LEX SECURE®
24H OPIEKA PRAWNA

RZECZPOSPOLITA
RANKING KANCELARII PRAWNICZYCH
XXIII
I MIEJSCE

Sopot, dnia 14 sierpnia 2026 r.

Sygn.: 082400

OPINIA PRAWNA

Przedmiot opinii:

1. Jakie kroki prawne powinien podjąć administrator danych osobowych pacjentów w związku z ryzykiem naruszenia ochrony ich danych osobowych przez dostawcę oprogramowania do prowadzenia dokumentacji medycznej?

Wnioski i rekomendacje:

Administratorem danych osobowych pacjentów jest placówka medyczna, do której zgłasza się pacjent – podmiot leczniczy albo praktyka zawodowa osoby wykonującej zawód medyczny. Dostawca oprogramowania do prowadzenia dokumentacji medycznej lub umawiania wizyt jest natomiast podmiotem przetwarzającym.

Uzyskanie dostępu do danych osobowych pacjentów zawartych w dokumentacji medycznej przez osoby nieuprawnione **stanowi naruszenie ochrony danych osobowych**. W przypadku stwierdzenia takiego naruszenia, dostawca oprogramowania ma obowiązek zawiadomić administratora danych o naruszeniu bez zbędnej zwłoki.

Uzyskanie dostępu do danych osobowych pacjentów zgromadzonych w dokumentacji medycznej (imion, nazwisk, numerów PESEL, danych teleadresowych oraz danych dotyczących zdrowia) nie jest sytuacją, w której ryzyko naruszenia praw lub wolności osób fizycznych jest mało prawdopodobne. W związku z tym, **podmiot wykonujący działalność leczniczą** (podmiot leczniczy lub osoba wykonująca zawód medyczny w ramach praktyki zawodowej) **ma obowiązek zgłoszenia do Prezesa Urzędu Ochrony Danych Osobowych incydentu naruszenia ochrony danych osobowych swoich pacjentów**, w ciągu 72 godzin od stwierdzenia naruszenia. Obowiązek ten powstaje niezależnie od tego, czy dane osobowe pacjentów zostały w jakikolwiek sposób upublicznione lub wykorzystane. Liczy się bowiem sam fakt uzyskania dostępu do tych danych przez osoby nieuprawnione.

Momentem stwierdzenia naruszenia może być w niniejszej sprawie otrzymanie od dostawcy oprogramowania informacji o tym, że dane osobowe pacjentów placówki znajdują się wśród danych, do których dostęp uzyskały nieuprawnione osoby. **Rekomendowanym jest uzyskanie w pierwszej kolejności indywidualnej informacji od dostawcy oprogramowania** dotyczącej danych osobowych pacjentów danej placówki i w przypadku, gdy dostawca oprogramowania potwierdzi, że

dane pacjentów danej placówki znajdują się wśród ujawnionych danych, aktualizuje się obowiązek dokonania zawiadomienia do Prezesa UODO.

W ocenie opiniującego, w niniejszej sprawie ujawnienie danych osobowych pacjentów **może powodować wysokie ryzyko naruszenia praw lub wolności osób fizycznych**. Pacjenci korzystający z usług podmiotu wykonującego działalność leczniczą mają bowiem prawo do poszanowania ich prywatności, a dane zawarte w dokumentacji medycznej podlegają szczególnej ochronie. W sytuacji, w której nieuprawnione osoby uzyskały dostęp do danych osobowych pacjentów np. w postaci imienia i nazwiska, numeru PESEL oraz danych dotyczących zdrowia, rodzi to **wysokie ryzyko** wyrządzenia pacjentom szkody majątkowej, krzywdy lub tzw. kradzieży tożsamości. W związku z tym, w przypadku otrzymania od dostawcy oprogramowania informacji o tym, że dane pacjentów placówki są objęte naruszeniem, **administratorzy mają obowiązek dokonania zawiadomienia swoich pacjentów o naruszeniu ochrony ich danych osobowych.**

Należy przy tym wskazać, że nie jest wymagane, aby ww. zawiadomienie zostało dokonane w formie pisemnej - istotne jest, aby administrator mógł później wykazać, że dokonał zawiadomienia. Rekomendowanym jest, aby zawiadomienie zostało dokonane w formie umożliwiającej szybkie zapoznanie się z jego treścią, zatem **możliwe jest wystosowanie w tej sprawie wiadomości SMS albo e-mail do pacjentów (z funkcją ukrycia odbiorców)**. Jeżeli wiązałoby się to dla administratora z nadmiernym wysiłkiem (np. z uwagi na liczbę osób objętych naruszeniem i brak środków technicznych do dokonania indywidualnego zawiadomienia), konieczne byłoby wówczas zawiadomienie pacjentów w inny sposób, np. poprzez **komunikat na stronie internetowej podmiotu wykonującego działalność leczniczą.**

Podstawy prawne:

1. Art. 4 pkt 7, 8 i 12, art. 32 ust. 1, art. 33 ust. 1, 3 i 5, art. 34 ust. 1-4, art. 77 ust. 1, art. 78 ust. 1, art. 79 ust. 1, art. 82 ust. 1-3 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) (t.j. Dz.Urz.UE.L.2016.119.1 ze zm.);
2. P. Litwiński (red.), Ustawa o ochronie danych osobowych. Komentarz [w:] Ogólne rozporządzenie o ochronie danych osobowych. Ustawa o ochronie danych osobowych. Wybrane przepisy sektorowe. Komentarz, wyd. 2, 2025.

Stan prawny:

W celu udzielenia odpowiedzi na zadane pytanie prawne, należy odnieść się do treści przepisów 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) (dalej jako RODO).

Według art. 4 pkt 7 RODO, ,,administrator'' oznacza osobę fizyczną lub prawną, organ publiczny, jednostkę lub inny podmiot, który samodzielnie lub wspólnie z innymi ustala cele i sposoby przetwarzania danych osobowych; jeżeli cele i sposoby takiego przetwarzania są określone w prawie Unii lub w prawie państwa członkowskiego, to również w prawie Unii lub w prawie państwa członkowskiego może zostać wyznaczony administrator lub mogą zostać określone konkretne kryteria jego wyznaczania. Jak zaś stanowi art. 4 pkt 8 RODO, ,,podmiot przetwarzający'' oznacza osobę fizyczną lub prawną, organ publiczny, jednostkę lub inny podmiot, który przetwarza dane osobowe w imieniu administratora.

Administratorem danych osobowych pacjentów jest placówka medyczna, do której zgłasza się pacjent – podmiot leczniczy albo praktyka zawodowa osoby wykonującej zawód medyczny. Dostawca oprogramowania do prowadzenia dokumentacji medycznej lub umawiania wizyt jest natomiast podmiotem przetwarzającym.

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.**

Jak zaś stanowi art. 33 ust. 2 RODO, **podmiot przetwarzający po stwierdzeniu naruszenia ochrony danych osobowych bez zbędnej zwłoki zgłasza je administratorowi**.

Uzyskanie dostępu do danych osobowych pacjentów zawartych w dokumentacji medycznej przez osoby nieuprawnione **stanowi naruszenie ochrony danych osobowych**. W przypadku stwierdzenia takiego naruszenia, dostawca oprogramowania ma obowiązek zawiadomić administratora danych o naruszeniu bez zbędnej zwłoki.

Kolejno, w myśl art. 33 ust. 1 RODO **w przypadku naruszenia ochrony danych osobowych, administrator bez zbędnej zwłoki -** w miarę możliwości, nie później niż w terminie 72 godzin po stwierdzeniu naruszenia - **zgłasza je organowi nadzorczemu** właściwemu zgodnie z art. 55, chyba że jest mało prawdopodobne, by naruszenie to skutkowało ryzykiem naruszenia praw lub wolności osób fizycznych. Do zgłoszenia przekazanego organowi nadzorczemu po upływie 72 godzin dołącza się wyjaśnienie przyczyn opóźnienia.

Wedle zaś art. 33 ust. 3 RODO, zgłoszenie, o którym mowa w ust. 1, musi co najmniej:

1. opisywać charakter naruszenia ochrony danych osobowych, w tym w miarę możliwości wskazywać kategorie i przybliżoną liczbę osób, których dane dotyczą, oraz kategorie i przybliżoną liczbę wpisów danych osobowych, których dotyczy naruszenie;
2. zawierać imię i nazwisko oraz dane kontaktowe inspektora ochrony danych lub oznaczenie innego punktu kontaktowego, od którego można uzyskać więcej informacji;

3. opisywać możliwe konsekwencje naruszenia ochrony danych osobowych;
4. 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.

Uzyskanie dostępu do danych osobowych pacjentów zgromadzonych w dokumentacji medycznej (imion, nazwisk, numerów PESEL, danych teleadresowych oraz danych dotyczących zdrowia) nie jest sytuacją, w której ryzyko naruszenia praw lub wolności osób fizycznych jest mało prawdopodobne. W związku z tym, **podmiot wykonujący działalność leczniczą** (podmiot leczniczy lub osoba wykonująca zawód medyczny w ramach praktyki zawodowej) **ma obowiązek zgłoszenia do Prezesa Urzędu Ochrony Danych Osobowych incydentu naruszenia ochrony danych osobowych swoich pacjentów**, w ciągu 72 godzin od stwierdzenia naruszenia. Obowiązek ten powstaje niezależnie od tego, czy dane osobowe pacjentów zostały w jakikolwiek sposób upublicznione lub wykorzystane. Liczy się bowiem sam fakt uzyskania dostępu do tych danych przez osoby nieuprawnione.

Momentem stwierdzenia naruszenia może być w niniejszej sprawie otrzymanie od dostawcy oprogramowania informacji o tym, że dane osobowe pacjentów placówki znajdują się wśród danych, do których dostęp uzyskały nieuprawnione osoby. **Rekomendowanym jest uzyskanie w pierwszej kolejności indywidualnej informacji od dostawcy oprogramowania** dotyczącej danych osobowych pacjentów danej placówki i w przypadku, gdy dostawca oprogramowania potwierdzi, że dane pacjentów danej placówki znajdują się wśród ujawnionych danych, aktualizuje się obowiązek dokonania zawiadomienia do Prezesa UODO.

Warto mieć na uwadze, że zgodnie z art. 33 ust. 5 RODO, administrator dokumentuje wszelkie naruszenia ochrony danych osobowych, **w tym okoliczności naruszenia ochrony danych osobowych, jego skutki oraz podjęte działania zaradcze.** Dokumentacja ta musi pozwolić organowi nadzorczemu weryfikowanie przestrzegania niniejszego artykułu.

Kolejno, zgodnie z art. 34 ust. 1 RODO, jeżeli naruszenie ochrony danych osobowych może powodować wysokie ryzyko naruszenia praw lub wolności osób fizycznych, **administrator bez zbędnej zwłoki zawiadamia osobę, której dane dotyczą, o takim naruszeniu.**

Należy w tym miejscu powtórzyć za P. Litwińskim, że: *jak wskazuje się w literaturze, w tym przypadku RODO posługuje się kategorią "naruszenia praw lub wolności osób fizycznych", wskazując na ich uniwersalny zakres i charakter, a więc na prawa i wolności przysługujące jednostce na podstawie obowiązującego prawodawstwa, w tym Konstytucji RP, KPP, TFUE, EKPCz, RODO i innych aktów. Jak również wskazuje się w piśmiennictwie, "naruszeniem prawa lub wolności podmiotu będzie sytuacja, w której administrator danych lub podmiot przetwarzający nie zrealizuje lub zaniecha realizacji któregoś z praw przysługujących podmiotowi danych" (...)*

*Odmiennie niż w przypadku zgłoszenia naruszenia z art. 33 RODO, obowiązek powiadomienia z art. 34 RODO **dotyczy sytuacji hipotetycznych,** a więc potencjalnego ryzyka naruszenia praw i wolności*

podmiotu danych i jego poziomu. Omawiana przesłanka nie wymaga, by wysokie ryzyko się zmaterializowało i by faktycznie doszło do naruszenia praw lub wolności.

W myśl art. 34 ust. 2 RODO, zawiadomienie, o którym mowa w ust. 1 niniejszego artykułu, jasnym i prostym językiem opisuje charakter naruszenia ochrony danych osobowych oraz zawiera przynajmniej informacje i środki, o których mowa w art. 33 ust. 3 lit. b), c) i d). Jak zaś stanowi ust, 3 ww. przepisu, zawiadomienie, o którym mowa w ust. 1, nie jest wymagane, w następujących przypadkach:

1. administrator wdrożył odpowiednie techniczne i organizacyjne środki ochrony i środki te zostały zastosowane do danych osobowych, których dotyczy naruszenie, w szczególności środki takie jak szyfrowanie, uniemożliwiające odczyt osobom nieuprawnionym do dostępu do tych danych osobowych;
2. administrator zastosował następnie środki eliminujące prawdopodobieństwo wysokiego ryzyka naruszenia praw lub wolności osoby, której dane dotyczą, o którym mowa w ust. 1;
3. wymagałoby ono niewspółmiernie dużego wysiłku. W takim przypadku wydany zostaje publiczny komunikat lub zastosowany zostaje podobny środek, za pomocą którego osoby, których dane dotyczą, zostają poinformowane w równie skuteczny sposób.

W ocenie opiniującego, w niniejszej sprawie ujawnienie danych osobowych pacjentów **może powodować wysokie ryzyko naruszenia praw lub wolności osób fizycznych**. Pacjenci korzystający z usług podmiotu wykonującego działalność leczniczą mają bowiem prawo do poszanowania ich prywatności, a dane zawarte w dokumentacji medycznej podlegają szczególnej ochronie. W sytuacji, w której nieuprawnione osoby uzyskały dostęp do danych osobowych pacjentów np. w postaci imienia i nazwiska, numeru PESEL oraz danych dotyczących zdrowia, rodzi to **wysokie ryzyko** wyrządzenia pacjentom szkody majątkowej, krzywdy lub tzw. kradzieży tożsamości. W związku z tym, w przypadku otrzymania od dostawcy oprogramowania informacji o tym, że dane pacjentów placówki są objęte naruszeniem, **administratorzy mają obowiązek dokonania zawiadomienia swoich pacjentów o naruszeniu ochrony ich danych osobowych.**

Należy przy tym wskazać, że nie jest wymagane, aby ww. zawiadomienie zostało dokonane w formie pisemnej - istotne jest, aby administrator mógł później wykazać, że dokonał zawiadomienia. Rekomendowanym jest, aby zawiadomienie zostało dokonane w formie umożliwiającej szybkie zapoznanie się z jego treścią, zatem **możliwe jest wystosowanie w tej sprawie wiadomości SMS albo e-mail do pacjentów (z funkcją ukrycia odbiorców)**. Jeżeli wiązałoby się to dla administratora z nadmiernym wysiłkiem (np. z uwagi na liczbę osób objętych naruszeniem i brak środków technicznych do dokonania indywidualnego zawiadomienia), konieczne byłoby wówczas zawiadomienie pacjentów w inny sposób, np. poprzez **komunikat na stronie internetowej podmiotu wykonującego działalność leczniczą.**

Niezależnie od powyższego, zgodnie z art. 34 ust. 4 RODO, jeżeli administrator nie zawiadomił jeszcze osoby, której dane dotyczą, o naruszeniu ochrony danych osobowych, **organ nadzorczy** – biorąc pod uwagę prawdopodobieństwo, że to naruszenie ochrony danych osobowych spowoduje wysokie ryzyko

– **może od niego tego zażądać lub może stwierdzić, że spełniony został jeden z warunków, o których mowa w ust. 3.**

Prezes UODO w związku z otrzymanym zawiadomieniem **może zażądać od administratora poinformowania pacjentów o tym naruszeniu**, albo stwierdzić, że zachodzi okoliczność zwalniająca administratora z takiego obowiązku.

Na marginesie, w zakresie odpowiedzialności za incydent naruszenia ochrony danych osobowych, należy wskazać, iż zgodnie z art. 77 ust. 1 RODO, bez uszczerbku dla innych administracyjnych lub środków ochrony prawnej przed sądem **każda osoba, której dane dotyczą, ma prawo wnieść skargę do organu nadzorczego,** w szczególności w państwie członkowskim swojego zwykłego pobytu, swojego miejsca pracy lub miejsca popełnienia domniemanego naruszenia, jeżeli sądzi, że przetwarzanie danych osobowych jej dotyczące narusza niniejsze rozporządzenie.

Ponadto, zgodnie z art. 78 ust. 1 RODO, bez uszczerbku dla innych administracyjnych lub pozasądowych środków ochrony prawnej **każda osoba fizyczna lub prawna ma prawo do skutecznego środka ochrony prawnej przed sądem przeciwko prawnie wiążącej decyzji organu nadzorczego jej dotyczącej.**

Kolejno, osobie, której dane naruszono, przysługuje prawo do dochodzenia roszczeń **przeciwko administratorowi lub podmiotowi przetwarzającemu.** W myśl art. 82 ust. 1-2 RODO, każda osoba, która poniosła szkodę majątkową lub niemajątkową w wyniku naruszenia niniejszego rozporządzenia, ma prawo uzyskać od administratora lub podmiotu przetwarzającego odszkodowanie za poniesioną szkodę.

Każdy administrator uczestniczący w przetwarzaniu odpowiada **za szkody** spowodowane przetwarzaniem naruszającym niniejsze rozporządzenie. **Podmiot przetwarzający odpowiada za szkody spowodowane przetwarzaniem wyłącznie, gdy nie dopełnił obowiązków, które niniejsze rozporządzenie nakłada bezpośrednio na podmioty przetwarzające, lub gdy działał poza zgodnymi z prawem poleceniami administratora lub wbrew takim poleceniom.**

Administrator lub podmiot przetwarzający zostają zwolnieni z odpowiedzialności wynikającej z ust. 2, **jeżeli udowodnią, że w żaden sposób nie ponoszą winy za zdarzenie, które doprowadziło do powstania szkody** (art. 82 ust. 3 RODO).

Administratorzy w niniejszej sytuacji mogliby zwolnić się z odpowiedzialności za ewentualne szkody poniesione przez pacjentów, w związku z tym, że incydent naruszenia ochrony danych ma charakter ogólnokrajowy, na poziomie dostawcy oprogramowania do prowadzenia dokumentacji medycznej i nie wynika z działań lub zaniechań administratora. Odpowiedzialność administratora będzie wyłączona, jeżeli administrator dopełni wyżej wskazanych obowiązków bez zbędnej zwłoki i w porozumieniu z organem nadzorczym.

LEX SECURE
24H OPIEKA PRAWNA

RZECZPOSPOLITA RANKING KANCELARII PRAWNICZYCH XXIII I MIEJSCE

Klauzula prawna:

Przygotowując niniejszą Opinię prawną przeanalizowano i polegano wyłącznie na informacjach otrzymanych od Klienta. Nie badano ani nie weryfikowano prawdziwości przedstawionego stanu faktycznego. Lex Secure S.A. zastrzega sobie prawo weryfikacji niniejszego opracowania w przypadku ujawnienia faktów nieznanych w momencie jego sporządzenia.

Niniejszą Opinię prawną wydaje się do wiadomości i do użytku Klienta wraz z prawem do publikacji przez Klienta. Opinia prawna dotyczy wyłącznie kwestii w niej określonych i nie może być interpretowana jako obejmująca, w tym przez domniemanie, inne, niewspomniane w niej kwestie.

W niniejszej Opinii prawnej zaprezentowano niezależną, subiektywną ocenę Lex Secure S.A., dotyczącą prawnych aspektów przedmiotu analizy. W szczególności ocena prawna przedstawiona w Opinii prawnej nie daje gwarancji wyniku danej sprawy w przypadku skierowania jej na drogę postępowania sądowego lub administracyjnego.

Z poważaniem

RADCA PRAWNY
Kotrysiak
Dawid Kotrysiak

LEX SECURE
SPÓŁKA AKCYJNA
Al. Niepodległości 723/6
81-853 Sopot

NIP: 5862017484
REGON: 191884226
KRS: 0001174017

biuro@opiekaprawna.pl
www.opiekaprawna.pl
www.lexsecure.pl

tel. +48 58 500 59 00
24h Infolinia Prawna
+48 501 538 539