



**GENERALNY INSPEKTOR
OCHRONY DANYCH
OSOBOWYCH**

dr Edyta Bielak-Jomaa

Warszawa, dnia 19 sierpnia 2015 r.

DOLIS-035-1157/15

**Członek Zarządu
M Y G**

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. 2014 r. poz. 1182, z późn. zm.), zgodnie z którym Generalny Inspektor może kierować do osób fizycznych i prawnych, jednostek organizacyjnych niebędących osobami prawnymi oraz innych podmiotów wystąpienia zmierzające do zapewnienia skutecznej ochrony danych osobowych zwracam się do Państwa o podjęcie działań mających na celu dostosowanie procesu przetwarzania danych osobowych do wymogów określonych przepisami ustawy o ochronie danych osobowych.

Impulsem do skierowania niniejszego wystąpienia jest powzięta przez Generalnego Inspektora Ochrony Danych Osobowych informacja dotycząca udostępnienia przez Biuro Sprzedaży A G adresów poczty elektronicznej klientów - poprzez wysłanie wiadomości ujawniającej listę mailingową, zawierającą dane osobowe innych adresatów tejże wiadomości - takie jak adres email oraz imię i nazwisko. 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.). Zgodnie z Konstytucją RP każdy ma prawo m.in. do ochrony prawnej życia prywatnego, rodzinnego, czci i dobrego imienia (art. 47 Konstytucji), nikt nie może być obowiązany inaczej niż na podstawie ustawy do ujawniania informacji dotyczących jego osoby (art. 51 ust. 1 konstytucji), a zasady i tryb gromadzenia oraz udostępniania informacji o osobie określa ustawa (art. 51 ust. 5). Dyspozycję art. 51 ust. 5 Konstytucji wypełnia właśnie ustawa 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). Na gruncie cytowanej ustawy, o zgodnym z prawem przetwarzaniu (pod którym to pojęciem – stosownie do jej art. 7 pkt 2 – rozumie się jakiegokolwiek 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 określonych przepisami powołanego na wstępie aktu prawnego, obowiązków.

Na gruncie przepisów ustawy o ochronie danych osobowych adres poczty elektronicznej może być uznany za daną osobową. Zgodnie 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 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. Elementarnym kryterium ułatwiającym uznanie adresu e-mail za daną osobową będzie w szczególności jego treść (np. zawierająca imię lub skrót imienia i nazwisko). Adres poczty elektronicznej - zwłaszcza w połączeniu z imieniem i nazwiskiem - 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.

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 (w tym poczty elektronicznej) 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. W związku z powyższym, na podstawie art. 23 ust. 1 ustawy przetwarzanie danych jest dopuszczalne po spełnieniu jednego z następujących warunków: osoba, której dane dotyczą, wyrazi na to zgodę, chyba że chodzi o usunięcie dotyczących jej danych (pkt 1); jest to niezbędne dla zrealizowania uprawnienia lub spełnienia obowiązku wynikającego z przepisu prawa (pkt 2); 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 (pkt 3); jest niezbędne do wykonania określonych prawem zadań realizowanych dla dobra publicznego (pkt 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 (pkt 5).

Stosownie do treści art. 26 ust. 1 pkt 1 ustawy, administrator danych przetwarzający dane powinien dołożyć szczególnej staranności w celu ochrony interesów osób, których dane dotyczą, a w szczególności jest obowiązany zapewnić, aby dane te były przetwarzane zgodnie z prawem. Z kolei ustęp 1 pkt 2 tego artykułu nakłada na administratora danych obowiązek zapewnienia, by dane osobowe były zbierane dla oznaczonych, zgodnych z prawem celów i nie poddawane dalszemu przetwarzaniu niezgodnemu z tymi celami, z zastrzeżeniem ust. 2 tego przepisu.

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 ustawy o ochronie danych osobowych, z którego wynika 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, zabranieniem przez osobę nieuprawnioną, przetwarzaniem z naruszeniem ustawy oraz zmianą, utratą, uszkodzeniem lub zniszczeniem. Ponadto zgodnie z art. 39 ust. 2 ustawy osoby, które zostały upoważnione do przetwarzania danych, są obowiązane zachować w tajemnicy te dane osobowe oraz sposoby ich zabezpieczenia.

Stąd należy także wnosić, że w przypadku wysyłania korespondencji do większej liczby osób należy dbać o to, aby żaden z odbiorców nie mógł zapoznać się z adresami poczty elektronicznej innych adresatów wiadomości.

Nie można przy tym jednoznacznie zanegować możliwości przesyłania wiadomości drogą elektroniczną do wielu odbiorców - które odbywałoby się zgodnie z obowiązującymi przepisami

prawa - jednak zwrócić należy szczególną uwagę, iż we wskazywanej przez organ do spraw ochrony danych osobowych sytuacji, mając na względzie sposób skierowania korespondencji, podmioty, których dane osobowe zostały udostępnione osobom nieuprawnionym indywidualnie kontaktowały się z administratorem danych osobowych i ponad wszelką wątpliwość oczekiwały indywidualnej odpowiedzi (wysłanej wyłącznie do ich wiadomości) na swoją korespondencję.

Istnieje zatem 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, zabranie 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.

Warto wskazać, iż za nieprzestrzeganie przepisów o ochronie danych osobowych, np. polegające na udostępnieniu danych osobowych osobom do tego nieupoważnionym ponieść można zarówno odpowiedzialność administracyjną, jak i karną, o której mowa w rozdziale 8 ustawy o ochronie danych osobowych. Zgodnie z art. 51 ust. 1, kto administrując zbiorem danych lub będąc obowiązany do ochrony danych osobowych udostępnia je lub umożliwia dostęp do nich osobom nieupoważnionym, podlega grzywnie, karze ograniczenia wolności albo pozbawienia wolności do lat 2. Ustęp 2 powyższego przepisu określa, iż w sytuacji, gdy sprawca działa nieumyślnie, podlega grzywnie, karze ograniczenia wolności albo pozbawienia wolności do roku.

Mając na uwadze powyższe zwracam się do Państwa o podjęcie stosownych działań mających na celu wyeliminowanie na przyszłość sytuacji, w których dochodzi do zapoznania się przez osoby nieuprawnione z danymi znajdującymi się w wyłącznej dyspozycji M Y G, jak również o poinformowanie o wynikach tych działań **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