GENERALNY INSPEKTOR OCHRONY DANYCH OSOBOWYCH

dr Wojciech R. Wiewiórowski

Warszawa, dnia 2 lipca 2014 r.

DOLiS-035-1238/14

Prezes Zarządu
Spółki Medycznej

W y s t ą p i e n i e

na podstawie art. 19a ust. 1 ustawy z dnia 29 sierpnia 1997 r. o ochronie danych osobowych (Dz. U. z 2002 r. nr 101, poz. 926, z późn. zm.), zgodnie z którym Generalny Inspektor może kierować do osób fizycznych i prawnych wystąpienia zmierzające do zapewnienia skutecznej ochrony danych osobowych zwracam się do Pani o podjęcie działań mających na celu dostosowanie procesu przetwarzania danych osobowych do wymogów określonych przepisami ustawy o ochronie danych osobowych.

Generalny Inspektor Ochrony Danych Osobowych powziął informację o tym, że pracownicy Spółki Medycznej stosują praktykę przesyłania na adresy poczty elektronicznej informacji handlowych, udostępniają przy tej okazji wszystkim odbiorcom wiadomości listę mailingową zawierającą dane osobowe innych osób, takie jak adres email. Działanie takie pozostaje w sprzeczności z zasadami określonymi w ustawie o ochronie danych osobowych.

Na wstępie podkreślić należy, że istotą ochrony danych osobowych jest ochrona prywatności osoby, której dane dotyczą. Źródło tej ochrony wynika przede wszystkim z przepisów ustawy z dnia 2 kwietnia 1997 r. – Konstytucja Rzeczypospolitej Polskiej (Dz. U. Nr 78, poz. 483 ze zm.). I tak, stosownie do treści jej art. 47, każdy ma prawo m.in. do ochrony prawnej życia prywatnego, rodzinnego, czci i dobrego imienia. Ponadto, zgodnie z art. 51 ust. 5 Konstytucji Rzeczypospolitej Polskiej, zasady i tryb gromadzenia oraz udostępniania informacji o osobie określa ustawa. Dyspozycję powołanego przepisu wypełniają właśnie przepisy ustawy o ochronie danych osobowych, która określa zasady postępowania przy przetwarzaniu danych osobowych oraz prawa osób fizycznych, których dane osobowe są lub mogą być przetwarzane w zbiorach danych (art. 2 ust. 1 ustawy).

Wskazuję, że na gruncie przepisów ustawy o ochronie danych osobowych w niektórych sytuacjach adres poczty elektronicznej może być uznany za daną osobową. Zgodnie bowiem z treścią art. 6 ust. 1 ustawy o ochronie danych osobowych za dane osobowe uważa się wszelkie informacje dotyczące zidentyfikowanej lub możliwej do zidentyfikowania osoby fizycznej. Osobą

ul. Stawki 2
00-193 Warszawa

tel. 860-70-83
fax. 860-70-86
www.giodo.gov.pl

możliwą do zidentyfikowania jest osoba, której tożsamość można określić bezpośrednio lub pośrednio, w szczególności przez powołanie się na numer identyfikacyjny albo jeden lub kilka specyficznych czynników określających jej cechy fizyczne, fizjologiczne, umysłowe, ekonomiczne, kulturowe lub społeczne (art. 6 ust. 2). Stosownie do ust. 3 powołanego przepisu, informacji nie uważa się za umożliwiającą określenie tożsamości osoby, jeżeli wymagałoby to nadmiernych kosztów, czasu lub działań. Danymi osobowymi będą zatem zarówno takie dane, które pozwalają na określenie tożsamości konkretnej osoby, jak i takie, które nie pozwalają na jej natychmiastową identyfikację, ale są przy pewnym nakładzie kosztów, czasu i działań, wystarczające do jej ustalenia. Adres poczty elektronicznej będzie stanowił daną osobową, o ile nie będą zachodziły przesłanki z wyżej przytoczonego art. 6 ust. 3 ustawy. Kryterium ułatwiającym uznanie adresu e-mail za daną osobową może być w szczególności jego treść. Adres poczty elektronicznej należy zatem traktować jako informację, która potencjalnie może być daną osobową, ale z uwzględnieniem wszelkich okoliczności występujących w konkretnym przypadku. Każdorazowo decydujące znaczenie dla ewentualnego uznania ich za dane osobowe będzie miała możliwość identyfikacji pośredniej określonego użytkownika, a więc identyfikacja z wykorzystaniem dodatkowych informacji będących w posiadaniu administratora danych lub innych osób.

Na gruncie cytowanej ustawy, o zgodnym z prawem przetwarzaniu (pod którym to pojęciem – stosownie do jej art. 7 pkt 2 – rozumie się jakiekolwiek operacje wykonywane na danych osobowych, takie jak zbieranie, utrwalanie, przechowywanie, opracowywanie, zmienianie, udostępnianie i usuwanie, a zwłaszcza te które wykonuje się w systemach informatycznych) danych osobowych, mówić można jedynie w sytuacji, gdy ich administrator dopełnia wszelkich obowiązków określonych przepisami powołanego na wstępie aktu prawnego. Proces przetwarzania danych osobowych (przy czym stosownie do treści art. 7 pkt 2 ustawy o ochronie danych osobowych za przetwarzanie należy rozumieć także udostępnianie) tzw. zwykłych, jak np. imię i nazwisko czy adres jest procesem legalnym, gdy ich administrator opiera swoje działanie na jednej ze wskazanych w art. 23 ust. 1 pkt 1 – 5 ustawy przesłanek legalności przetwarzania danych osobowych. Zgodnie z tymi postanowieniami przetwarzanie danych jest dopuszczalne jedynie, 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,
3) 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,
4) jest niezbędne do wykonania określonych prawem zadań realizowanych dla dobra publicznego,
5) 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.

Osoba do której skierowana jest korespondencja przesyłana także do innych odbiorców, co do zasady, nie powinna mieć możliwości zapoznawania się z danymi pozostałych adresatów wiadomości. Administrator danych osobowych jest bowiem zobowiązany do przestrzegania przepisów ustawy o ochronie danych osobowych, w tym art. 36 ust. 1 w/w ustawy, który nakłada obowiązek zastosowania środków technicznych i organizacyjnych zapewniających ochronę przetwarzanych danych osobowych odpowiednią do zagrożeń oraz kategorii danych objętych ochroną. W myśl cytowanego przepisu administrator w szczególności powinien zabezpieczyć dane przed ich udostępnieniem osobom nieupoważnionym, zabraniem przez osobę nieuprawnioną, przetwarzaniem z naruszeniem ustawy oraz zmianą, utratą, uszkodzeniem lub zniszczeniem. Stąd należy także wnosić, że w przypadku wysyłania korespondencji do większej liczby osób należy dbać o to, aby dane osobowe nie były udostępniane wszystkim adresatom wiadomości.

Dlatego też za dobrą praktykę należy uznać przesyłanie wiadomości skierowanej do większej ilości odbiorców w taki sposób, aby żaden z nich nie mógł zapoznać się z adresami poczty elektronicznej innych adresatów wiadomości.

Zgodnie z treścią art. 18 ust. 1 ustawy, Generalny Inspektor, w przypadku stwierdzenia naruszenia przepisów ochrony danych osobowych, może w drodze decyzji administracyjnej nakazać przywrócenie stanu zgodnego z prawem. W szczególności może nakazać zastosowanie dodatkowych środków zabezpieczających zgromadzone dane. Ma to usprawnić realizację podstawowego obowiązku administratora, jakim jest właściwe zabezpieczenie danych (art. 36 ust. 1 ustawy). Oznacza on konieczność zastosowania środków technicznych i organizacyjnych zapewniających ochronę przetwarzanych danych osobowych odpowiednią do zagrożeń oraz kategorii danych objętych ochroną, a w szczególności zabezpieczenie danych przed ich udostępnieniem osobom nieupoważnionym, zabraniem przez osobę nieuprawnioną, przetwarzaniem z naruszeniem ustawy oraz zmianą, utratą, uszkodzeniem lub zniszczeniem. Innymi słowy art. 36 ust. 1 ustawy zobowiązuje każdego administratora danych do wprowadzenia takich środków oraz rozwiązań technicznych i organizacyjnych, które zapewnią danym osobowym, w konkretnych warunkach i okolicznościach przetwarzania, skuteczną ochronę przed potencjalnymi zagrożeniami.

Zgodnie z postanowieniem art. 12, Inspektor może w celu zapewnienia wykonania obowiązków określonych w w/w decyzji stosować środki egzekucyjne przewidziane w ustawie z dnia 17 czerwca 1966 r. o postępowaniu egzekucyjnym w administracji (Dz.U. z 2005 r., nr 229, poz. 1954 z późn. zm.).

Przypominam także, że zgodnie z brzmieniem art. 51 ustawy o ochronie danych osobowych udostępnianie przez administratora zbioru danych (spółka) albo osoby obowiązane do ochrony danych osobowych (pracownicy) osobom do tego nieupoważnionym jest czynem karalnym zagrożonym przynajmniej karą grzywny. Zgodnie z postanowieniem art. 201 ustawy z dnia 15 września 2000 r. Kodeks spółek handlowych (tekst jednolity: Dz.U. 2013 r. poz. 1030) ewentualna odpowiedzialność za wyżej określone działania może spoczywać, obok pracowników spółki, także na osobach kierujących spółką, która występuje w roli administratora danych osobowych

zobowiązanego do przestrzegania zasad przetwarzania danych osobowych zgodnie z obowiązującymi przepisami prawa.

Jedynie na marginesie niniejszej korespondencji i informacyjnie wskazuję także, że w oparciu o znowelizowane przepisy szczególne ustawy z dnia 18 lipca 2002 r. o świadczeniu usług drogą elektroniczną (Dz.U. z 2002 nr 144 poz. 1204 z późn. zm.), regulującej kwestie dotyczące obowiązków usługodawców związanych ze świadczeniem usług drogą elektroniczną oraz zasady ochrony danych osobowych użytkowników poczty elektronicznej, zakazane jest zgodnie z art. 10 ust. 1 ww. ustawy przesyłanie za pomocą środków komunikacji elektronicznej, w szczególności poczty elektronicznej, niezamówionej informacji handlowej skierowanej do oznaczonego odbiorcy będącego osobą fizyczną (w/w przepis ustawy nie będzie miał zatem zastosowania np. w przypadku wysyłania ofert do osób prawnych). Informację handlową – w myśl art. 10 ust. 2 ustawy – uważa się za zamówioną, jeżeli odbiorca wyraził zgodę na jej otrzymywanie, w szczególności udostępnił w tym celu identyfikujący go adres elektroniczny. Art. 4 ust. 1 powołanej ustawy stanowi zaś, iż jeżeli ustawa wymaga uzyskania zgody usługobiorcy, to zgoda ta nie może być domniemana lub dorozumiana, ponadto może być odwołana w każdym czasie.

Mając na uwadze powyższe zwracam się o podjęcie stosownych działań mających na celu wyeliminowanie na przyszłość działań, które potencjalnie mogą stanowić naruszenie ustawy o ochronie danych osobowych i poinformowanie o tych działaniach Generalnego Inspektora Ochrony Danych Osobowych **w terminie 30 dni** od dnia otrzymania niniejszego pisma, stosownie do treści art. 19a ustęp 3 ustawy o ochronie danych osobowych. Wskazuję także, że treść wystąpienia wraz z udzieloną odpowiedzią zostaną umieszczone na stronie internetowej Generalnego Inspektora Ochrony Danych Osobowych.