GENERALNY INSPEKTOR
OCHRONY DANYCH
OSOBOWYCH

dr Edyta Bielak-Jomaa

DOLiS- 033-18/16

Warszawa, dnia 4 lutego 2016 r.

Pani

Katarzyna Głowala

Podsekretarz Stanu w Ministerstwie Zdrowia

ul. Miodowa 15

00 – 952 Warszawa

w nawiązaniu do przesłanej drogą elektroniczną w dniu 3 lutego 2016 r. nowej propozycji sformułowania przepisów ustawy o zmianie ustawy o publicznej służbie krwi, Generalny Inspektor Ochrony Danych Osobowych przedstawia następujące zastrzeżenia:

1) W proponowanym art. 17 ust. 11 wskazano, iż wymiana danych między systemem e-krew a podmiotami leczniczymi oraz Systemem Monitorowania Zagrożeń odbywa się drogą elektroniczną. W tym kontekście podkreślenia wymaga, iż każde przetwarzanie danych osobowych powinno być planowane z uwzględnieniem koncepcji ochrony prywatności w fazie projektowania (*privacy by design*). Idea *privacy by design* zrodziła się jako sposób spojrzenia na budowanie systemów teleinformatycznych. Polega ona na tym, by od samego początku tworzenia jakiegoś systemu, na każdym etapie, rozważać wpływ tworzonych rozwiązań na sferę prywatności i nie tyle odpowiadać na pojawiające problemy, co już wcześniej przewidywać najważniejsze z nich i im przeciwdziałać. Zasada ochrony prywatności w fazie projektowania została zawarta również w przepisach nowego rozporządzenia Parlamentu Europejskiego i Rady w sprawie ochrony osób fizycznych w zakresie przetwarzania danych osobowych. Dlatego rozważyć należy, czy uregulowanie w taki sposób kwestii wymiany danych jest wystarczające z punktu widzenia ochrony prywatności.

Jednocześnie ze względu na powyższe, jak i informacje przekazane na spotkaniu roboczym w dniu 3 lutego 2016 r., projektodawca powinien wziąć pod uwagę, iż przesyłanie danych osobowych, w tym z kategorii tzw. danych szczególnie chronionych za pośrednictwem sieci Internet pociąga za sobą wiele, nie tylko potencjalnych zagrożeń dla bezpieczeństwa przetwarzanych danych. Należy zatem mieć to na uwadze, zwłaszcza przy projektowaniu przepisów wykonawczych.

2) Niecelowe jest przypisanie (zgodnie z projektowanym art. 17 ust. 15) odpowiedzialności za prawidłowość danych gromadzonych w systemie e-krew jednostkom, o których mowa w art. 4 ust. 3, bowiem odpowiedzialność ta i tak spoczywać będzie na ministrze właściwym do spraw zdrowia, jako administratorze danych osobowych. Minister nie może zrzec się tej odpowiedzialności (co wynika wprost z art. 26 ust. 1 pkt 3 ustawy o ochronie danych osobowych, zgodnie z którym administrator danych powinien zapewnić, aby przetwarzane przez niego dane były merytorycznie poprawne) na rzecz podmiotów, których działalność w systemie e-krew ogranicza się do wprowadzenia danych osobowych przez upoważnionych pracowników jednostki. W przypadku zaistnienia jakichkolwiek nieprawidłowości dotyczących danych przetwarzanych w systemie e-krew, odpowiedzialność spoczywać będzie na ministrze właściwym do spraw zdrowia, niezależnie od tego, że dane do systemu wprowadziła inna jednostka.

   W tym kontekście trzeba zwrócić uwagę na art. 32 ust. 1 ustawy o ochronie danych osobowych, zgodnie z którym każda osoba ma prawo do kontroli przetwarzania danych, które jej dotyczą, zawartych w zbiorach danych, w tym m.in. prawo do żądania uzupełnienia, uaktualnienia, sprostowania danych osobowych, czasowego lub stałego wstrzymania ich przetwarzania lub ich usunięcia, jeżeli są one niekompletne, nieaktualne, nieprawdziwe lub zostały zebrane z naruszeniem ustawy albo są już zbędne do realizacji celu, dla którego zostały zebrane (pkt 6). W przypadku takiego zorganizowania systemu e-krew to na ministrze właściwym do spraw zdrowia, jako administratorze danych osobowych, spoczywa obowiązek zapewnienia osobom, których dane dotyczą, realizacji ich praw. Jednostki, które zgodnie z projektowanym art. 17 ust. 15 miałyby odpowiadać za prawidłowość danych gromadzonych w systemie, same danymi osobowymi nie dysponują, a zatem nie mają możliwości weryfikacji czy dane osoby występującej z określonym żądaniem są niekompletne, nieaktualne, nieprawdziwe lub zostały zebrane z naruszeniem ustawy albo są już zbędne do realizacji celu, dla którego zostały zebrane. Komentowany przepis staje się zatem zbędny, gdyż wprowadzałby do ustawy niezrozumiałą i sprzeczną z przepisami ustawy o ochronie danych osobowych konstrukcję.

3) Ponadto, zwrócić uwagę należy na projektowany art. 17 ust. 18, zawierający delegację do wydania rozporządzenia wykonawczego. Przepis ten posługuje się pojęciem „danych

prawnie chronionych objętych wpisem do systemu e-krew", które nie jest zdefiniowane w jakichkolwiek przepisach. Pojęcie takie szczególnie nie powinno być wprowadzane na poziomie przepisów rozporządzenia, w związku z czym wskazane byłoby poprzestanie na sformułowaniu „danych objętych wpisem do systemu e-krew". Wyjaśnienia ponadto wymaga, czy według koncepcji projektodawcy dane z systemu e-krew miałyby być przekazywane również do innych systemów, poza Systemem Monitorowania Zagrożeń. Jeżeli tak, to systemy te muszą być wyraźnie wskazane na poziomie przepisów ustawy, jeśli nie – w delegacji do wydania rozporządzenia powinien być wskazany wyłącznie System Monitorowania Zagrożeń, tak, aby wykluczyć możliwość rozszerzania wymiany o kolejne systemy za pomocą przepisów wykonawczych, co w świetle obowiązujących przepisów byłoby niedopuszczalne, jak wykraczające poza regulację ustawową. Ponadto, w projektowanym art. 17 ust. 18, w związku z zaliczeniem urządzeń w punktach poboru (nazywanych we wcześniejszej wersji projektu modułem lokalnym) do systemu e-krew należy w delegacji ustawowej wprowadzić zapis zobowiązujący również do opracowania sposobu przekazywania w punktach poboru krwi (jednostkach organizacyjnych publicznej służby krwi) informacji z urządzeń specjalistycznych służących do poboru i analizy krwi do systemu e-krew.

4) Podkreślenia również wymaga, iż na ministrze właściwym do spraw zdrowia, jako administratorze danych osobowych zgromadzonych w systemie e-krew, spoczywać będą wszelkie obowiązki wynikające z przepisów ustawy o ochronie danych osobowych, w tym obowiązek zastosowania odpowiednich środków organizacyjnych i technicznych zapewniających ochronę przetwarzanych danych (art. 36 ust. 1 ustawy o ochronie danych osobowych). Ponadto, należy nadmienić, iż o tym, kto w konkretnym przypadku jest administratorem danych, rozstrzygać powinno nie wskazanie tego podmiotu w przepisie ustawy, a decydowanie o celach i środkach przetwarzania danych osobowych, które to cele i środki muszą w sposób jednoznaczny wynikać z przepisów regulujących dane zagadnienie.