Artur Górecki

# *Czy prywatną służbę zdrowia stać na brak ochrony danych osobowych pacjentów?*

*Can a private health service afford the absence of protection of patient's personal data?*

mgr Artur Górecki,
Prezes Zarządu Standarder Sp. z o.o.,
ul. Kolista 25, 40-486 Katowice
artur.gorecki@standarder.pl

*Słowa kluczowe:*
*dane osobowe, dokumentacja medyczna*

*Key words:*
*personal data, medical records*

## Czy prywatną służbę zdrowia stać na brak ochrony danych osobowych pacjentów?

Tytuł artykułu może trochę zaskakiwać, bo po pierwsze: dlaczego skupiać się na placówkach prywatnych skoro mamy także placówki publiczne? Mało tego, w jednym i drugim przypadku mamy do czynienia z przetwarzaniem danymi „wrażliwych", a ustawa o ochronie danych osobowych takiego podziału nie wprowadza. Po drugie: oczywiste jest, że nikt świadomie nie chce płacić jakichkolwiek kar czy też ponosić konsekwencji zaniedbań. Poza tym, użycie słowa „stać" może na pierwszy rzut oka wydawać się niefortunne, ale w moim odczuciu nie jest, co postaram się wykazać w dalszej części artykułu. Wreszcie, po trzecie: słowo „stać" sugeruje zaglądanie do portfeli właścicieli/ zarządzających placówkami prywatnymi. Nie taki jest cel, ale z punktu widzenie dzisiejszych rozważań, nie jest to bez znaczenia.

## Po pierwsze: dlaczego placówki prywatne...

Zarówno placówki prywatne jak i publiczne są zobowiązane z mocą ustawy do takiej samej, szczególnej ochrony przetwarzanych danych (dokładnie opisał to Adam Piątek w IS nr 1(7)2013) Niestety, w obu przypadkach nie wygląda to dobrze. Błędnie rozumiana konieczność rejestrowania zbiorów danych osobowych w ogólnokrajowym rejestrze danych osobowych, zakorzenione tzw. „nawyki branżowe" poparte argumentami „po co zmieniać, zawsze tak robiliśmy i było dobrze" świadczy o braku świadomość w zakresie danych osobowych (pisał o tym szczegółowo Kajetan Jordan w IS nr 2(6) 2012). Należałoby jeszcze dodać nagminne przypadki dostępu do danych medycznych przypadkowych osób i zwykłe bałaganiarstwo. Bardzo częstym przypadkiem (piętnowanym przez GIODO) jest umożliwienie dostępu do danych pacjentów osobom nieupoważnionym. Poza pielęgniarkami, położnymi i osobami które z racji bezpośredniego uczestniczenia w leczeniu pacjenta dostęp do danych medycznych mieć powinny faktyczny dostęp ma administracja, ochrona a nawet personel sprzątający (regulacje prawne dotyczące prowadzenia i udostępniania dokumentacji medycznej zawierają przepisy m. in. ustawy z dnia 6 listopada 2008 r. o prawach pacjenta i Rzeczniku Praw Pacjenta oraz rozporządzenia Ministra Zdrowia z dnia 21 grudnia 2010 r.). Bardzo częstym przypadkiem jest przetwarzanie danych medycznych w niezabezpieczonych systemach teleinformatycznych, stwarza to ryzyko ich wycieku. Aby temu zapobiec niezbędny jest „sys-

### Streszczenie

*Dlaczego sektor prywatny służby zdrowia jest bardziej narażony na konsekwencje braku ochrony danych osobowych? Najczęstsze „grzechy" sektora medycznego w zakresie ochrony danych osobowych. Kary i inne konsekwencje braku w placówce systemu ochrony danych osobowych.*

### Abstract

*Why is the private sector of health service more exposed to the consequences of absence of protection of personal data? The most common „sins" of the medical sector in terms of protection of personal data. Retributions and other consequences of absence of protection of personal data in the institution.*

tem ochrony danych osobowych", ale… Aby wprowadzić „system" ochrony danych osobowych potrzebne są chęci, pieniądze i decyzja. W przypadku placówek publicznych wygląda to różnie. Zwykle są chęci, ale nie ma pieniędzy (te które są, przeznaczane są na łatanie dachów, wymiany kotłowni lub okien). W związku z tym decyzji zwykle nie ma i w efekcie niewiele się zmienia.

Znacznie lepiej wygląda to w sektorze prywatnym. Pieniądze łatwiej się znajdują, kiedy w połączeniu z decyzją, chęciami i konsekwencją dają sprawnie działający system ochrony danych osobowych. Sektor prywatny chętniej korzysta z outsourcingu, różnego rodzaju nowinek technologicznych, także w tym przypadku bez właściwych procedur ochrony danych może się skończyć tragicznie. Poza tym mam wrażenie (mogę oczywiście się

mylić), że świadomość tematu ochrony danych w sektorze prywatnym jest większa oraz większa jest chęć pogłębiania wiedzy w tym temacie. Oczywiście, nadal mogą trafić się właściciele prywatnych placówek medycznych, którzy są przekonani, że w ich jednostkach wszystko działa zgodnie z wymogami ustawy o ochronie danych osobowych, a w rzeczywistości jest inaczej. Proponuję to zweryfikować, bo właśnie na osobie właściciela lub prezesa spoczywa odpowiedzialność za należyte, bezpieczne przetwarzanie danych osobowych zgodnie z wymogami ustawy o ochronie danych osobowych.

## Po drugie: kary... konsekwencje...

Temat bardzo nielubiany, choć nie przez wszystkich. Kilkakrotnie zetknąłem się z relacjami ze szkoleń dla pracowników sektora ochrony zdrowia, gdzie sankcje karne były bardzo mocno akcentowane, a prowadzący szkolenie mówiąc o nich z satysfakcją patrzyli na szeroko otwarte ze strachu oczy uczestników. Chciałbym się skupić na innych konsekwencjach braku lub nienależytej ochrony danych osobowych. Jeszcze nie tak dawno, bo 2-3 lata temu, temat ochrony danych osobowych był tematem mało znanym i mało popularnym. O ochronie danych mówiło się rzadko, a na pewno nie tak powszechnie jak dziś. Często osobom zajmującym decyzyjne stanowiska należało tłumaczyć, co to są dane osobowe i dlaczego należy je chronić. Przypomnijmy zatem, że ustawa z dnia 29 sierpnia 1997 roku o ochronie danych osobowych obowiązuje od 30 kwietnia 1998 roku nawet dziś obowiązek stosowania się do jej wymogów.

Dziś jest inaczej. Temat jest chyba wszystkim znany, a i pacjenci są świetnie wyedukowani. Z jednej strony dobrze, bo tak być powinno, z drugiej zaś strony niesie to pewne zagrożenia. Znane mi są przypadki żądania zadośćuczynienia finansowego za konsekwencje wydania dokumentacji medycznej osobie nieuprawnionej, spraw sądowych pacjentów z placówkami medycznymi o odszkodowania za naruszenie prawa do prywatności (wyciek danych medycznych). Nie można nie wspomnieć o kilku przypadkach z ostatnich miesięcy, kiedy to niezadowoleni pacjenci w spornych sprawach straszyli lub wskazywali nieprawidłowości w ochronie danych osobowych właściwemu urzędowi (GIODO). Znane są przypadki gdy zwolnieni pracownicy placówek medycznych „donoszą" w zemście na pracodawcy o nieprawidłowościach do GIODO, PIP, US itp. instytucji. Jeszcze kilka lat wstecz GIODO nie byłoby na tej liście.

Jakie są lub mogą być tego konsekwencje ?

- pogorszenie wizerunku placówki, lekarza
- w konsekwencji utrata pacjentów,
- kontrole GIODO utrudniające bieżące działanie jednostki
- strata czasu na rozprawy sądowe itp.
- niepotrzebny stres utrudniający pracę

Konsekwencje finansowe

- zasądzone odszkodowania,
- przestoje w funkcjonowaniu placówki
- utrata dochodu
- nałożone kary pieniężne (do 200 tys. zł)

Konsekwencje prawne,

- kara ograniczenia wolności albo pozbawienia wolności do lat 3

Nie wygląda to dobrze, a ma być jeszcze gorzej. Według projektu unijnych zmian, kary pieniężne mają sięgać do miliona euro lub 2% obrotów.

## Po trzecie: czy placówki prywatne „stać"...

Nie jest moim celem rozważanie czy 200 tys. zł kary do kwota duża czy nie. Pewnie będą tacy którzy stwierdzą że nie jest wysoka, będą także tacy którzy powiedzą, że kara jest wysoka i niepotrzebna. Nie zapominajmy o tym, że ciągle rosnąca świadomość w tematyce ochrony danych osobowych daje pole do popisu ludziom, którzy specjalizują się w wyłudzaniu odszkodowań wspierani przez wyspecjalizowane kancelarie prawne. W Polsce, w porównaniu z innymi krajami takimi jak: Francja, Wielka Brytania, Niemcy czy USA nie są to liczne przypadki, ale jest i będzie ich coraz więcej. Czy takie osoby wezmą na cel publiczny szpital lub przychodnię? Czy może prywatną placówkę? Proszę odpowiedzieć sobie na to pytanie.

## Podsumowanie:

Problem opisany powyżej dotyczy całego sektora ochrony zdrowia, a jedynie dla uwypuklenia pewnych zależności skupiłem się na sektorze prywatnym. Czy prywatną służbę zdrowia stać na brak ochrony danych osobowych pacjentów? Pewnie większość czytelników stwierdzi że nie stać.

Jedno jest pewne, każdą jednostkę stać na system ochrony danych osobowych; ten wydatek i wysiłek się opłaca. Dzięki niemu możemy spać spokojnie, nie musimy się bać incydentów, kontroli. Możemy powiedzieć: „pacjencie drogi, my chronimy Twoje dane, u nas są bezpieczne". No i możemy być zgodni z wymogami ustawy o ochronie danych osobowych".