GENERALNY INSPEKTOR OCHRONY DANYCH OSOBOWYCH
Michał Serzycki

DOLiS – 033 – 433 / 09 /45897

Warszawa, dnia 10 grudnia 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 23 listopada 2009 r. (znak:MZ-PZ-TSZ-0212-5231-13/SW/09) uprzejmie informuję, iż w projekcie *rozporządzenia Ministra Zdrowia w sprawie tworzenia niepowtarzalnego oznakowania umożliwiającego identyfikację dawcy komórek, tkanek i narządów, sposobu oznaczania komórek, tkanek i narządów za pomocą tego oznakowania oraz wymagań w zakresie monitorowania komórek, tkanek i narządów* 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.) budzi jego § 9, stosownie do treści którego, do przetwarzania danych osobowych, stosuje się wysoki poziom bezpieczeństwa przetwarzania danych osobowych w systemie informatycznym w rozumieniu przepisów w sprawie 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 § 9 implikuje wniosek, iż do wszelkich form przetwarzania danych osobowych, przewidzianych w treści 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 wyłącznie w systemie informatycznym. Powyższe możliwe byłoby natomiast poprzez rozpoczęcie § 9 projektu od sformułowania, „Do przetwarzania danych osobowych w formie elektronicznej stosuje się wysoki poziom bezpieczeństwa (...)".

Analogiczną, jak powyżej wskazaną, uwagę należy podnieść w stosunku do § 2 ust. 8 projektu *rozporządzenia w sprawie szczegółowych warunków wywozu ludzkich komórek, tkanek i narządów z terytorium Rzeczypospolitej Polskiej i przywozu tych komórek, tkanek i narządów na to terytorium oraz monitorowania stanu wywiezionych i przywiezionych ludzkich komórek, tkanek i narządów w drodze między dawcą a biorcą.*

Ponadto podważenia wymaga przewidziana w § 2 ust. 4 projektu forma dokonywania zgłoszeń istotnych zdarzeń niepożądanych w czasie wywozu lub przywozu narządów za pomocą listu poleconego. Wzgląd na bezpieczeństwo danych osobowych (obowiązek właściwego zabezpieczenia przez administratora danych przetwarzanych przez niego danych osobowych wynika z art. 36 ustawy o ochronie danych osobowych) przemawia raczej za unikaniem tej formy dostarczania korespondencji. Prawdopodobnym jest bowiem jej utrata, a w konsekwencji powyższego dostęp osób nieupoważnionych do danych osobowych zawartych w treści korespondencji – w tym przypadku także danych szczególnie chronionych w rozumieniu art. 27 ust. 1 ustawy o ochronie danych osobowych.

Niezależnie od powyższego wskazuję, iż zasługującym na aprobatę jest wprowadzenie do przepisów projektowanych rozporządzeń uregulowań odnoszących się do kwestii zabezpieczenia danych osobowych przetwarzanych w postaci tradycyjnej w zakresie bardziej restrykcyjnym, niż wynika to z przepisów o ochronie danych osobowych. Powyższe musi jednak w odpowiedni sposób zostać sformułowane w treści przedłożonych projektów.

z poważaniem

Generalny Inspektor Ochrony Danych Osobowych
z up. Zastępca Generalnego Inspektora Ochrony Danych Osobowych

Andrzej [illegible]