# Naruszenia ochrony danych osobowych w placówkach medycznych

Mimo że przepisy o ochronie danych osobowych obowiązują od kilku lat, nadal regulacje te nastręczają wiele problemów interpretacyjnych i trudności w ich stosowaniu. Do ich przestrzegania zobowiązane są wszystkie placówki medyczne – zarówno szpitale, przychodnie, jak i nieduże gabinety lekarskie. Nie ma również znaczenia, czy dana placówka medyczna udziela świadczenia zdrowotnego w ramach Narodowego Funduszu Zdrowia, czy realizuje świadczenia medyczne wyłącznie komercyjnie.

Anna Madajczyk-Pietrzak, Dział Prawny Okręgowej Izby Lekarskiej w Łodzi

Można powiedzieć, że na placówce medycznej ciąży większy obowiązek przestrzegania przepisów dotyczących przetwarzania i ochrony danych osobowych niż na zwykłym przedsiębiorcy. Dzieje się tak dlatego, że podmioty te operują setkami, a nawet tysiącami danych osobowych różnych pacjentów, podczas gdy dany przedsiębiorca ma zawężoną działalność skierowaną do danej grupy odbiorców, a tym samym przetwarza mniejszą liczbą danych. Dodatkowo na szczególną uwagę zasługuje rodzaj informacji. Podczas gdy większość przedsiębiorców operuje zwykłymi danymi, podmiot medyczny przetwarza dane wrażliwe, dotyczące stanu zdrowia pacjentów. Jak wynika z art. 9 ust. 1 Rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/679 z 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 (RODO), dane dotyczące zdrowia stanowią szczególną kategorię danych osobowych, a ich przetwarzanie jest zabronione. Przepis ten nie ma zastosowania, jeśli spełniony jest jeden z warunków wskazanych w art. 9 ust. 2.

Przestrzeganie powyższych uregulowań jest istotne z punktu widzenia ochrony praw i ochrony prywatności pacjentów placówek medycznych. W związku z tym zabezpieczenie danych w podmiocie leczniczym będzie różniło się od zabezpieczenia danych w przedsiębiorstwie, które swoim zakresem działalności nie udziela świadczeń medycznych. Oczywiście rozważania te nie mają na celu wskazywania które dane są „ważniejsze” i powinny być np. lepiej chronione. Mają one jedynie na celu uświadomienie osobom kierującym placówkami medycznymi, z jak ważną tematyką mają do czynienia i jakie konsekwencje mogą grozić w przypadku wdrażania nieprawidłowego lub wadliwego sposobu ochrony danych osobowych oraz naruszeń ochrony tych danych.

Konstytucja Rzeczypospolitej Polskiej jako akt państwowy najwyższej rangi w art. 51 pkt. 1 traktuje o prawie do ochrony danych osobowych stanowiąc, że *nikt nie może być obowiązany inaczej niż na podstawie ustawy do ujawniania informacji dotyczących jego osoby.* Natomiast w preambule RODO motywie 7 wskazano, że *osoby fizyczne powinny mieć kontrolę nad własnymi danymi osobowymi.*

**Kiedy mamy do czynienia z naruszeniem ochrony danych osobowych?**

Pojęcie „naruszenia ochrony danych osobowych" zostało zdefiniowane w Rozporządzeniu Parlamentu Europejskiego i Rady (UE) 2016/679 z 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, a więc w przywołanym przeze mnie powyżej tzw. RODO. Zgodnie z art. 4 ust. 12 za takie naruszenie uważa się *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.*

Najczęstszą przyczyną naruszeń jest brak wiedzy wynikający z braku szkoleń personelu w tym zakresie oraz brak przyjęcia odpowiednich procedur opartych na obowiązujących przepisach prawa.

W monografii pod red. M. Jędrzejczak wskazano, że *kluczową rolę we właściwym stosowaniu przepisów odnoszących się do ochrony danych osobowych w podmiotach leczniczych [...] odgrywa personel tych podmiotów*. *Zmiany dotychczasowych, często rutynowych zachowań personelu zarówno medycznego, jak i administracyjnego mogą być implikowane przeprowadzaniem regularnych i ciągłych szkoleń – wymaganych w szczególności przez przepisy RODO.*[1]

Poniżej zestawienie naruszeń ochrony danych osobowych w sektorze medycznym wraz z tabelami statystycznymi przygotowane przez Inspektora Ochrony Danych Osobowych panią Bożenę Chmielewską. Opracowano na podstawie własnych obserwacji IOD oraz Sprawozdań Prezesa UODO za lata 2018–2022 https://archiwum.uodo.gov.pl/pl/437

**Liczba zgłoszonych naruszeń do Urzędu Ochrony Danych Osobowych w latach 2018–2021**

| rok | sektor prywatny | sektor publiczny | międzynarodowy sektor informatyczny (IMI) | razem |
|---|---|---|---|---|
| 2021 | 8172 | 4738 | 36 | 12946 |
| 2020 | 4661 | 2691 | 155 | 7507 |

| | | | | |
|---|---|---|---|---|
| 2019 | 3894 | 2145 | 69 | 6108 |
| 2018 (od maja) | 1882 | 564 | 0 | 2446 |

[1] Jędrzejczak M. (red.), *Ochrona danych osobowych w prawie publicznym*, Wydawnictwo Wolters Kluwer Polska, b.m.w. 2021.

Najczęstsze naruszenia ochrony danych osobowych w sektorze medycznym:

- wysłanie korespondencji zawierającej dane osobowe zarówno w formie tradycyjnej, jak i na elektroniczną skrzynkę pocztową e-mail do niewłaściwego odbiorcy,
- wysyłanie korespondencji elektronicznej z niezaszyfrowanymi załącznikami, zawierającymi wyniki badań pacjentów lub kopie dokumentacji medycznej,
- ujawnienie danych niewłaściwej osobie – udostępnianie danych osobowych pacjentów (lub wydania dokumentacji medycznej) bez sprawdzenia, czy osoba odbierająca jest upoważniona do odbioru dokumentacji,
- wystawienie i wydanie recepty innemu pacjentowi – brak weryfikacji pacjenta,
- zamiana dokumentacji przez pacjentów w gabinetach fizjoterapeutycznych,
- podczepienie pojedynczych wyników do dokumentacji innego pacjenta i wydanie niewłaściwemu pacjentowi,
- pomyłki/błędy w karcie pacjenta – np. dokonywanie wpisów w karcie dotyczących innego pacjenta, wpisanie przez lekarza błędnego nr PESEL na skierowaniu na badania,
- brak weryfikacji tożsamości pacjenta – udzielenie świadczenia niewłaściwej osobie,
- telefoniczne udzielanie informacji o pacjencie bez weryfikacji tożsamości osób dzwoniących i bez sprawdzenia, czy są uprawnione do uzyskania informacji o pacjencie,
- dokumentacja papierowa zgubiona lub skradziona – przewożenie dokumentacji na wizyty domowe i pozostawienie w sklepie, w urzędzie „po drodze”,
- dokumentacja papierowa lub w formie elektronicznej na nośnikach – pozostawiona w niezabezpieczonej lokalizacji – pozostawianie otwartych gabinetów, pozostawianie kluczy w drzwiach gabinetu, dokumentacja papierowa włożona w drzwi i zostawiona bez nadzoru, dokumentacja medyczna przechowywania w otwartych szafach lub na półkach bez możliwości zamknięcia na klucz,
- zgubienie lub kradzież nośnika danych/urządzenia umożliwiającego dostęp do danych (laptop) – niezaszyfrowany sprzęt, pozostawiony bez opieki w samochodzie,
- zniszczenie dokumentacji medycznej poprzez zalanie kawą,
- przetwarzanie danych osobowych pacjentów przez nieupoważniony do tego celu personel placówki leczniczej – brak upoważnień nadanych przez administratora,
- udostępnianie przez personel swoich loginów i haseł do systemów informatycznych współpracownikom,
- obsługa systemów informatycznych na cudzym loginie – nieuprawniony dostęp do danych pacjentów oraz nieuprawnione dokonywanie zapisów w dokumentacji

medycznej,
- nieuprawnione uzyskiwanie danych w zakresie wizerunku – utrwalenie na nagraniu z monitoringu przebiegu leczenia stomatologicznego bez uprzedniego powiadomienia pacjenta i bez jego zgody,
- brak klauzul informacyjnych dotyczących stosowania monitoringu wizyjnego w placówce,
- ataki hakerskie – złośliwe oprogramowanie ingerujące w poufność, integralność lub dostępność danych oraz nieuprawnione uzyskanie dostępu do informacji poprzez złamanie zabezpieczeń, wymuszanie okupu (*ransomware*),
- pozostawianie uprawnień dostępu do systemów informatycznych pracownikom, którzy zakończyli pracę w placówce medycznej,
- głośne rozmowy i uwagi personelu na temat pacjentów, plotkowanie o pacjentach i współpracownikach poza miejscem pracy, umożliwiające zidentyfikowanie osób, o których się rozmawia,
- udzielanie informacji o pacjentach przez osoby nieuprawnione – np. przez personel sprzątający,
- przechowywanie dokumentacji medycznej przez czas niezgodny z określonym w ustawie o prawach pacjenta i Rzeczniku Praw Pacjenta.

Powyższe naruszenia opracowane przez Inspektora Ochrony Danych Osobowych nie stanowią katalogu zamkniętego. Wynikają one z obserwacji Inspektorki, popartej jej wieloletnią praktyką zawodową w dziedzinie ochrony danych osobowych. Wiadomo, że jak wiele ludzi, tak wiele przypadków. Co zatem zrobić, aby ryzyko wystąpienia naruszeń zminimalizować do zera? Największy nacisk położyć należy na szkolenia. Tylko dobrze przeszkolony personel jest w stanie czuwać nad prawidłową ochroną danych osobowych w placówce medycznej. Pracownicy powinni być przeszkalani z zakresu regulacji prawnych dotyczących RODO oraz powinni być uświadamiani co do typowych zaniedbań czy istniejących zagrożeń związanych z ochroną danych osobowych pacjentów. Każdy z pracowników powinien znać dobrze system, na którym pracuje oraz znać zasady bezpieczeństwa informacji. Wiedzieć, jak postępować w sytuacji, kiedy doszłoby do naruszenia danych osobowych.

Przeszkolenie każdego nowego pracownika oraz prowadzenie szkoleń przynajmniej raz do roku dla wieloletnich pracowników, powinno być gwarantem prawidłowego wdrażania i stosowania przepisów RODO.

Do powyższej tematyki odniosła się również Najwyższa Izba Kontroli, wskazując na to, jak ważną rolę odgrywają szkolenia minimalizując nieprawidłowości w ochronie danych osobowych. NIK w okresie od 25 maja 2018 r. do 23 kwietnia 2019 r. przeprowadziła w 24 podmiotach leczniczych z terenu sześciu województw kontrolę, której głównym celem była

odpowiedź na pytanie, czy dane osobowe w podmiotach leczniczych są prawidłowo chronione i przetwarzane? Prawie w żadnej z kontrolowanych placówek dane osobowe pacjentów nie były ani prawidłowo chronione, ani prawidłowo przetwarzane. Z kolei *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 najistotniejszych 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. […] Zapewnienie prawidłowego przetwarzania i ochrony danych osobowych wymaga zmiany rutynowych zachowań personelu medycznego i administracyjnego*[1].

Kolejną bardzo istotną kwestią jest to, aby po zakończonej współpracy z danym pracownikiem odbierać mu stosowne upoważnienia, którymi posługiwał się przy wykonywaniu swojej pracy na rzecz danego podmiotu. Pracownik, który zakończył współpracę, nie powinien mieć już dostępu do haseł, dokumentów i sprzętu, którymi się posługiwał, m.in. właśnie dlatego, aby nie wystąpiło ryzyko przepływu danych wrażliwych do osób trzecich i co za tym idzie – bezprawnego ich użycia. Zasadne jest, aby minimum raz do roku przeprowadzać kontrolę umów kadry pracowniczej, by uaktualnić informacje o osobach zatrudnionych w danej placówce medycznej, jak i tych, które zakończyły już współpracę. Równie istotną kwestię stanowi niedopuszczanie do danych wrażliwych osób, które nie posiadają stosownych upoważnień i nie zostały przeszkolone w tym zakresie, jak np. praktykanci, stażyści. Można to czynić dopiero po pełnym przeszkoleniu i nadaniu takiej osobie niezbędnych uprawnień.

[1] Raport Najwyższej Izby Kontroli, *Wdrożenie przez podmioty lecznicze regulacji dotyczących ochrony danych osobowych.*

[1] Jędrzejczak M. (red.), *Ochrona danych osobowych w prawie publicznym*, Wydawnictwo Wolters Kluwer Polska, b.m.w. 2021.

Na szczególną uwagę w kwestii ochrony danych osobowych zasługują dwa dokumenty. Pierwszym z nich jest „Przewodnik RODO w służbie zdrowia”. Każda z placówek medycznych znajdzie w nim wskazówki związane z ochroną danych osobowych przy czynnościach rejestracji pacjentów, sposoby wywoływania pacjenta w podmiocie leczniczym, zagadnienia dotyczące możliwości zamieszczania tabliczek o stanie zdrowia na tzw. kartach przyłóżkowych itd.[1]. Przewodnik powstał we współpracy z Rzecznikiem Praw Pacjenta i jest oficjalnym dokumentem sygnowanym przez Ministerstwo Zdrowia.

Z kolei drugim bardzo ważnym dokumentem jest kodeks postępowania dotyczącego ochrony danych osobowych przetwarzanych w małych placówkach medycznych. Jest to „świeża” regulacja prawna, kodeks bowiem został zatwierdzony przez Prezesa Urzędu Ochrony Danych Osobowych 14 grudnia 2022 r. Akt ten został opracowany przez zespół specjalistów Jamano Sp. z o.o. we współpracy z Federacją Porozumienie Zielonogórskie[2]. Jednym z głównych celów kodeksu jest pomoc podmiotom medycznym w prawidłowym stosowaniu przepisów RODO, poszerzanie świadomości co do ochrony danych osobowych, jak również zapewnienie należytej ochrony tych danych pacjentom  placówek medycznych.

**Co zrobić w sytuacji naruszenia?**

Jak wynika z art. 33 ust. 1 RODO, każda placówka medyczna w przypadku naruszenia danych osobowych, ma obowiązek zawiadomić o tym właściwy organ nadzorczy bez zbędnej zwłoki, w miarę możliwości nie później, niż w ciągu 72 godzin od stwierdzenia naruszenia. Wyjątkiem od obowiązku zgłoszenia jest sytuacja, kiedy występuje małe prawdopodobieństwo, aby naruszenie to skutkowało ryzykiem naruszenia praw lub wolności osób fizycznych. Do zgłoszenia przekazanego organowi nadzorczemu po upływie 72 godzin dołącza się wyjaśnienie przyczyn opóźnienia.

Abyśmy mogli mówić o prawidłowości zgłoszenia naruszenia, powinno ono:

[1] https://www.gov.pl/web/rpp/przewodnik-po-rodo-w-sluzbie-zdrowia

[2] https://jamano.pl/kodeksfpz/

a) opisywać charakter naruszenia ochrony danych osobowych, w tym w miarę możliwości wskazywać kategorię i przybliżoną liczbę osób, których dane dotyczą oraz kategorię i przybliżoną liczbę wpisów danych osobowych, których dotyczy naruszenie,

b) zawierać imię i nazwisko oraz dane kontaktowe inspektora ochrony danych lub oznaczenie innego punktu kontaktowego, od którego można uzyskać więcej informacji;

c) opisywać możliwe konsekwencje naruszenia ochrony danych osobowych,

d) opisywać środki zastosowane lub proponowane przez administratora w celu zaradzenia naruszeniu ochrony danych osobowych, w tym w stosownych przypadkach środki w celu zminimalizowania jego ewentualnych negatywnych skutków.

Powyższy przepis wskazuje obowiązek zawiadomienia właściwego organu nadzorczego. Nie jest to jedyny podmiot, który w przypadku naruszenia ochrony danych osobowych powinien zostać o tym fakcie poinformowany. Jak wynika bowiem z art. 34 ust. 1

przedmiotowego rozporządzenia, w sytuacji, gdy naruszenie ochrony danych osobowych może powodować wysokie ryzyko naruszenia praw lub wolności osób fizycznych, administrator jest zobowiązany bez zbędnej zwłoki zawiadomić osobę, której dane dotyczą, o takim naruszeniu. Zgodnie z ust. 2 tegoż artykułu, prawidłowe zawiadomienie powinno jasnym i prostym językiem opisywać charakter naruszenia ochrony danych osobowych oraz zawierać przynajmniej informacje i środki, o których mowa w art. 33 ust. 3 lit. b), c) i d), a więc:

a) imię i nazwisko oraz dane kontaktowe inspektora ochrony danych lub oznaczenie innego punktu kontaktowego, od którego można uzyskać więcej informacji,

b) opis możliwych konsekwencji naruszenia ochrony danych osobowych,

c) opis środków zastosowanych lub proponowanych przez administratora w celu zaradzenia naruszeniu ochrony danych osobowych, w tym stosownych przypadkach środków w celu zminimalizowania jego ewentualnych negatywnych skutków.

*Zgłaszanie naruszeń ochrony danych osobowych przez administratorów stanowi skuteczne narzędzie przyczyniające się do realnej poprawy bezpieczeństwa przetwarzania danych osobowych oraz pozwala organowi nadzorczemu na właściwą reakcję mogącą ograniczyć skutki takich naruszeń*[1].

Niezwykle istotne jest, aby w przypadku naruszenia danych osobowych placówka medyczna niezwłocznie dopełniła powyższych obowiązków, nie tylko z uwagi na konsekwencje związane z naruszeniem praw pacjenta, ale również z uwagi na konsekwencje finansowe. W tym miejscu chciałabym wskazać na decyzję Prezesa Urzędu Ochrony Danych Osobowych z 6 lipca 2022 r., DKN.5131.34.2021, mocą której na Uniwersyteckie Centrum Kliniczne Warszawskiego Uniwersytetu Medycznego w Warszawie została nałożona administracyjna kara pieniężna w wysokości 10 tys. zł. Podstawą do jej nałożenia było naruszenie przez wskazaną placówkę przepisów art. 33 ust.1 i art. 34 ust. 1 ww. rozporządzenia. Naruszenie to polegało na niezgłoszeniu prezesowi UODO naruszenia ochrony danych osobowych bez zbędnej zwłoki, nie później niż w terminie 72 godzin po stwierdzeniu naruszenia oraz na niezawiadomieniu o naruszeniu ochrony danych osobowych, bez zbędnej zwłoki osoby, której dane dotyczą.

W związku z powyższym każda placówka medyczna powinna mieć na uwadze, że *w sytuacji, gdy na skutek naruszenia ochrony danych osobowych, występuje wysokie ryzyko naruszenia praw lub wolności osób fizycznych, administrator zobowiązany jest wdrożyć wszelkie odpowiednie środki techniczne i organizacyjne, by od razu stwierdzić naruszenie ochrony danych osobowych i szybko poinformować organ nadzorczy, jak również osoby, których dane dotyczą. Administrator powinien zrealizować przedmiotowy obowiązek*

*możliwie najszybciej*[2].

Podsumowując, uznać należy, że kluczową rolę w celu zminimalizowania ryzyka naruszenia danych osobowych, odgrywają 3 elementy:

- dbanie o prawidłowe przeszkalanie personelu,
- wprowadzanie odpowiednich zabezpieczeń,
- kontrolowanie nadawanych uprawnień.

Zasadne jest przytoczenie w tym miejscu łacińskiej paremii „Ignorantia iuris nocet", nieznajomość bowiem przepisów o ochronie danych osobowych oraz ich nieumiejętne stosowanie może pociągać za sobą poważne konsekwencje zarówno dla pacjentów, jak i dla podmiotów medycznych.

[1] Decyzja Prezesa Urzędu Ochrony Danych Osobowych z dnia 6 lipca 2022 r., DKN.5131.34.2021.

[2] Ibidem.

Panaceum 3/2023