprowadzone przepisami RODO zmieniły zasady przetwarzania, wykorzystywania i przechowywania danych osobowych oraz nałożyły nowe obowiązki na ich administratorów. Podmioty prowadzące działalność leczniczą musiały dokonać przeglądu i sprawdzić skuteczność stosowanych rozwiązań. Najwyższa Izba Kontroli oceniła[1] efekty tych działań w wybranych szpitalach. Niemal we wszystkich skontrolowanych placówkach nie zapewniono właściwego bezpieczeństwa i odpowiedniego sposobu przetwarzania danych osobowych pacjentów.

RODO a dane pacjentów

W Polsce przepisy RODO[2] zaczęły obowiązywać od 25 maja 2018 r. W tym samym czasie weszły też w życie regulacje z nim związane, określone w znowelizowanej ustawie o ochronie danych osobowych[3]. Konieczność stosowania tych norm prawnych dotyczy wszystkich placówek medycznych, publicznych i niepublicznych. Nie ma również znaczenia skala działalności takiego podmiotu. Przepisy RODO muszą być przestrzegane zarówno w dużych szpitalach, zatrudniających wielu lekarzy, pielęgniarek i położnych, jak również w gabinetach, gdzie prowadzona jest indywidualna praktyka lekarska.

Najważniejsze zmiany, jakie wprowadzono, dotyczyły sposobu przetwarzania, wykorzystywania i przechowywania danych osobowych oraz nałożenia nowych obowiązków na Administratora Danych Osobowych (ADO)[4]. Wszystkie jednostki prowadzące działalność leczniczą

[1] Artykuł opracowany na podstawie Informacji o wynikach kontroli: *Wdrożenie przez podmioty lecznicze regulacji dotyczących ochrony danych osobowych*, nr ewid. 149/2019/P/19/063/LBI, Delegatura NIK w Białymstoku, listopad 2019 r., <www.nik.gov.pl/kontrole/P/19/063/>.

[2] Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2016/679 z 27.4.2016 *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 4.5.2016, s. 1, ze zm.).

[3] Ustawa z 10.5.2018 *o ochronie danych osobowych* (Dz.U. z 2019 r. poz. 1781).

[4] Administrator Danych Osobowych – 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).

w związku z wejściem w życie nowych przepisów zostały obowiązane do dokonania analizy i przeglądu stosowanych rozwiązań dotyczących ochrony danych osobowych oraz sprawdzenia ich skuteczności.

RODO w przeciwieństwie do wcześniej obowiązujących przepisów, wprowadza jedynie ogólne zasady zarządzania bezpieczeństwem danych osobowych. Nie określa, jak należy prowadzić dokumentację ich przetwarzania oraz nie wskazuje, jakie metody do właściwej ochrony tych danych powinien zastosować zarządzający jednostką. W rezultacie, już przed wejściem w życie przepisów RODO kierownicy podmiotów prowadzących działalność leczniczą zgłaszali wątpliwości z tym związane.

Odpowiedzią na to było m.in. podjęcie już w 2017 roku działań, które miały na celu opracowanie „Kodeksu postępowania dla sektora ochrony zdrowia". Chciano tam zawrzeć zbiór zasad zgodnych z RODO i ustawodawstwem krajowym dotyczących podnoszenia poziomu ochrony osób fizycznych w związku z przetwarzaniem danych osobowych.

Stosowanie Kodeksu miało stanowić potwierdzenie wywiązywania się z obowiązków nałożonych wyżej wymienionymi regulacjami na ADO oraz podmioty przetwarzające, które działają na rynku wykonujących działalność leczniczą. Kodeks miał więc służyć realizacji zasady rozliczalności, czyli obowiązkowi wykazania, że są przestrzegane zasady ochrony danych osobowych wymienionych w art. 5 ust. 1 RODO.

Jak wynika z informacji zamieszczonych na stronie <www.rodowzdrowiu.pl>, dokument – wraz z wnioskiem o jego przyjęcie – został złożony do Prezesa Urzędu Ochrony Danych Osobowych (dalej: PUODO) 13 listopada 2018 r. Następnie jego zaktualizowaną wersję przekazano do Urzędu 11 października 2019 r.

Innym działaniem, które miało na celu zapewnienie właściwej implementacji RODO było powołanie w Ministerstwie Cyfryzacji, w lipcu 2018 roku, Grupy Roboczej ds. Ochrony Danych Osobowych w Ministerstwie Cyfryzacji. W efekcie jej działania we wrześniu 2018 roku stworzono i opublikowano „Przewodnik po RODO dla Służby Zdrowia". Wskazano w nim odpowiedzi na najczęściej pojawiające się pytania dotyczące m.in.: metod rejestracji pacjentów z poszanowaniem ich prywatności, kwestii związanych z opisywaniem leków dla pacjenta w sposób umożliwiający jego identyfikację, zagadnień dotyczących możliwości zamieszczania tabliczek ze specjalnością lekarza na drzwiach gabinetów oraz o stanie zdrowia na tzw. kartach przyłóżkowych[5].

Rozporządzenie RODO już na etapie preambuły definiuje pojęcie danych osobowych dotyczących zdrowia. W myśl motywu 35. są nimi „...wszystkie dane o stanie zdrowia osoby, której dane dotyczą, ujawniające informacje o przeszłym, obecnym lub przyszłym stanie fizycznego lub psychicznego zdrowia konkretnej osoby". Ponadto do danych medycznych zaliczane są również informacje pochodzące

[5] https://www.gov.pl/cyfryzacja/rodo-w-sluzbie-zdrowia-po-pierwsze-pacjent>, dostęp 16.4.2020.

z badań laboratoryjnych lub lekarskich o częściach ciała lub płynach ustrojowych, w tym (co stanowi nowość w porównaniu z przepisami krajowymi obowiązującymi przed wejściem RODO), 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 albo badanie diagnostyczne *in vitro*.

RODO wskazuje również, że dane dotyczące zdrowia stanowią, w myśl art. 9 ust. 1, szczególną kategorię danych osobowych, których przetwarzanie jest zabronione, chyba że zostanie spełniony jeden z 10 warunków wskazanych w art. 9 ust. 2 tego rozporządzenia. Stosowanie się do tych postanowień jest istotne dla zachowania właściwej ochrony prywatności pacjentów i szczególnie ważne tam, gdzie ujawnienie danych może wiązać się z pewnego rodzaju stygmatyzacją, np. w przychodniach i oddziałach psychiatrycznych szpitali.

Ministerstwo Zdrowia na swojej stronie internetowej wskazuje m.in., że „...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”[6]. Postęp technologiczny sprawia, że coraz częściej do gromadzenia, przechowywania i przetwarzania danych osobowych są wykorzystywane systemy informatyczne. W efekcie korzystanie np. z Internetu i połączeń sieciowych, które umożliwiają wymianę informacji i przepływ danych medycznych, stwarza ryzyko wystąpienia nieuprawnionego dostępu, przejęcia lub zniszczenia tych zasobów. Przy tych zagrożeniach warto wspomnieć, że dane medyczne są bardzo cennymi informacjami dla cyberprzestępców. Potwierdzają to liczne doniesienia medialne, m.in. o ujawnieniu dokumentów z danymi osobowymi i medycznymi pacjentów, znajdującymi się w wielu szpitalach. Były to dane dostępowe do różnych systemów informatycznych oraz osobowe pracowników szpitali[7]. Co szczególnie istotne, część upublicznionych informacji dotyczyła szpitali psychiatrycznych oraz ich pacjentów.

Założenia i wybrane ustalenia kontroli

Kontrola przeprowadzona w 24 szpitalach z terenu sześciu województw[8] wykazała, że jedynie trzy[9] z nich wprowadziły rozwiązania organizacyjne i techniczne,

[6] https://www.gov.pl/web/zdrowie/informatyzacja-w-ochronie-zdrowia, dostęp 16.4.2020.

[7] https://niebezpiecznik.pl/post/dane-pacjentow-i-szpitali-wyciekly-z-helpdesku-eskulapa-szpitale-powinny-zmienic-hasla/, dostęp 16.4.2020.

[8] 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.

[9] 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.

które stwarzały odpowiednie warunki rejestracji wizyt do lekarza, identyfikacji pacjenta na oddziale i przechowywania jego papierowej dokumentacji medycznej. Pozostałe nie zapewniły skutecznej ochrony danych osobowych i medycznych pacjentów przed ujawnieniem osobom postronnym.

Przygotowanie organizacyjne

W art. 32 RODO wprowadzono obowiązek wdrożenia odpowiednich środków technicznych i organizacyjnych, które powinny zapewnić stopień bezpieczeństwa odpowiadający stwierdzonemu ryzyku. Wiąże się to z koniecznością przeprowadzenia analizy ryzyka dotyczącego procesów przetwarzania danych osobowych oraz wynikającego z przypadkowego lub niezgodnego z prawem zniszczenia bądź nieuprawnionego dostępu do danych przesyłanych, przechowywanych albo w inny sposób przetwarzanych. Z tego obowiązku do chwili wejścia przepisów RODO wywiązało się jedynie 13 skontrolowanych szpitali[10] (54,2%), a kolejne dziewięć wykonało analizę do końca 2018 roku. W dwóch pozostałych natomiast impulsem do jej przeprowadzenia była dopiero kontrola NIK. Wprawdzie RODO nie określa kiedy analiza miałaby zostać przeprowadzona i w jakiej formie, jednak – zdaniem Najwyższej Izby Kontroli – powinna być wykonana w terminie umożliwiającym podjęcie właściwych decyzji dotyczących zapewnienia środków technicznych i organizacyjnych związanych z bezpieczeństwem danych osobowych. Opóźnienie obniżało więc jego poziom.

Kolejnym istotnym elementem służącym zagwarantowaniu ochrony praw i wolności osób fizycznych w związku z przetwarzaniem danych osobowych jest wdrożenie odpowiednich środków technicznych i organizacyjnych. Obowiązek ten spoczywa na ADO (w myśl art. 24 ust. 1 RODO), w 11 skontrolowanych podmiotach leczniczych (46%), według stanu na dzień wejścia w życie RODO, nie były jednak zaktualizowane podstawowe dokumenty opisujące bezpieczeństwo danych i sposoby ich przetwarzania. W siedmiu[11] z nich aktualizację wewnętrznej dokumentacji dokonano z opóźnieniem, a w czterech[12]

[10] 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.

[11] 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.

[12] 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.

do zakończenia kontroli NIK nadal jej nie zaktualizowano.

Jedynym dokumentem, jakiego opracowanie i forma wynika bezpośrednio z przepisów RODO, jest rejestr czynności przetwarzania. Zastąpił on rejestry zbiorów danych osobowych, prowadzone do 25 maja 2018 r. na podstawie przepisów dawnej ustawy o ochronie danych osobowych. Rejestr czynności powinien stanowić kompleksową ewidencję wszystkich operacji dokonywanych przez szpitale na danych osobowych. W poprzednim stanie prawnym podmioty lecznicze nie miały obowiązku rejestracji zbiorów zawierających dane korzystających z usług medycznych[13]. Większość skontrolowanych szpitali wypełniła obowiązek założenia i prowadzenia rejestru czynności przetwarzania. Mimo tego sześć[14] podmiotów leczniczych opracowało go z opóźnieniem (od 12 do 263 dni po wejściu w życie RODO). W Specjalistycznym Psychiatrycznym ZOZ w Suwałkach rejestru nie założono do końca kontroli NIK, co argumentowano zmianą na stanowisku Inspektora Ochrony Danych (IOD)[15] oraz dużą ilością innych obowiązków.

Wprawdzie we wszystkich skontrolowanych placówkach powołano IOD, jednak w pięciu[16] szpitalach ADO poinformował o tym PUODO z opóźnieniem, a w trzech[17] kolejnych na stronach internetowych podmiotów leczniczych nie zamieszczono danych IOD oraz sposobu i formy kontaktu z nim, mimo że obowiązek taki wynikał z przepisów RODO.

Szkolenia a naruszenia ochrony danych

Do naruszeń ochrony danych osobowych doszło w ponad połowie skontrolowanych szpitali[18], przy czym w sześciu sytuacja stała się na tyle poważna, że konieczne było powiadomienie PUODO. Jeden

[13] Art. 43 ust. 1 pkt 5 ustawy z 29.8.1997 o ochronie danych osobowych (Dz.U. z 2016 r. poz. 922, ze zm.), według stanu prawnego na 24.5.2018.

[14] 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.

[15] O którym mowa w art. 37 RODO.

[16] 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.

[17] Specjalistyczny Psychiatryczny ZOZ w Suwałkach, Szpital Miejski Specjalistyczny im. Gabriela Narutowicza w Krakowie, Wojewódzki Szpital dla Nerwowo i Psychicznie Chorych „Dziekanka" im. Aleksandra Piotrowskiego w Gnieźnie.

[18] 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.

z incydentów dotyczył kradzieży trzech kartotek pacjentów zawierających dane medyczne. Niewłaściwe zabezpieczenie i przechowywanie papierowej dokumentacji, która aż w dziewięciu z 24 skontrolowanych szpitali była umieszczana w niezamykanych szafkach lub na półkach, wynikało z przyzwyczajeń personelu.

Takie zachowanie pracowników w dużej mierze było skutkiem braku szkoleń, gdyż jedynie w dziewięciu[19] szpitalach (37,5%) szkolenia związane z wejściem w życie przepisów RODO oraz bezpieczeństwem danych osobowych w systemach informatycznych objęły co najmniej 95% personelu. W efekcie, w podmiotach tych stwierdzono najmniej istotnych nieprawidłowości. W pozostałych siedmiu[20] wskaźnik ten wynosił od 51% do 94%, a w ośmiu kolejnych – mniej niż połowę. Zdaniem NIK, szkolenia z tego zakresu powinny być jednym z najistotniejszych elementów przygotowania podmiotu leczniczego do wejścia w życie RODO. Obowiązek ich przeprowadzania został określony w art. 39 ust. 1 lit. b RODO i spoczywał na IOD. Jako przyczynę braku szkoleń kierownicy szpitali wskazywali głównie specyfikę działalności, która znacząco utrudniała przeszkolenie całej kadry w jednym ustalonym terminie. Należy jednak przypomnieć, że 25-miesięczne *vacatio legis* dla RODO pozwalało na odpowiednie zaplanowanie i przeprowadzenie szkoleń dla większej grupy pracowników.

Dostęp do dokumentacji i danych osobowych

Kolejne ustalenia kontroli NIK dotyczące dokumentacji medycznej pacjentów były związane z udostępnianiem jej innym osobom, np. członkom rodziny. W dwóch skontrolowanych szpitalach[21] kopie dokumentacji zostały przekazane osobom, których pacjent nie upoważnił, nie były zatem uprawnione do takiego dostępu. Ponadto nie dochowano procedur związanych z udostępnianiem dokumentacji. W jednym ze szpitali dokumentację medyczną pełnoletniego pacjenta przekazano na podstawie listu otrzymanego przez szpital od osoby podającej się za matkę pacjenta, a w kolejnym dane przesłano pocztą elektroniczną na wniosek złożony w ten sam sposób. Takie postępowanie, oprócz naruszenia przepisów RODO, było również sprzeczne z obowiązującymi procedurami w tych podmiotach, bowiem określały one, że warunkiem wydania dokumentacji powinno być złożenie

[19] 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.

[20] 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.

[21] SP ZOZ w Augustowie, Białostockim Centrum Onkologii im. M. Skłodowskiej-Curie w Białymstoku.

odpowiedniego wniosku oraz okazanie dokumentu tożsamości w chwili odbioru.

Szpitale umożliwiały nieuprawniony dostęp do dokumentacji medycznej nie tylko osobom spoza danego podmiotu leczniczego, ale także pracownikom obsługi. Taka sytuacja miała miejsce w siedmiu[22] skontrolowanych szpitalach (29,2%), gdzie praktykowano udzielanie upoważnień do przetwarzania danych osobowych, w tym medycznych, pracownikom obsługi: salowym i sanitariuszom. Funkcje tych osób nie wiązały się jednak bezpośrednio z udzielaniem świadczeń opieki zdrowotnej i nie powinny one mieć dostępu do danych medycznych pacjentów. Jako główną przyczynę wskazywano przyjęty sposób organizacji pracy podmiotów leczniczych. Upoważnienia te wydawano osobom transportującym pacjentów na badania lub zabiegi, wraz ze skierowaniem lub wynikami badań. Najwyższa Izba Kontroli wskazywała, że możliwa jest jednak organizacja transportu chorego i odbioru wyników badań zapewniająca właściwą ochronę danych. Podobnie czynności związane ze sprzątaniem pomieszczeń, dbaniem o czystość i higienę pacjentów oraz transportem chorych nie stanowią przesłanki do przetwarzania, uzasadniającego dostęp do danych z historii choroby pacjentów szpitali. Należy jednocześnie zauważyć, że NIK nie kwestionowała dostępu do zwykłych danych osobowych pacjentów (jak imię i nazwisko) personelowi pomocniczemu i pracownikom obsługi, jeżeli jest to niezbędne do właściwej realizacji zadań.

Szpitale równie lekceważąco podchodziły do kwestii odbierania byłym pracownikom uprawnień w systemach informatycznych. Aż w 15[23] podmiotach leczniczych (62,5%) nie w pełni wywiązano się z obowiązku wynikającego z § 20 ust. 2 pkt 5 rozporządzenia KRI[24], zgodnie z którym zarządzanie bezpieczeństwem informacji realizowane jest przez bezzwłoczną zmianę uprawnień w wypadku zmiany zadań osób

[22] 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.

[23] 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.

[24] Rady Ministrów z 12.4.2012 *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).

zaangażowanych w proces przetwarzania informacji. Byli pracownicy mogli zatem, po uzyskaniu fizycznego dostępu do komputerów szpitalnych, mieć wgląd w dokumentację medyczną pacjentów, w takim zakresie, w jakim mieli w okresie zatrudnienia.

Szpitale nie przestrzegały podstawowych zasad zabezpieczenia dostępu do urządzeń komputerowych, jakim jest nadanie poszczególnym jego użytkownikom zindywidualizowanych loginów oraz haseł o odpowiedniej złożoności. Ustalenia kontroli wykazały, że w trzech[25] podmiotach (12,5%) część komputerów można było uruchomić bez uwierzytelniania hasłem, a w dwunastu[26]– login i hasło przyznawano grupie osób. Stanowiło to naruszenie przepisów § 20 ust. 7 lit. c rozporządzenia KRI, w myśl którego obowiązkiem kierownictwa jednostki jest zapewnienie ochrony przetwarzanych informacji przed ich kradzieżą, nieuprawnionym dostępem, uszkodzeniami lub zakłóceniami, przez zastosowanie środków uniemożliwiających nieautoryzowany dostęp na poziomie systemów operacyjnych, usług sieciowych i aplikacji. Wprowadzenie takich rozwiązań w części szpitali uniemożliwia odebranie dostępu do systemu operacyjnego komputera pojedynczemu pracownikowi oraz ustalenie osoby, która dokonywała określonych działań w systemie (rozliczalność danych, o której mowa w § 21 rozporządzenia KRI). Jak wskazywała Najwyższa Izba Kontroli, ustalenie takiej osoby może być szczególnie ważne w sytuacji nieuprawnionego usunięcia lub modyfikacji danych, bądź ich wycieku poza szpital. Stosowanie tych samych danych autoryzacyjnych dla grupy osób uniemożliwia więc przypisanie odpowiedzialności konkretnemu użytkownikowi.

Bardzo istotnym zagrożeniem dla bezpieczeństwa danych gromadzonych w systemach informatycznych było również niedopełnienie obowiązku zapewnienia, aby osoby zaangażowane w proces przetwarzania informacji posiadały stosowne uprawnienia i uczestniczyły w tym procesie w stopniu adekwatnym do realizowanych zadań. W dziesięciu[27] podmiotach leczniczych, aż 167 pracowników (z 720 objętych

[25] 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.

[26] 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 oraz Lubuski Szpital Specjalistyczny Pulmonologiczno-Kardiologiczny w Torzymiu Sp. z o. o. – po dziewięć, Samodzielny Publiczny Szpital dla Nerwowo i Psychicznie Chorych w Międzyrzeczu – jeden.

[27] 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.

analizą NIK[28]) posiadało uprawnienia administratora w systemach operacyjnych wykorzystywanych przez nich komputerów, chociaż nie mieli w swych zakresach obowiązków zadań związanych z administrowaniem systemami. Taka sytuacja pozwalała im na nieograniczoną możliwość instalacji dowolnego oprogramowania na użytkowanych komputerach, wyłączenia ochrony antywirusowej i ingerowania w inne ustawienia. Ponadto stwarzała ryzyko obniżenia skuteczności ochrony przetwarzanych danych i zainstalowania na komputerze, chociażby nieumyślnie, złośliwego oprogramowania, umożliwiającego penetrację systemu informatycznego.

Kolejnym niepokojącym zjawiskiem, związanym z zabezpieczeniem elektronicznej dokumentacji medycznej były przypadki przekazywania danych osobowych pacjentów firmom informatycznym serwisującym systemy szpitalne. Ustalenia kontroli wykazały, że taka sytuacja miała miejsce w 11[29] skontrolowanych szpitalach i dotyczyła danych osobowych 41 pacjentów, w tym danych medycznych 31 z nich. Należy zauważyć, że Najwyższa Izba Kontroli nie zgłaszała zastrzeżeń do samych zabezpieczeń systemów informatycznych, czy też potencjalnego dostępu serwisantów do danych wrażliwych pacjentów. Wskazywano natomiast na to, że zgłoszenia serwisowe zawierały informacje o pacjencie i jego historii leczenia, mimo że nie były konieczne do usunięcia usterek. Izba zauważyła, że w związku z tak przekazywanymi informacjami o awariach, istnieje znaczne zagrożenie wycieku danych, podając jako przykład przypadek z 2017 roku, kiedy nieuprawnione osoby weszły w posiadanie danych osobowych oraz medycznych 50 tysięcy pacjentów jednego ze szpitali w Kole. Przesyłano je bowiem w zgłoszeniach serwisowych do systemu helpdesk i gromadzono na serwerze zewnętrznym, skąd – w wyniku błędu podczas migracji danych na nowy serwer – zostały ujawnione i tym samym stały się dostępne dla wszystkich użytkowników Internetu.

Prawo pacjenta do prywatności

Błędy w zabezpieczeniu systemów wykorzystywanych do tworzenia i przetwarzania oraz niewłaściwa ochrona dokumentów papierowych zawierających informacje medyczne to nie jedyne elementy ochrony danych osobowych pacjentów, na potrzebę poprawy których zwróciła uwagę NIK. Istotną kwestią jest bowiem prawo do zachowania prywatności w newralgicznych momentach pobytu w szpitalu, tj.: podczas rejestracji do poradni, oczekiwania na wizytę, wzywania do gabinetu oraz w trakcie pobytu na oddziale. Ustalenia kontroli wykazały,

[28] 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.

[29] 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.

że w dziewięciu[30] z 24 skontrolowanych szpitali pacjentom nie zagwarantowano odpowiednich warunków do prywatności w trakcie rejestracji. Stwierdzono bowiem, że odległość pomiędzy okienkami rejestracji była zbyt mała lub nie wyznaczono strefy oddzielającej pacjentów obsługiwanych od oczekujących w kolejce. W tych sytuacjach osoby postronne mogły usłyszeć treści rozmów, dotyczących np. stanu zdrowia pacjenta, w tym szczegóły związane z dolegliwościami i procesem leczenia. W Białostockim Centrum Onkologii im. M. Skłodowskiej-Curie w Białymstoku zamieszczono jedynie informację o treści: „Przy okienku rejestracji może przebywać tylko jedna osoba". W konsekwencji pacjenci stali w bezpośredniej odległości za osobą, która się rejestrowała. Taki sposób rejestracji mógł nie zapewniać należytej ochrony danych osobowych, zwłaszcza nie odpowiadał dobrym praktykom podanym w „Przewodniku po RODO dla Służby Zdrowia".

Podobne ustalenia dotyczyły ochrony danych pacjentów przebywających na oddziałach szpitalnych. Wprawdzie we wszystkich skontrolowanych placówkach wywiązano się z obowiązku (określonego w art. 36 ust. 3 ustawy z 15 kwietnia 2011 r. o działalności leczniczej[31]) zaopatrzenia pacjentów w znaki identyfikacyjne, tzw. opaski na nadgarstki, niemniej aż w 11[32] nie zrobiono tego właściwie. Na opaskach zamieszczono bowiem, poza numerem księgi głównej bądź kodem kreskowym, także imię i nazwisko pacjenta, a w niektórych przypadkach nr PESEL[33]. Takie rozwiązania stanowiły naruszenie art. 36 ust. 5 ustawy o działalności leczniczej, w myśl którego opaska powinna zawierać informacje zapisane w sposób uniemożliwiający identyfikację pacjenta przez osoby nieuprawnione. Podobnie w trzech[34] szpitalach umieszczono dane osobowe pacjentów na łóżkach, tak, że były widoczne np. dla odwiedzających innego chorego. Co ciekawe, w tych samych podmiotach

[30] 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.

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

[32] 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.

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

[34] 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 w trzech oddziałach objętych oględzinami.

leczniczych, na innych oddziałach, funkcjonowały rozwiązania chroniące dane osobowe pacjentów. Stosowano tam karty przyłóżkowe, ale z ramkami zasłaniającymi personalia pacjentów.

Znacznie lepiej przedstawiała się sytuacja gdy wzywano pacjentów do gabinetów lekarskich. W prawie wszystkich szpitalach posługiwano się przy tym komunikatem: „proszę kolejną osobę" lub podawano imię pacjenta i godzinę wizyty, ewentualnie numer, który pacjent otrzymał podczas rejestracji. Tylko w jednym szpitalu (SP ZOZ w Radzyniu Podlaskim), w jednej z trzech skontrolowanych poradni była wywieszona lista pacjentów, na której zamieszczono godzinę planowanej wizyty oraz pierwsze trzy litery imienia i pierwsze cztery litery nazwiska. Najwyższa Izba Kontroli zwróciła uwagę, że w wypadku pacjentów o krótkich imionach i nazwiskach stosowanie takiego rozwiązania może doprowadzić do ujawnienia ich danych osobowych.

Podsumowanie

Wyniki kontroli przeprowadzonych w 24 szpitalach wskazały jednoznacznie, że dane osobowe i medyczne pacjentów w 21 podmiotach leczniczych nie były odpowiednio chronione. W konsekwencji, kierownicy tych podmiotów i IOD nie zapewnili pacjentom pełnego zabezpieczenia ich danych. Personel medyczny i administracyjny postępował rutynowo, według schematów wypracowanych przed wejściem w życie uregulowań RODO i znowelizowanej ustawy o ochronie danych osobowych.

Ponad połowa skontrolowanych podmiotów leczniczych (67%) nie była właściwie przygotowana do stosowania RODO. Dokumenty i procedury związane z wejściem w życie tych przepisów zostały bowiem wdrożone z opóźnieniem lub do zakończenia kontroli NIK ich nie wprowadzono.

Jedną z głównych przyczyn wymienionych nieprawidłowości była nieznajomość zagadnień bezpieczeństwa danych osobowych. Jak wykazała kontrola, tylko w dziewięciu szpitalach szkoleniami w tym zakresie objęto prawie cały personel. W rezultacie w podmiotach tych stwierdzono najmniej istotnych nieprawidłowości dotyczących ochrony danych osobowych pacjentów.

Tylko w trzech szpitalach przyjęte rozwiązania organizacyjne i techniczne stworzyły odpowiednie warunki do rejestracji wizyt 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 także ustalonej w RODO zasady ograniczania dostępu do danych osobowych w zakresie niezbędnym do osiągnięcia celu ich przetwarzania. W rezultacie byłym pracownikom personelu medycznego (62,5%) podmiotów leczniczych nie odebrano niezwłocznie dostępu do systemów informatycznych. Z kolei w 11 szpitalach w nieuprawniony sposób przekazywano dane osobowe pacjentów podmiotom serwisującym te systemy.

Istotną i dość powszechnie występującą nieprawidłowością było nieprzestrzeganie wymogów dotyczących nadawania właściwych uprawnień do administrowania systemami informatycznymi oraz odpowiedniej autoryzacji.

Poprawie przyjętych sposobów ochrony danych osobowych oraz właściwemu

wdrożeniu regulacji RODO może sprzyjać szybkie przyjęcie przez PUODO „Kodeksu postępowania dla sektora ochrony zdrowia", którego celem, jak wskazano we wstępie, 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. Najwyższa Izba Kontroli nie odnosiła się do treści i nie oceniała proponowanych rozwiązań w „Kodeksie postępowania dla sektora ochrony zdrowia", ponieważ nie badała jego przepisów, wskazała jedynie na potrzebę zawarcia w nim 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, mogą bowiem odgrywać ważną rolę w procesie „uwiarygodnienia" przedsiębiorstw i instytucji pod względem zgodności przetwarzania danych z przepisami prawa.

Wnioski pokontrolne

W związku z ustaleniami kontroli oraz mając na celu właściwą ochronę i przetwarzanie danych osobowych w podmiotach leczniczych, Najwyższa Izba Kontroli skierowała wymienione niżej wnioski pokontrolne.

1. Do Prezesa Urzędu Ochrony Danych Osobowych o:
- przeprowadzanie systemowych kontroli przestrzegania zasad ochrony danych osobowych w jednostkach z sektora ochrony zdrowia;
- niezwłoczne zakończenie działań związanych z przyjęciem „Kodeksu postępowania dla sektora ochrony zdrowia" oraz wprowadzenie regulacji dotyczących certyfikacji, o której mowa w art. 42 RODO.

2. Do organów założycielskich szpitali o objęcie nadzorem w podległych podmiotach leczniczych zagadnień związanych z ochroną danych osobowych pacjentów.

3. Do kierowników podmiotów leczniczych o:
- analizowanie ryzyka dotyczącego ochrony danych osobowych, uwzględniającego aktualny stan wiedzy technicznej, a następnie stosowanie rozwiązań adekwatnych do ustalonych zagrożeń;
- przeprowadzanie regularnych szkoleń osób uczestniczących w procesach przetwarzania informacji, ze szczególnym uwzględnieniem zagrożeń jej bezpieczeństwa, skutków naruszeń takich zasad, odpowiedzialności prawnej oraz stosowania środków zapewniających bezpieczeństwo informacji;
- nadawanie pracownikom uprawnień w systemach operacyjnych komputerów oraz systemach HIS[35] w stopniu koniecznym do realizacji przez nich zadań;
- wprowadzenie zindywidualizowanej autoryzacji dostępu do posiadanych zasobów informatycznych;

[35] HIS (*Hospital Information System*) – system informatyczny służący tworzeniu, archiwizacji, przetwarzaniu i udostępnianiu danych związanych z realizacją procesu diagnostyczno-terapeutycznego.

• przechowywanie kopii bezpieczeństwa zasobów informacyjnych w innym miejscu niż dane produkcyjne;
• zapewnienie fizycznych zabezpieczeń infrastruktury informatycznej, uniemożliwiających dostęp osób nieuprawnionych oraz zapewniających ochronę przed skutkami zdarzeń losowych (np. pożar, powódź, wichura);
• zapewnienie osobom uzyskującym dostęp do danych osobowych posiadanie stosownych upoważnień ADO;
• przekazywanie firmom świadczącym usługi serwisowe jedynie danych osobowych niezbędnych do usunięcia usterek oprogramowania.

W związku z wynikami badań przedstawionymi w Informacji o wynikach kontroli, zatwierdzonej przez Prezesa NIK 19 sierpnia 2019 r., PUODO poinformował m.in., że podziela stanowisko Najwyższej Izby Kontroli w odniesieniu do wskazanych przez nią działań. Jednocześnie podkreślił także potrzebę kontroli podmiotów leczniczych, które, jak wskazał, zostały ujęte w planie kontroli sektorowych na 2019 rok. W odniesieniu do prac nad „Kodeksem postępowania dla sektora ochrony zdrowia" poinformował o intensywnych konsultacjach zmierzających do stworzenia spójnych przepisów w kwestii stosowania RODO w kilku obszarach. Jak zadeklarował PUODO, opinia w sprawie Kodeksu i jego zatwierdzenie nastąpi, gdy uzna, że regulacje w nim zawarte będą gwarantowały odpowiednie zabezpieczenie danych osobowych. Oznacza to, że w dalszym ciągu nie jest znana data zatwierdzenia Kodeksu, co z pewnością nie przyczyni się do upowszechnienia wśród placówek ochrony zdrowia jednolitego i zgodnego z regulacjami RODO podejścia do kwestii związanych z ochroną danych osobowych pacjentów.

PAWEŁ TOŁWIŃSKI
Delegatura NIK w Białymstoku

Słowa kluczowe: RODO, wdrażanie regulacji, podmioty lecznicze, ochrona danych osobowych pacjentów, placówki medyczne

ABSTRACT

PAWEŁ TOŁWIŃSKI: Protection of Patients' Personal Data – Implementation of GDPR by Medical Entities

In Poland, the provisions of GDPR came into force on 25 May 2018. At the same time, the related regulations were introduced, set out in the amended act on personal data protection. All medical entities, public and private alike, are obliged to comply with these regulations. The audit was conducted at twenty-four hospitals in six Polish administrative regions. In his article, the author discusses the detailed results of the audit.

Key words: GDPR, implementation of regulations, medical entities, protection of patients' personal data, medical facilities