



GENERALNY INSPEKTOR OCHRONY DANYCH OSOBOWYCH

Michał Serzycki

Warszawa, dnia 31 sierpnia 2009 r.

DIS/DEC-876/31611/09

dot. [...]

DECYZJA

Na podstawie art. 104 § 1 ustawy z dnia 14 czerwca 1960 r. Kodeks postępowania administracyjnego (Dz. U. z 2000 r. Nr 98, poz. 1071 z późn. zm.) oraz art. 12 pkt 2, art. 18 ust. 1 pkt 1 i pkt 6 i art. 22 w związku z art. 27 ust. 2 pkt 2 ustawy z dnia 29 sierpnia 1997 r. o ochronie danych osobowych (Dz. U. z 2002 r. Nr 101, poz. 926 z późn. zm.), po przeprowadzeniu postępowania administracyjnego w sprawie przetwarzania danych osobowych przez Pana J. B. prowadzącego działalność gospodarczą pod firmą L.,

Nakazuję Panu J. B. prowadzącemu działalność gospodarczą pod firmą L., przywrócenie stanu zgodnego z prawem, poprzez usunięcie z urządzenia [...] typu [...] danych osobowych Pana E. B., w terminie miesiąca od dnia, w którym niniejsza decyzja stanie się ostateczna.

Uzasadnienie

Inspektorzy, upoważnieni przez Generalnego Inspektora Ochrony Danych Osobowych przeprowadzili u Pana J. B. prowadzącego działalność gospodarczą pod firmą L., kontrolę zgodności przetwarzania danych osobowych z przepisami o ochronie danych osobowych sygn. akt [...], tj. ustawą z dnia 29 sierpnia 1997 r. o ochronie danych osobowych (Dz. U. z 2002 r. Nr 101, poz. 926 z późn. zm.), zwaną dalej ustawą oraz rozporządzeniem Ministra Spraw Wewnętrznych i

Administracji z dnia 29 kwietnia 2004 r. w sprawie dokumentacji przetwarzania danych osobowych oraz warunków technicznych i organizacyjnych, jakim powinny odpowiadać urządzenia i systemy informatyczne służące do przetwarzania danych osobowych (Dz. U. Nr 100, poz. 1024).

W toku kontroli odebrano od Pana J. B. ustne wyjaśnienia, skontrolowano system informatyczny służący do przetwarzania danych osobowych oraz dokonano oględzin pomieszczeń, w których odbywa się przetwarzanie danych osobowych. Stan faktyczny został szczegółowo opisany w protokole kontroli sygn. akt [...], który został podpisany przez Pana J. B.

Na podstawie tak zgromadzonego materiału dowodowego ustalono, że w procesie przetwarzania danych osobowych Pan J. B. prowadzący działalność gospodarczą pod firmą L. naruszył przepisy o ochronie danych osobowych. Uchybienie to polegało na przetwarzaniu bez podstawy prawnej, o której mowa w art. 27 ust. 2 pkt. 2 ustawy o ochronie danych osobowych danych osobowych pacjentów C. Sp. z o.o. (w tym danych osobowych Pana E. B.).

W związku z powyższym pismem z dnia [...] czerwca 2009 r. sygn. [...], zawiadamiającym o wszczęciu postępowania administracyjnego w przedmiotowej sprawie, Pan J. B. prowadzący działalność gospodarczą pod firmą L. (zwany dalej także Przedsiębiorcą) został poinformowany o prawie czynnego udziału w każdym stadium postępowania, a przed wydaniem decyzji wypowiedzenia się co do zebranych dowodów i materiałów oraz zgłoszonych żądań.

W odpowiedzi na zawiadomienie o wszczęciu postępowania administracyjnego Przedsiębiorca pismem z dnia [...] czerwca 2009 r. przesłał wyjaśnienia w zakresie stwierdzonego uchybienia. Z udzielonych wyjaśnień wynika, że:

1. Zasadne byłoby przeprowadzenie dowodu z wyjaśnień złożonych pismem z dnia [...] maja 2009 r. przez Autoryzowanego Dystrybutora G. (producenta urządzenia [...] typu [...]), w zakresie istnienia możliwości samodzielnego, usunięcia danych osobowych z tego urządzenia. Gdyż jak wynika z wyjaśnień tego podmiotu usunięcie danych osobowych pacjentów z tego urządzenia jest możliwe. Natomiast z informacji jakie pozyskał Pan J. B. na szkoleniach w zakresie obsługi tego urządzenia wynika, iż jako użytkownik tego urządzenia nie może usunąć danych osobowych pacjentów. Natomiast całkowite usunięcie byłoby możliwe jedynie przez pracownika serwisu, mającego uprawnienia do ingerencji w treść oprogramowania.
2. Zgodnie z umową zlecenia Nr [...] zawartą w dniu [...] lutego 2002 r. pomiędzy Panem J. B., a C. Sp. z o.o. wynika, iż C. Sp. z o.o. (zlecniodawca) było zobowiązane do zapewnienie bazy lokalowo-administracyjnej i wsparcia technicznego. Natomiast Pan J. B., był zobowiązany do prowadzenie działalności lekarskiej w ramach prywatnej praktyki wyłącznie na terenie placówek C. Sp. z o.o., udzielania konsultacji i badań diagnostycznych pacjentom wyłącznie w placówkach C. Sp. z o.o. z uwzględnieniem cennika stosowanego przez C. Sp. z o.o. Z postanowień zawartej umowy, zdaniem Pana J. B. wynika, iż osoby poddawane badaniom mieli być pacjentami Pana J. B., dlatego też w jego ocenie administrował on danymi osobowymi tych pacjentów.

3. Jako lekarz wykonujący praktykę lekarską Pan J. B. miał obowiązek prowadzenia i przechowywania dokumentacji medycznej pacjentów, zgodnie z obowiązującym wówczas rozporządzeniem Ministra Zdrowia z 30 lipca 2001 r. w sprawie rodzajów indywidualnej dokumentacji medycznej, sposobu jej prowadzenia oraz szczególnych warunków jej udostępniania (Dz. U. nr 83, poz. 903).

4. Pan J. B. pozyskał dane osobowe Pana E. B. w C. Sp. z o.o. bezpośrednio od tego pacjenta w związku z koniecznością wpisania ich do dokumentacji medycznej, w celu przeprowadzenia badania [...].

5. Zarówno wykonując badanie [...] pacjenta Pana E. B., jak również przekazując dane tego pacjenta Niepublicznemu Zakładowi Opieki Zdrowotnej K. w celu zaproszenia pacjenta na badanie kontrolne, Pan J. B. działał (w jego przekonaniu), zgodnie z ustawą z dnia 5 grudnia 1996 r. o zawodach lekarza i lekarza dentysty (Dz. U. 2008 r. Nr 136, poz. 857 z późn. zm.) oraz zgodnie z Kodeksem Etyki Lekarskiej z dnia 2 stycznia 2004 r. Zgodnie bowiem z art. 2 ust. 2 ww. kodeksu, najwyższym nakazem etycznym lekarza jest dobro chorego. 6. Zgodnie z pkt. 4.3.b Rekomendacji R (97) 5 Rady Europy Komitetu Ministrów do Państw Członkowskich dotyczących ochrony danych medycznych, dane dotyczące zdrowia mogą być gromadzone i przetwarzane w celach terapeutycznych związanych z osobą, której dotyczą lub dla celów ochrony żywotnych interesów osoby, której dotyczą, zaś zgodnie z pkt. 4.4 jeżeli zostały zgromadzone w celach diagnostycznych. Mogą być przetwarzane dla celów wykonywania usługi medycznej w interesie pacjenta.

7. W ocenie Pana J. B. przyjęcie, że dane osobowe pacjentów pozyskane w związku z wykonywaniem badań w okresie współpracy z C. Sp. z o.o. są własnością C. Sp. z o.o., jest o tyle nieprawidłowe, że dane te pozostają nadal w urządzeniu, [...], zaś osobą (podmiotem) przetwarzającą te dane, zarówno w dacie przeprowadzonego badania tj. w dniu 11 listopada 2004 r., jak i do dnia dzisiejszego jest Pan J. B.

Po zapoznaniu się z całością materiału dowodowego zebranego w sprawie Generalny Inspektor Ochrony Danych Osobowych zważył, co następuje:

Zgodnie z art. 27 ust. 1 ustawy zabrania się przetwarzania danych ujawniających pochodzenie rasowe lub etniczne, poglądy polityczne, przekonania religijne lub filozoficzne, przynależność wyznaniową, partyjną lub związkową, jak również danych o stanie zdrowia, kodzie genetycznym, nałogach lub życiu seksualnym oraz danych dotyczących skazań, orzeczeń o ukaraniu i mandatów karnych, a także innych orzeczeń wydanych w postępowaniu sądowym lub administracyjnym. Natomiast zgodnie z art. 27 ust. 2 pkt 2 ustawy przetwarzanie danych, o których mowa w ust. 1, jest jednak dopuszczalne, gdy przepis szczególny innej ustawy zezwala na przetwarzanie takich danych bez zgody osoby, której dane dotyczą, i stwarza pełne gwarancje ich ochrony.

Jak ustalono w toku kontroli, badanie [...] Pana E. B., wykonane zostało przez Pana J. B. w dniu [...] października 2004 r. w C. Sp. z o.o. Czynności te Pan J. B. wykonał na podstawie umowy cywilno – prawnej tj. umowy zlecenia Nr [...] zawartej w dniu [...] lutego 2002 r. pomiędzy Panem J. B. a C. Sp. z o.o., która została rozwiązana w dniu [...] września 2006 r. Przedmiotowe badanie zostało wykonane przy użyciu urządzenia [...] typu [...] nr [...] i w związku z tym, w urządzeniu tym zostały zapisane dane osobowe pacjenta Pana E. B. W dniu [...] lutego 2007 r. nastąpiła deinstalacja ww. urządzenia w C. Sp. z o.o. Ponadto, jak ustalono w toku kontroli z urządzenia tego nie zostały jednak usunięte dane osobowe pacjentów C., w tym dane osobowe Pana E. B., a tym samym dane ww. osób przetwarzane są nadal w tym urządzeniu pomimo, iż Pan J. B. nie współpracuje już z C. Sp. z o.o.

Ponadto, w toku kontroli ustalono również, iż dane osobowe Pana E. K. zostały udostępnione przez Pana J. B. osobom nieupoważnionym tj. Niepublicznemu Zakładowi Opieki Zdrowotnej K., podmiotowi w którym obecnie użytkowane jest przedmiotowe urządzenie.

Odnosząc się do ww. wyjaśnień złożonych pismem z dnia [...] czerwca 2009 r. jako odpowiedzi na zawiadomienie o wszczęciu postępowania administracyjnego, w ocenie Generalnego Inspektora Ochrony Danych Osobowych nie ma konieczności przeprowadzania dowodu z wyjaśnień złożonych w piśmie z dnia [...] maja 2009 r. Autoryzowanego Dystrybutora [...] (producenta urządzenia [...] typu [...] nr [...]), gdyż Generalny Inspektor Ochrony Danych Osobowych nie kwestionuje, iż całkowite usunięcie danych osobowych z urządzenia [...] typu [...] może być dokonane tylko przez pracownika ww. serwisu. Natomiast fakt ten nie usprawiedliwia Pana J. B., jako właściciela tego urządzenia, by jako podmiot nieupoważniony już do przetwarzania danych osobowych pacjentów C. Sp. z o.o., nadal wykorzystywał dane tych pacjentów.

Ponadto, odnosząc się do wyjaśnień Pana J. B., iż w związku z realizacją umowy zlecenia Nr [...] zawartej w [...] lutego 2002 r. z C. Sp. z o.o. był on zobowiązany do prowadzenia i przechowywania dokumentacji medycznej pacjentów - nie można zgodzić się z takim stwierdzeniem, gdyż z treści przedmiotowej umowy (§ 3) wynika, iż C. Sp. z o.o., zobowiązane jest zarówno do zapewnienia obsługi związanej z rejestracją pacjentów i rozliczeniami należności, jak również do ewidencjonowania i przechowywania dokumentacji lekarskiej. Ponadto, nie można również uznać, iż administratorem danych pacjentów pozyskanych w związku z wykonywaniem badań [...] przy użyciu przedmiotowego urządzenia w ramach realizacji ww. umowy zlecenia jest Pan J. B. Zgodnie bowiem z art. 7 pkt 4 ustawy o ochronie danych osobowych, ilekroć w ustawie jest mowa o administratorze danych rozumie się przez to organ, jednostkę organizacyjną, podmiot lub osobę o których mowa w art. 3 ustawy, decydujące o celach i środkach przetwarzania danych osobowych. Wobec powyższego należy uznać, iż administratorem danych pacjentów badanych przy użyciu przedmiotowego urządzenia w ramach realizacji ww. umowy zlecenia jest C. Sp. z o.o., gdyż podmiot, ten zawierając przedmiotową umowę decydował o celach i środkach przetwarzanych

danych osób, o których mowa powyżej. Ponadto, z treści przedmiotowej umowy zlecenia wynika, iż Pan J. B. zobowiązany jest do przestrzegania regulaminów obowiązujących w C. Sp. z o.o., w tym regulaminu pracy.

Nie można również uznać, iż po rozwiązaniu przedmiotowej umowy zlecenia, jak również umów o współpracy zawartych z C. Sp. z o.o., przekazując dane pacjenta Pana E. B. Niepublicznemu Zakładowi Opieki Zdrowotnej K. w celu zaproszenia osoby tej na badanie kontrolne, Pan J. B. działał zgodnie z ustawą z dnia 5 grudnia 1996 r. o zawodach lekarza i lekarza dentysty (Dz. U. 2008 r. Nr 136, poz. 857 z późn. zm.) oraz zgodnie z Kodeksu Etyki Lekarskiej z dnia 2 stycznia 2004 r. Bowiem zgodnie z art. 32 ust. 1 ustawy o zawodach lekarza i lekarza dentysty, lekarz może przeprowadzić badanie lub udzielić świadczeń zdrowotnych, z zastrzeżeniem wyjątków przewidzianych w ustawie, po wyrażeniu zgody przez pacjenta. Ponadto, zgodnie z art. 15 pkt 1 Kodeksu Etyki Lekarskiej postępowanie diagnostyczne, leczenie zapobiegawcze wymaga zgody pacjenta. Z pozyskanego materiału dowodowego wynika, iż nie została pozyskana zgoda pacjenta Pana E. B. na przeprowadzenie kontrolnego badania diagnostycznego.

Na podstawie materiału dowodowego zebranego w niniejszej sprawie, należy stwierdzić, iż dane osobowe Pana E.B. pacjenta C. Sp. z o.o., Przedsiębiorca przetwarza bez podstawy prawnej, o której mowa w art. 27 ust. 2 pkt 2 ustawy o ochronie danych osobowych.

Wobec powyższego, Generalny Inspektor Ochrony Danych Osobowych rozstrzygnął jak w sentencji.

Decyzja jest ostateczna. Na podstawie art. 21 ust. 1 ustawy o ochronie danych osobowych oraz art. 129 § 2 Kodeksu postępowania administracyjnego, strona niezadowolona z niniejszej decyzji może zwrócić się do Generalnego Inspektora Ochrony Danych Osobowych (adres: ul. Stawki 2, 00-193 Warszawa) z wnioskiem o ponowne rozpatrzenie sprawy, w terminie 14 dni od dnia doręczenia niniejszej decyzji.