GENERALNY INSPEKTOR OCHRONY DANYCH OSOBOWYCH

dr Edyta Bielak-Jomaa

Warszawa, dnia 9 listopada 2016 r.

DOLiS-033-378/16/BG

Pan

Piotr Warczyński

Podsekretarz Stanu w Ministerstwie Zdrowia

ul. Miodowa 15

00-952 Warszawa

w odpowiedzi na pismo z dnia 3 listopada 2016 r. (znak: FZP.073.14.2016.RM, IK: 748470), dotyczące **projektu ustawy o zmianie ustawy o systemie informacji w ochronie zdrowia oraz niektórych innych ustaw w wersji z dnia 3 listopada 2016 r.**, Generalny Inspektor Ochrony Danych Osobowych na wstępie zauważa, iż przedstawiony do zaopiniowania dokument znacząco wykracza poza pierwotnie zaproponowaną nowelizację. Zdziwienie budzi fakt, iż zmiany o tak fundamentalnym charakterze proponowane są dopiero na etapie konferencji uzgodnieniowej, co znacząco ogranicza możliwość dokonania przez projektodawcę rzetelnej oceny skutków tych rozwiązań dla ochrony danych osobowych (tzw. *privacy impact assessment*) oraz kompleksowej ich analizy przez pozostałych uczestników procesu legislacyjnego.

Do przedstawionego projektu Generalny Inspektor Ochrony Danych Osobowych – z punktu widzenia przepisów ustawy z dnia 29 sierpnia 1997 r. o ochronie danych osobowych (Dz. U. z 2016 r. poz. 922) – zgłasza następujące uwagi.

I. Utworzenie rejestru medycznego, o którym mowa w art. 19 ust. 1 ustawy o systemie informacji w ochronie zdrowia, następuje w drodze rozporządzenia, które określa zamknięty katalog danych osobowych, jakie mogą być w tym rejestrze przetwarzane. Konsekwencją możliwości wymiany danych osobowych między rejestrami (zaproponowanej w projektowanym art. 19 ust. 8a) może być stan, w którym do poszczególnych rejestrów będą

ul. Stawki 2
00-193 Warszawa

tel. (22) 531 03 00
fax. (22) 531 03 01

trafiać dane w zakresie szerszym, niż zezwalają na to przepisy wykonawcze, co byłoby sprzeczne z zasadą legalizmu, wyrażoną w art. 26 ust. 1 pkt 1 ustawy o ochronie danych osobowych. Pamiętać należy, iż administrator powinien przetwarzać tylko takiego rodzaju dane i tylko o takiej treści, które są niezbędne ze względu na cel zbierania danych. Dane osobowe nie mogą być zbierane na zapas, „na wszelki wypadek", tj. bez wykazania celowości ich pozyskania i niezbędności dla realizacji zadań administratora danych (zasada adekwatności – art. 26 ust. 1 pkt 3 ustawy o ochronie danych osobowych). Administrator powinien również zapewnić, aby dane osobowe były zbierane dla oznaczonych, zgodnych z prawem celów i nie poddawane dalszemu przetwarzaniu niezgodnemu z tymi celami (zasada celowości – art. 26 ust. 1 pkt 2 ustawy o ochronie danych osobowych). Mimo iż ogólne cele tworzenia rejestrów medycznych – wskazane w art. 19 ust. 1 ustawy o systemie informacji w ochronie zdrowia – są wspólne, należy zauważyć, że każdy z rejestrów dedykowany jest określonej kwestii, zatem szczegółowe cele ich prowadzenia są odmienne, ograniczone zakresem przetwarzanych danych. Wymiana danych między rejestrami medycznymi mogłaby skutkować naruszeniem wyżej wspomnianej zasady celowości, jako że w efekcie dochodziłoby do zmiany pierwotnego celu przetwarzania danych. Podkreślenia również wymaga, iż przekazanie danych osobowych innemu podmiotowi wiąże się z koniecznością spełnienia obowiązku informacyjnego wobec osoby, której dane dotyczą (art. 25 ustawy o ochronie danych osobowych). Wymóg uprzedniego informowania o przekazaniu danych osobowych podkreślony został w wyroku Trybunału Sprawiedliwości Unii Europejskiej z 1 października 2015 r. w sprawie C-201/14 Smaranda Bara i in. przeciwko Presedintele Casei Nationale de Asigurări de Sănătate i in.

Dodatkowo, projektowany przepis nie precyzuje w jakim trybie miałaby się odbywać wymiana danych osobowych między rejestrami medycznymi, a mianowicie czy intencją projektodawcy było umożliwienie wymiany *online*, czy raczej udostępnianie danych w trybie wnioskowym. Nie są również określone częstotliwość i zakres dokonywania takiej wymiany. Rozumiejąc, iż pozyskiwanie danych z innych rejestrów może być w pewnych sytuacjach uzasadnione, Generalny Inspektor wskazuje, iż nie może być to dostęp o charakterze stałym, a ograniczony wyłącznie do możliwości pozyskiwania danych w indywidualnych przypadkach i w określonym w przepisach celu.

Zauważyć ponadto wypada, iż konstrukcja zaproponowana w projektowanym art. 19 ust. 8a ustawy o systemie informacji w ochronie zdrowia zdaje się przeczyć pierwotnym założeniem ustawodawcy w odniesieniu do tworzenia i prowadzenia rejestrów medycznych – jako że wymiana danych w oparciu o tak ogólnie sformułowany przepis mogłaby w efekcie doprowadzić do ujednolicenia zawartości poszczególnych rejestrów, co podważa sens ich funkcjonowania.

II. Wątpliwości Generalnego Inspektora Ochrony Danych Osobowych wzbudza także rozwiązanie przewidziane w projektowanym art. 19 ust. 10a ustawy o systemie informacji w ochronie zdrowia. Przede wszystkim, wydaje się, iż dla sformułowanych w tym przepisie celów *monitorowania zapotrzebowania na świadczenia opieki zdrowotnej, monitorowania jakości i efektywności kosztowej badań lub procedur medycznych oraz prowadzenia profilaktyki zdrowotnej* zbędne jest dysponowanie przez Narodowy Fundusz Zdrowia danymi osobowymi o charakterze jednostkowym. Konieczne jest zatem dokonanie oceny, czy wprowadzenie rozwiązania, o którym mowa w projektowanym art. 19 ust. 10a, jest rzeczywiście niezbędne i należycie uzasadnione i czy dla realizacji określonych w tym przepisie celów nie byłoby wystarczające pozyskiwanie danych pozbawionych charakteru zindywidualizowanego – podobnie jak ma się to odbywać w przypadku przekazywania danych z rejestrów medycznych ministrowi właściwemu do spraw zdrowia (projektowany art. 19 ust. 10). Zastanowić się również należy, czy skutkiem przyjęcia w obecnym kształcie projektowanego przepisu art. 19 ust. 10a nie byłoby umożliwienie profilowania osób, których dane dotyczą. Podkreślenia w tym kontekście wymaga, iż zgodnie z art. 22 Rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (ogólne rozporządzenie o ochronie danych) – które będzie bezpośrednio stosowane w Polsce od dnia 25 maja 2018 r. – dopuszczalność profilowania podlegać będzie ścisłym ograniczeniom, zwłaszcza, gdy jego podstawą miałyby być między innymi dane szczególnie chronione.

Odnosząc się zaś do proponowanych zmian w przepisach ustawy o świadczeniach opieki zdrowotnej finansowanych ze środków publicznych, stwierdzić należy, iż wymagają one dalszego doprecyzowania. Dodanie nowego art. 188e, zgodnie z którym prezes Narodowego Funduszu Zdrowia jest obowiązany do prowadzenia i utrzymywania elektronicznego systemu monitorowania programów zdrowotnych (ust. 1) sugeruje, iż zostanie stworzony nowy rejestr danych osobowych (zgodnie z definicją zawartą w art. 7 pkt 1 ustawy o ochronie danych osobowych). Tymczasem nie jest jasne, jaki miałby być sposób zasilania takiego rejestru – a tym samym z jakich źródeł, w jakiej formie oraz w jakim trybie Fundusz pozyskiwałby dane niezbędne dla realizacji określonych w przepisach celów. Przy czym – podobnie jak wskazano wyżej w odniesieniu do projektowanego art. 19 ust. 10a ustawy o systemie informacji w ochronie zdrowia – ogólnie określony cel monitorowania programów zdrowotnych nie przesądza, iż dla jego realizacji konieczne jest przetwarzanie danych o zindywidualizowanym charakterze. Jeżeli intencją projektodawcy było np. stworzenie

podstaw prawnych dla wysyłki imiennych zaproszeń na badania przesiewowe, to taki cel przetwarzania danych powinien zostać w sposób wyraźny wyartykułowany w projektowanych przepisach. W tym kontekście należy przypomnieć wystąpienie Generalnego Inspektora Ochrony Danych Osobowych z dnia 19 sierpnia 2016 r.[1], w którym zwrócił się do Ministra Zdrowia z prośbą o rozważenie przeprowadzenia prac legislacyjnych mających na celu uregulowanie kwestii przetwarzania danych o stanie zdrowia w związku z prowadzeniem profilaktyki zdrowotnej lub realizacją programów zdrowotnych albo programów polityki zdrowotnej, w tym stworzenie właściwych podstaw prawnych funkcjonowania Systemu Informatycznego Monitorowania Profilaktyki (SIMP). Generalny Inspektor podkreślił m.in., iż *tylko stworzenie odpowiednich ustawowych podstaw funkcjonowania SIMP – w postaci unormowań dotyczących katalogu danych przetwarzanych w SIMP, sposobu i źródeł zasilania SIMP, katalogu (albo kręgu) podmiotów mających uprawnienie do dostępu do SIMP, katalogu (albo kręgu) podmiotów, którym udostępniane są informacje (dane) zgromadzone w SIMP oraz zasad tego udostępniania, okresu przechowywania danych w SIMP – pomoże uniknąć wątpliwości jakie obecnie ujawniają się w praktyce, a związanych z możliwością udostępniania danych zgromadzonych w SIMP innym podmiotom, czy prowadzeniem wysyłki imiennych zaproszeń na badania profilaktyczne*. Rozwiązania przewidziane w opiniowanym projekcie nie spełniają w sposób wystarczający wyrażonych w wystąpieniu postulatów, co – w razie przyjęcia przepisów w zaproponowany kształcie – skutkować będzie w praktyce dalszymi wątpliwościami interpretacyjnymi.

III. Z uwagi na konieczność ochrony praw osób, których dane dotyczą oraz zagwarantowania wysokiego poziomu bezpieczeństwa danych szczególnie chronionych, Generalny Inspektor Ochrony Danych Osobowych opowiada się za utrzymaniem zakazu dalszego powierzania przetwarzania danych zawartych w rejestrach medycznych (tzw. podpowierzania), sformułowanego obecnie w art. 20 ust. 8 ustawy o systemie informacji w ochronie zdrowia. Przepisy ustawy o ochronie danych osobowych nie regulują bezpośrednio konstrukcji tzw. podpowierzania przetwarzania danych, jednak przyjąć należy, iż jego dopuszczalność jest uzależniona od spełnienia określonych warunków. Generalny Inspektor stoi na stanowisku, iż dalsze powierzenie przetwarzania danych osobowych jest możliwe pod warunkiem, że będzie następowało na podstawie autonomicznej decyzji administratora danych, a nie podmiotu przetwarzającego oraz właściwego umocowania takiego działania w pierwotnej umowie powierzenia, a kwestie te powinny znaleźć właściwe odzwierciedlenie w przepisach

[1] sygnatura DOLiS-035-924/16, http://www.giodo.gov.pl/1520260/id_art/9643/j/pl/

powszechnie obowiązującego prawa. Kolejne umowy nie mogą prowadzić do osłabienia statusu administratora danych, który nie może być pozbawiony realnej możliwości decydowania o celach i środkach przetwarzania danych, w tym kontroli nad procesem przetwarzania danych osobowych. Powierzenie przetwarzania danych przez administratora nie prowadzi bowiem do zmiany jego statusu – niezależnie od faktu zawarcia umowy powierzenia, to administrator danych pozostaje podmiotem decydującym o celach i środkach ich przetwarzania. Nie jest dopuszczalne przyjęcie zaproponowanej przez projektodawcę konstrukcji, zgodnie z którą dla podpowierzenia przetwarzania danych wystarczające byłoby jedynie uzyskanie pisemnego upoważnienia administratora danych, gdyż takie rozwiązanie w praktyce pozbawiłoby administratora realnego wpływu na organizację procesu przetwarzania danych.

Dalsze powierzanie przetwarzania danych zawartych w rejestrach medycznych *innym podmiotom wyspecjalizowanym w utrzymywaniu infrastruktury techniczno-systemowej i zapewnianiu obsługi technicznej systemów teleinformatycznych* (*vide* projektowany art. 20 ust. 5a) nie może również prowadzić do osłabienia poziomu bezpieczeństwa tych danych, które – jako tzw. dane wrażliwe – podlegają szczególnemu reżimowi ochrony zgodnie z art. 27 ustawy o ochronie danych osobowych. Tymczasem, projektodawca nakłada wyłącznie na podmioty, o których mowa w projektowanym art. 20 ust. 5 szereg obowiązków, takich jak: obowiązek stworzenia warunków organizacyjnych i technicznych zapewniających ochronę przetwarzanych danych przed nieuprawnionym dostępem, nielegalnym ujawnieniem lub pozyskaniem, a także ich modyfikacją, uszkodzeniem, zniszczeniem lub utratą (ust. 6), obowiązek przekazania danych administratorowi w przypadku zaprzestania przetwarzania danych w rejestrze medycznym (ust. 9), obowiązek zachowania w tajemnicy informacji związanych z usługobiorcami uzyskanych w związku z tym powierzeniem (ust. 10). Nie jest zrozumiałe, dlaczego wskazane obowiązki miałyby nie spoczywać również na podmiotach, którym „podpowierzono" przetwarzanie danych. W razie przyjęcia zaproponowanej konstrukcji, przetwarzanie danych osobowych odbywałoby się poza wszelką kontrolą administratora danych, co z całą pewnością nie może zostać uznane za stan prawidłowy. Rozwiązanie to budzi kategoryczny sprzeciw Generalnego Inspektora, jako stwarzające ogromne ryzyko dla ochrony praw jednostek i bezpieczeństwa danych szczególnie chronionych.

IV. W opinii Generalnego Inspektora nie jest jasne *ratio legis* propozycji odstąpienia od realizacji obowiązku informacyjnego wobec osób, których dane osobowe są przetwarzane w rejestrach medycznych (uchylenie art. 19 ust. 8 ustawy o systemie informacji ochronie zdrowia zostało zaproponowane w piśmie przewodnim, lecz nie przewidziano go w

załączonym projekcie). Przepis art. 19 ust. 8 w obecnym kształcie wszedł w życie z dniem 1 stycznia 2012 r., a przeniesienie usytuowania administratora danych z poziomu ministra właściwego do spraw zdrowia na poziom podmiotu prowadzącego rejestr nie powinno mieć wpływu na zmianę obowiązującego stanu prawnego – zwłaszcza, iż obowiązek ten od początku spoczywał na podmiocie prowadzącym rejestr, a nie na administratorze danych. Przypomnieć należy, iż Generalny Inspektor Ochrony Danych Osobowych sprzeciwiał się koncepcji tworzenia rejestrów medycznych na podstawie rozporządzeń, a wprowadzenie obowiązku informacyjnego wobec osób, których dane dotyczą i są przetwarzane w rejestrach, stanowić miało dodatkową gwarancję ochrony ich praw. Odejście od obowiązującej zasady w konsekwencji doprowadzi do osłabienia tej ochrony w stosunku do osób, których dane – w tym szczególnie chronione - zaczną być przetwarzane w rejestrach po ewentualnym wejściu w życie nowych regulacji. Taki stan rzeczy nie może spotkać się z akceptacją ze strony organu do spraw ochrony danych osobowych.