



**GENERALNY INSPEKTOR
OCHRONY DANYCH
OSOBYWYCH**
Michał Serzycki

DOLIS - 033 - 381 / 09

Warszawa, dnia 2 listopada 2009 r.

Pan

Marek Twardowski

Podsekretarz Stanu

w Ministerstwie Zdrowia

ul. Miodowa 15

00 - 952 Warszawa

Szanowny Panie Ministrze

w nawiązaniu do pisma z dnia 21 października 2009 r. (znak: MZ-PZ-TSZ-401-5262-12/SP/09) uprzejmie informuję, iż w projekcie rozporządzenia Ministra Zdrowia w sprawie sposobu działania ośrodków kwalifikujących do przeszczepiania oraz sposobu kwalifikacji potencjalnego biorcy 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) § 3 ust. 2, stosownie do treści którego zawiadomienie, o którym mowa w ust. 1, jest przekazywane przesyłką poleconą lub drogą elektroniczną. W ust. 1 jest z kolei mowa o tym, że po przeprowadzonej konsultacji ośrodek zawiadamia zakład opieki zdrowotnej lub stację dializ, które zgłosiły potencjalnego biorcę, o zakwalifikowaniu albo niezakwalifikowaniu potencjalnego biorcy do przeszczepienia.

Wskazać w tym miejscu należy, że w § 2 ust. 4 i 5 projektu, odnoszącym się do dokumentacji leczenia potencjalnego biorcy oraz jej przesyłania, położono nacisk na konieczność zabezpieczenia tej dokumentacji przed, cyt.: „(...) ich utratą i dostępem osób nieuprawnionych (...)”. Podobny wymóg zawiera § 5 ust. 4 projektu, odnoszący się do przesyłania wniosku lekarza leczącego potencjalnego biorcę, czy danych wskazanych w § 7 ust. 1 projektu (§ 7 ust. 2).

W świetle powyższego, brak analogicznego zastrzeżenia w stosunku do przesyłania zawiadomienia, o którym jest mowa w § 3 ust. 2, implikuje jednoznaczny wniosek, że w tym przypadku nie jest konieczne stosowanie zabezpieczeń przywołanych w innych przepisach projektu.

Departament Polityki Zdrowotnej

ul. Stawki 2

2009-11-02 Warszawa

SEKRETARIAT
PODSEKRETARZA STANU
Marka Twardowskiego

02 LIS. 2009

tel (022) 860-70-81

fax (022) 860 70 90

www.pinda.gov.pl

Kak sroaw...
zakazano... 13360

Powstaje zatem konieczność doprecyzowania § 3 ust. 2 przedłożonego projektu tak, aby nie budziła wątpliwości kwestia konieczności przesyłania także tego zawiadomienia w sposób zapewniający właściwą ochronę zawartych w jego treści danych osobowych.

2) Zgodnie z § 8 projektu, do przetwarzania danych osobowych, o których mowa w § 2 ust. 1, § 4 ust. 1 i § 7 ust. 1, 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 właściwszym 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 § 8 implikuje wniosek, iż do wszelkich form przetwarzania danych osobowych, przewidzianych w treści projektu (np. w stosunku do prowadzonej w formie „tradycyjnej” dokumentacji leczenia potencjalnego biorcy – § 2 ust. 1, czy zgromadzonych w prowadzonej w takiej formie bazie danych informacji o kwalifikowanych potencjalnych biorcach – § 4 projektu) należy stosować te środki. Takie rozwiązanie nie jest natomiast możliwe z technicznego punktu widzenia.

Sugeruję zatem 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.

z powodzeniem
[Signature]