



**GENERALNY INSPEKTOR
OCHRONY DANYCH
OSOBOWYCH**
Michał Serzycki

2009 11.10
Rechenberg
[Signature]

DOLiS – 033 – 380 / 09 / 40362

Warszawa, dnia 3 listopada 2009 r.

PZ
[Signature]
PODSEKRETARZ STANU
w Ministerstwie zdrowia
Marek Twardowski
2009-11-10

Pan
Marek Twardowski
Podsekretarz Stanu
w Ministerstwie Zdrowia
ul. Miodowa 15
00 – 952 Warszawa

SEKRETARIAT
PODSEKRETARZA STANU
Marka Twardowskiego
09 LIS. 2009
Nr rejestru pozycji... MT-9220

Szanowny Panie Ministrze

w nawiązaniu do pisma z dnia 21 października 2009 r. (znak: MZ-PZ-TSZ-401-5262-11/SP/09) uprzejmie informuję, iż w projekcie rozporządzenia Ministra Zdrowia w sprawie ośrodków dawców szpiku wątpliwości pod kątem zgodności z przepisami ustawy z dnia 29 sierpnia 1997 r. o ochronie danych osobowych (t.j. Dz. U. z 2002 r. Nr 101, poz. 926, z późn. zm.) budzą następujące przepisy.

1) Nie można zaakceptować przewidzianej w § 4 ust. 5 projektu możliwości wykonywania badania antygenów zgodności tkankowej, cyt.: „(...) poza granicami kraju (...)”, w sytuacji, gdy z projektowanych przepisów nie wynika, czy w ww. przypadku chodzi o państwa należące do Europejskiego Obszaru Gospodarczego (na obszarze których obowiązują przepisy dotyczące ochrony danych osobowych), czy państwa spoza tego obszaru, a więc – w rozumieniu ustawy o ochronie danych osobowych – państwa trzecie (art. 7 pkt 7), które nie muszą dawać gwarancji ochrony danych osobowych przynajmniej takich, jakie obowiązują na terytorium Rzeczypospolitej Polskiej. Podkreślić należy, iż podstawą do przekazywania danych osobowych do państw trzecich (co niewątpliwie stanowi ingerencję w prawa i wolności jednostki zawarte w Konstytucji Rzeczypospolitej Polskiej), zgodnie z art. 31 ust. 3 Konstytucji RP, mogłyby być wyłącznie akt prawny rangi ustawy.

Proponuję zatem doprecyzowanie przepisu, poprzez wskazanie, o jakiego rodzaju państwa chodzi w tym przypadku (inne państwa Unii Europejskiej czy też – szerzej – państwa należące do

Europejskiego Obszaru Gospodarczego, albowiem – o czym była mowa wyżej – możliwość przekazywania danych do państw trzecich wymagałaby umocowania w akcie prawnym rangi ustawy).

2) Zgodnie z § 5 ust. 4 projektu, do przetwarzania danych osobowych, stosuje się wysoki poziom bezpieczeństwa przetwarzania danych osobowych w systemie informatycznym, w rozumieniu przepisów o dokumentacji przetwarzania danych osobowych oraz warunków technicznych i organizacyjnych, jakim powinny odpowiadać urządzenia i systemy informatyczne służące do przetwarzania danych osobowych.

W pierwszej kolejności należy zaznaczyć, iż bardziej właściwe byłoby w tym przypadku odwołanie się do całej nazwy aktu prawnego (rozporządzenie 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). Adresaci normy nie mieliby wówczas wątpliwości co do tego, w jakim akcie prawnym znajdują się przepisy, jakie muszą w opisywanym przypadku być przez nich respektowane.

Następnie należy zwrócić uwagę, iż wysoki poziom bezpieczeństwa, określony w części C załącznika do powyższego rozporządzenia, odnosi się wyłącznie do zabezpieczenia danych osobowych przetwarzanych w systemach informatycznych. Trudno mówić o możliwości zastosowania przez administratora danych zabezpieczeń obejmujących m.in. kontrolę przepływu informacji pomiędzy systemem informatycznym administratora danych a siecią publiczną i kontrolę działań inicjowanych z sieci publicznej i systemu informatycznego administratora danych (Część C pkt XII.2. załącznika) w sytuacji, gdy przetwarza on dane osobowe w tzw. postaci manualnej, poza systemem informatycznym. Brzmienie projektowanego § 5 ust. 4 implikuje wniosek, iż do wszelkich form przetwarzania danych osobowych, przewidzianych w treści projektu (np. w stosunku do prowadzonej w formie „tradycyjnej” dokumentacji potencjalnego dawcy komórek krwiotwórczych – § 5 ust. 2 projektu) należy stosować te środki. Takie rozwiązanie nie jest natomiast możliwe z technicznego punktu widzenia.

Sugeruję więc stworzenie takiej regulacji, która – stanowiąc o konieczności stosowania wysokiego poziomu bezpieczeństwa przez określonego administratora danych nie tylko wtedy, gdy choćby jedno urządzenie systemu informatycznego, służącego do przetwarzania danych osobowych, połączone jest z siecią Internet (co jest wymagane przez § 6 ust. 4 przywołanego rozporządzenia), ale także w przypadku braku takiego połączenia – odnosić będzie poziom wysoki zabezpieczeń do przetwarzania danych w systemie informatycznym.

2 *pozwoleniem*
Komisaryczny Inspektor Ochrony Danych Osobowych
dr Andrzej Lewiński
[Podpis]
Andrzej Lewiński