GENERALNY INSPEKTOR OCHRONY DANYCH OSOBOWYCH

dr Wojciech R. Wiewiórowski

Warszawa, dnia 22 października 2013 r.

Pan
dr Adam Bodnar
Wiceprezes Zarządu
Helsińska Fundacja Praw Człowieka

Pan
Maciej Nowicki
Sekretarz Zarządu
Helsińska Fundacja Praw Człowieka

W związku z przekazanym w dniu 15 października 2013 r. wnioskiem o udostępnienie informacji publicznej (sygn. 4359/MPL/BG) – data wpływu do Biura Generalnego Inspektora Ochrony Danych Osobowych: 17 października 2013 r. – przekazuję odpowiedź ze strony Generalnego Inspektora Ochrony Danych Osobowych na zadane pytania.

Pytanie nr 1.

Generalnemu Inspektorowi Ochrony Danych Osobowych nie są znane podstawy prawne do działania amerykańskiej Agencji Bezpieczeństwa Narodowego (NSA) na terytorium Polski.

Pytanie nr 2.

Generalny Inspektor Ochrony Danych Osobowych nie zlecał analiz prawnych na temat zgodności programu PRISM z polskim porządkiem prawnym. Tematyka ta była jednak jednym z tematów omawianym w stanowisku Generalnego Inspektora Ochrony Danych Osobowych w sprawie oceny wdrożenia decyzji Komisji Europejskiej nr 2000/520/WE, które GIODO przygotował w odpowiedzi na pismo Ministra Administracji i Cyfryzacji z dnia 2 sierpnia 2013 r. i które przesłał do Ministra Administracji i Cyfryzacji w dniu 14 października 2013 r. Kopię wyżej wzmiankowanego dokumentu załączam do niniejszego pisma.

Generalny Inspektor Ochrony Danych Osobowych zwraca uwagę, że pytanie znajdujące się we wniosku różni się od pytania opublikowanego w dokumencie pt. „*100 pytań o inwigilację do władz polskich*". Pytanie nr 31 w wyżej wymienionym dokumencie sugeruje, że Generalny Inspektor Ochrony Danych Osobowych mógłby być zleceniobiorcą wobec Prezesa Rady Ministrów w sprawie takiej analizy. Generalny Inspektor Ochrony Danych Osobowych pragnie wyjaśnić, że Prezes Rady Ministrów nie ma możliwości zlecania prac GIODO. Nigdy też nie podejmował żadnych działań, które sugerowałyby, że ma zamiar takie „zlecenia" wydawać. Byłoby to oczywistym naruszeniem zasady niezależności Generalnego Inspektora Ochrony Danych Osobowych.

Pytanie nr 3.

Z posiadanych przez Generalnego Inspektora Ochrony Danych Osobowych informacji nie wynika, by istniała podstawa prawna umożliwiająca bezpośrednie przekazywanie przez Agencję Bezpieczeństwa Wewnętrznego i inne służby danych telekomunikacyjnych polskich obywateli amerykańskiej Agencji Bezpieczeństwa Narodowego (NSA). GIODO zwraca jednak uwagę, że na mocy art. 43 ust. 2 w związku z art. 43 ust. 1 i 1a ustawy o ochronie danych osobowych uprawnienia Generalnego Inspektora do kontroli działań Agencji Bezpieczeństwa Wewnętrznego w wyżej wskazanym zakresie są znacząco ograniczone.

Wydaje się, że w konkretnych sprawach przekazanie informacji mogłoby nastąpić jedynie w ramach pomoc prawnej w trybie określonym Umową między Rzecząpospolitą Polską a Stanami Zjednoczonymi Ameryki dotyczącą stosowania Umowy między Rzecząpospolitą Polską a Stanami Zjednoczonymi Ameryki o wzajemnej pomocy prawnej w sprawach karnych, sporządzonej dnia 10 lipca 1996 r. , zgodnie z artykułem 3 ustęp 2 Porozumienia o wzajemnej pomocy prawnej w sprawach karnych między Unią Europejską a Stanami Zjednoczonymi Ameryki, podpisanego w Waszyngtonie dnia 25 czerwca 2003 r. (Dz. U. z 2010, nr 17, poz. 91). Jednakże należy pamiętać, że zgodnie z jej art. 2 ust. 1 przekazywanie i przyjmowanie wniosków o pomoc prawną odbywa się za pośrednictwem organu centralnego, którym zgodnie z ust. 2 jest Minister Sprawiedliwości lub wyznaczona przez niego osoba.

Pytanie nr 4.

Generalny Inspektor Ochrony Danych Osobowych nie uzyskał żadnych informacji o przekazywaniu amerykańskiej Agencji Bezpieczeństwa Narodowego (NSA) danych telekomunikacyjnych przez działających na polskim rynku operatorów telekomunikacyjnych.

Pytanie nr 5.

Generalny Inspektor Ochrony Danych Osobowych uczestniczy w koordynowanych przez Grupę roboczą ds. ochrony osób fizycznych w zakresie przetwarzania danych osobowych (Grupę Artykułu Art. 29) działaniach dotyczących wyjaśnienia sposobu działania programu PRISM oraz jego wpływu na ochronę danych osobowych na obszarze Unii Europejskiej. Częścią tego zagadnienia jest ewentualne udostępnianie danych o użytkownikach „przez takie firmy jak Google" organom publicznym w Stanach Zjednoczonych. W ramach prac Grupy Art. 29 w dniach 16-17 września 2013 r. odbyło się posiedzenie podgrupy *Borders, Travel and Law Enforcement* (BTLE) poświęcone temu zagadnieniu. W koordynacji z rzecznikami ochrony danych osobowych - w tym z GIODO - przewodniczący Grupy Art. 29 Pan Jacob Kohnstamm skierował również w dniu 13 sierpnia 2013 r. list poświęcony zagadnieniom PRISM (kopia w załączeniu) do Pani Wice Przewodniczącej Komisji Europejskiej Viviane Reding. Temat PRISM - m.in. na wniosek Generalnego Inspektora Ochrony Danych Osobowych - znalazł się również w programie 35. Międzynarodowej Konferencji

Rzeczników Ochrony Danych i Prywatności, która odbyła się w Warszawie w dniach 23-26 września 2013 r. W trakcie zamkniętej sesji tejże konferencji odbyło się spotkanie rzeczników ochrony danych osobowych z Panem Davidem Medine, Przewodniczący Rady ds. nadzoru nad przestrzeganiem ochrony prywatności i praw obywatelskich (USA) poświęcone praktyce działania programu PRISM. Zaś w części otwartej konferencji zorganizowano sesję pt. „Dostęp organów publicznych do danych sektora prywatnego" moderowaną przez Panią Prezes Katarzynę Szymielewicz z Fundacji Panoptykon z udziałem: prof. Joela Reidenberga (Uniwersytet Princeton i Uniwersytet Fordham, USA), Davida Medine, Iana Readheada (dyrektora Stowarzyszenia Komendantów Policji Zjednoczonego Królestwa) i Caspara Bowdena (niezależnego adwokata ochrony prywatności).

Generalny Inspektor Ochrony Danych Osobowych nie uważa by jakiekolwiek podjęte w tym zakresie przezeń działania naruszyły polskie prawo.

Pytanie nr 8.

Generalny Inspektor Ochrony Danych Osobowych nie podejmował żadnych działań związanych bezpośrednio z programem Tempora. Nie wystąpił również z zapytaniami do przedstawicieli administracji czy służb brytyjskich czy i na jakiej podstawie te działania mają miejsce.

Jednocześnie GIODO zwraca uwagę, że jedną z głównych zasad ochrony praw podstawowych w Unii Europejskiej jest niedokonywanie podziału na podstawie kryterium obywatelstwa. Podstawowym kryterium jakim kierować się powinien Generalny Inspektor Ochrony Danych Osobowych przy ustalaniu swojej właściwości jest kryterium terytorialne określone w art. 3 ust. 2 ustawy o ochronie danych osobowych. W tej sytuacji istotą oceny Generalnego Inspektora jest miejsce przetwarzania danych bądź ich ewentualny transfer do państw trzecich, nie zaś kryterium obywatelstwa osób, których dane dotyczą.

Z związku z tym, że pytania nr 6 i 7 nie stanowią pytań o informację publiczną w rozumieniu ustawy o dostępie do informacji zgodnie z ustalonym orzecznictwem sądów administracyjnych (wyroki NSA z 7 marca 2012, I OSK 2445/11; NSA z dnia 30 sierpnia 2012 r., I OSK 665/12; WSA w Warszawie z 28 sierpnia 2013 r., II SAB/Wa 198/13) Generalny Inspektor przekazuje więc odpowiedź w trybie art. 12 pkt 5 ustawy o ochronie danych osobowych (Dz.U. 2002 nr 101 poz. 926 z późn. zm.) oraz art. 9 i 11 kodeksu postępowania administracyjnego (Dz.U. 2013 poz. 267 j.t.).

Pytanie nr 6.

Dla Generalnego Inspektora Ochrony Danych Osobowych nie jest do końca jasne, jaki był zamiar pytającego przy formułowaniu pytania nr 6. Odpowiedź na problem „warunków", na jakich Google i Facebook udostępniają dane dotyczące polskich użytkowników usług musi być wielowarstwowa i przede wszystkim jest związana z tym jak rozumiane jest pojęcie udostępnienia.

Ustawa o ochronie danych osobowych nie definiuje pojęcia "udostępnianie", jednak uznaje je za jedną z form przetwarzania danych osobowych (art. 7 pkt 2). Zgodnie z ustaloną opinią doktryny należy to pojęcie traktować szeroko jako okazanie treści danych osobowych podmiotowi innemu niż administrator danych. Przy takim rozumieniu udostępniania wyróżnia się udostępnienie:

a) na wniosek innego podmiotu,

b) z własnej inicjatywy administratora udostępniającego dane.

Oba podmioty, które wymienione zostały w pytaniu prowadzą całą gamę usług internetowych, które tylko w przypadku Facebooka zgrupowane są wokół serwisu społecznościowego, podczas gdy w przypadku Google mają charakter odrębnych, choć powiązanych ze sobą serwisów. Oba podmioty, tym samym, „udostępniają dane" tak z własnej inicjatywy jak i na wniosek innych podmiotów.

Podstawowym problemem, z którym spotykamy się w przypadku usług świadczonych przez wymienione przez Państwa podmioty jest to kto jest administratorem danych osobowych używanych w danym serwisie. Z treści pytania wynika, że interesuje Państwa

Z związku z tym, że pytania nr 6 i 7 nie stanowią pytań o informację publiczną w rozumieniu ustawy o dostępie do informacji zgodnie z ustalonym orzecznictwem sądów administracyjnych (wyroki NSA z 7 marca 2012, I OSK 2445/11; NSA z dnia 30 sierpnia 2012 r., I OSK 665/12; WSA w Warszawie z 28 sierpnia 2013 r., II SAB/Wa 198/13) Generalny Inspektor przekazuje więc odpowiedź w trybie art. 12 pkt 5 ustawy o ochronie danych osobowych (Dz.U. 2002 nr 101 poz. 926 z późn. zm.) oraz art. 9 i 11 kodeksu postępowania administracyjnego (Dz.U. 2013 poz. 267 j.t.).

Pytanie nr 6.

Dla Generalnego Inspektora Ochrony Danych Osobowych nie jest do końca jasne, jaki był zamiar pytającego przy formułowaniu pytania nr 6. Odpowiedź na problem „warunków", na jakich Google i Facebook udostępniają dane dotyczące polskich użytkowników usług musi być wielowarstwowa i przede wszystkim jest związana z tym jak rozumiane jest pojęcie udostępnienia.

Ustawa o ochronie danych osobowych nie definiuje pojęcia "udostępnianie", jednak uznaje je za jedną z form przetwarzania danych osobowych (art. 7 pkt 2). Zgodnie z ustaloną opinią doktryny należy to pojęcie traktować szeroko jako okazanie treści danych osobowych podmiotowi innemu niż administrator danych. Przy takim rozumieniu udostępniania wyróżnia się udostępnienie:

a) na wniosek innego podmiotu,

b) z własnej inicjatywy administratora udostępniającego dane.

Oba podmioty, które wymienione zostały w pytaniu prowadzą całą gamę usług internetowych, które tylko w przypadku Facebooka zgrupowane są wokół serwisu społecznościowego, podczas gdy w przypadku Google mają charakter odrębnych, choć powiązanych ze sobą serwisów. Oba podmioty, tym samym, „udostępniają dane" tak z własnej inicjatywy jak i na wniosek innych podmiotów.

Podstawowym problemem, z którym spotykamy się w przypadku usług świadczonych przez wymienione przez Państwa podmioty jest to kto jest administratorem danych osobowych używanych w danym serwisie. Z treści pytania wynika, że interesuje Państwa

tylko ta część danych, które są administrowane przez Google lub Facebooka, stąd też w dalszych rozważaniach pominięty zostanie zakres danych udostępnianych przez użytkowników serwisów, którzy niekiedy również mogą być traktowania jako administratorzy danych osobowych. W przypadku zbiorów danych administrowanych przez Google lub Facebooka mamy do czynienia z udostępnianiem danych tak osobie, której dane dotyczą jak i osobom trzecim, w tym innym administratorom danych.

Przetwarzanie danych osobowych – w tym dla ich udostępniania – jest dopuszczalne tylko wtedy, gdy:

1) osoba, której dane dotyczą, wyrazi na to zgodę, chyba że chodzi o usunięcie dotyczących jej danych,

2) jest to niezbędne dla zrealizowania uprawnienia lub spełnienia obowiązku wynikającego z przepisu prawa, jest to konieczne do realizacji umowy, gdy osoba, której dane dotyczą, jest jej stroną lub gdy jest to niezbędne do podjęcia działań przed zawarciem umowy na żądanie osoby, której dane dotyczą,

3) jest to niezbędne do wykonania określonych prawem zadań realizowanych dla dobra publicznego,

4) jest to niezbędne dla wypełnienia prawnie usprawiedliwionych celów realizowanych przez administratorów danych albo odbiorców danych, a przetwarzanie nie narusza praw i wolności osoby, której dane dotyczą.

Warto jednak zwrócić uwagę, że w przypadku większości usług oferowanych przez Google lub Facebooka za podstawy przetwarzania danych przyjmuje się nie rozwiązania wynikające z prawa polskiego lecz rozwiązania pochodzące z prawa miejsca prowadzenia przedsiębiorstwa przez te podmioty. Tym nie mniej, tak Google jak Facebook, uznają, że podstawową przesłanką do przetwarzania danych osobowych – w tym ich udostępniania – jest zgoda użytkownika wyrażona w trakcie rejestracji do danego serwisu lub w momencie rozszerzania funkcjonalności serwisu o kolejne opcje. Warunki udzielenia takiej zgody i jej zakres opisany jest w regulaminach poszczególnych usług.

W obowiązującej w Unii Europejskiej dyrektywie 95/46/WE zgoda uznana została za niezbędny aspekt podstawowego prawa do ochrony danych osobowych poprzez umiejscowienie jej jako ogólnej przesłanki legalizującej przetwarzanie danych osobowych. Zgodnie z art. 2 lit. h dyrektywy 95/46/WE zgoda osoby, której dane dotyczą, oznacza konkretne i świadome, dobrowolne wskazanie przez osobę, której dane dotyczą, na to, że wyraża przyzwolenie na przetwarzanie odnoszących się do niej danych osobowych. Co istotne, brzmienie tego przepisu przesądza dopuszczalność zgody domniemanej jako dozwolonej przesłanki legalności oświadczenia woli, nie mniej jednak działanie osoby nie może pozostawiać żadnych wątpliwości co do zamiaru wyrażenia zgody (każde jednoznaczne działanie osoby, w tym zgoda wyraźna). Konieczność zachowania wymogu jednoznaczności w wyrażaniu zgody jest zagadnieniem szczególnie istotnym dla zgody udzielanej w środowisku *online*, gdzie bardzo często administratorzy danych stosują mechanizmy i procedury, które nie pozwalają uznać konkretnej zgody za jednoznaczną. Przykładowo domyślne ustawienia wielu serwisów zaprogramowane są w taki sposób, że użytkownik ma włączone wszystkie usługi przetwarzające jego dane w różny sposób. Nie można uznać, że brak działania użytkownika, który nie kliknął rezygnacji z odpowiedniej opcji w ustawieniach, stanowi jednoznaczną zgodę osoby na akceptację przetwarzania danych. Takiego braku działania administrator danych nie może bowiem uznać za wyrażenie zgody na udostępnienie danych w zakresie ustalonym w ustawieniach domyślnych.

Tytułem uzupełnienia nadmienię, że niedawno nowelizowana dyrektywa 2002/58/WE dotycząca przetwarzania danych osobowych i ochrony prywatności w sektorze łączności elektronicznej, stanowiąca *lex specialis* w stosunku do dyrektywy 95/46/WE stanowi wprost, iż definicje zawarte w tej dyrektywie stosuje się także względem dyrektywy 2002/58/WE.

Polska ustawa o ochronie danych osobowych implementuje większość zasad, jakie odnośnie zgody stanowi dyrektywa 94/46/WE, w tym wymóg dobrowolności i konkretności zgody, czy też możliwość odwołania jej w każdej chwili. Inaczej niż w dyrektywie polski ustawodawca odniósł się natomiast do możliwości wyrażenia zgody w sposób dorozumiany. Artykuł 7 pkt 5 ustawy o ochronie danych osobowych przesądza bowiem, iż zgoda nie może być domniemana lub dorozumiana z oświadczenia woli o innej treści. Generalny brak akceptacji dla zgody dorozumianej został potwierdzony przez Naczelny Sąd Administracyjny oraz w stanowiskach Generalnego Inspektora Ochrony Danych Osobowych. Zgoda udzielona na gruncie polskich przepisów musi mieć więc charakter wyraźny.

Na gruncie polskich przepisów zwraca się także uwagę na wymóg swobodnego, nieskrępowanego podjęcia decyzji i wyrażenia woli w sprawie zgody – osoba musi mieć pełną swobodę nie tylko w podjęciu decyzji o wyrażeniu zgody na przetwarzanie danych osobowych, lecz także o tym, jakie dane i w jakim celu zgadza się udostępnić. Mając powyższe na uwadze, niedopuszczalna jest sytuacja, którą często stosują administratorzy serwisów internetowych, gdzie użytkownik aby korzystać z usług jest zmuszony do zaakceptowania kompletu zgód na przetwarzanie danych osobowych. Użytkownik powinien mieć swobodę w wyrażeniu lub niewyrażeniu zgody na przetwarzanie danych osobowych – w przypadku różnych celów przetwarzania danych osobowych, należy pozyskiwać oddzielną zgodę na każdy z tych celów, tak aby osoba miała zapewnioną opcjonalność w podjęciu decyzji, jakie dane i w jakim celu je udostępnia.

Ustawa o świadczeniu usług drogą elektroniczną, która implementuje do polskiego porządku prawnego postanowienia wspomnianej dyrektywy 2002/58/WE, powtarza definicję zgody zawartą w ustawie o ochronie danych osobowych. Pamiętać należy jednak, że zazwyczaj wraz z akceptacją regulaminu danego serwisu między użytkownikiem a serwisem zostaje zawarta umowa o świadczenie usług drogą elektroniczną, co oznacza, że właściciele serwisów mogą przetwarzać dane osobowe użytkowników w zakresie wynikającym z art. 18 ust. 1 i 2 ustawy o świadczeniu usług drogą elektroniczną, zatem pozyskiwanie w tym przypadku dodatkowej zgody na przetwarzanie danych osobowych jest zbędne. Zgodnie bowiem z art. 23 ust. 1 pkt 2 ustawy o ochronie danych osobowych przetwarzanie danych jest dopuszczalne także wtedy, gdy jest to niezbędne do zrealizowania uprawnienia lub spełnienia obowiązku wynikającego z przepisu prawa.

Ze szczególnym przypadkiem mamy do czynienia wówczas gdy dane przetwarzane są wprost na terenie Rzeczypospolitej Polskiej. Ma to na przykład miejsce w przypadku usługi *Google Street View*. Dane bowiem zostały zebrane przy pomocy urządzeń, które znajdowały się na terenie Polski i przekazane zostały do przetwarzania w Stanach Zjednoczonych. W tym przypadku Google Inc. wypełnił wszystkie obowiązki wynikające z prawa polskiego w zakresie określenia podstaw zbierania danych i ich transferu oraz zabezpieczenia technicznego przetwarzania tych danych.

Innym szczególnym rodzajem udostępnienia danych jest udostępnienie danych na potrzeby służb publicznych, co może być dokonane na podstawie przepisów prawnych obowiązujących w poszczególnych krajach, w których przetwarzane są dane. W Polsce

odpowiednie przepisy zawiera przede wszystkim ustawa o świadczeniu usług drogą elektroniczną (art. 18 ust. 5).

Pytanie nr 7.

W ocenie Generalnego Inspektora Ochrony Danych Osobowych dane osobowe przekazywane do USA nie mogą być wykorzystywane przez amerykańską Agencję Bezpieczeństwa Narodowego (NSA) do celów będących w sprzeczności z dyrektywą 95/46/WE Parlamentu Europejskiego i Rady z dnia 24 października 1995 r. w sprawie ochrony osób fizycznych w zakresie przetwarzania danych osobowych i swobodnego przepływu tych danych.

GENERALNY INSPEKTOR OCHRONY DANYCH OSOBOWYCH
dr Wojciech R. Wiewiórowski