GENERALNY INSPEKTOR
OCHRONY DANYCH
OSOBOWYCH
dr Edyta Bielak-Jomaa

Warszawa, dnia 11 października 2016 r.

DOLiS-440-247/16/SPI/I/

Dyrektor
Wojewódzkiej i Miejskiej Biblioteki
Publicznej

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 (t.j. Dz. U. z 2016 r. poz. 922), 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 Pana o podjęcie działań mających na celu dostosowanie procesu przetwarzania danych osobowych do wymogów określonych przepisami ustawy z dnia 29 sierpnia 1997 roku o ochronie danych osobowych, w związku z prowadzeniem korespondencji drogą elektroniczną.

Generalny Inspektor Ochrony Danych Osobowych powziął informację o tym, że z adresu poczty e-mail *(...)* w dniu (…) lutego 2016 r. została przesłana wiadomość elektroniczna e-mail, w której każdy z jej odbiorców otrzymał pełną listę innych jej adresatów. 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 ustawa z dnia 29 sierpnia 1997 r. o ochronie danych osobowych (t.j. Dz. U. z 2016 r. poz. 922), zwana dalej ustawą, 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).

Stosownie do brzmienia art. 7 pkt 2 tej ustawy, pod pojęciem przetwarzania danych rozumieć należy 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. Przy czym, nawiązując do treści art. 6 ust 1 ustawy, za dane osobowe uważa się wszelkie informacje dotyczące zidentyfikowanej lub możliwej do zidentyfikowania osoby fizycznej. O zgodnym z prawem przetwarzaniu danych osobowych, mówić można jedynie w sytuacji, gdy ich administrator dopełnia wszelkich określonych przepisami powołanego na wstępie aktu prawnego, obowiązków. Proces przetwarzania danych osobowych (a więc również udostępniania), 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.

Odnosząc się natomiast do adresu poczty elektronicznej należy wskazać, że jest on związany z infrastrukturą sieciową zarządzaną przez określonego operatora/dostawcę, u którego podczas tworzenia konta poczty elektronicznej rejestrowane są dane użytkownika. Dla oceny, czy określony adres e-mail będzie daną osobową niezbędnym jest zatem analiza wszelkich informacji związanych z danym adresem e-mail (np. IP komputera, czy danych z formularza wypełnianego przy tworzeniu konta pocztowego). Informacje uzyskane z tej analizy mogą pozwolić na bezpośrednie zidentyfikowanie osoby fizycznej lub umożliwią jej pośrednią identyfikację. Należy zatem stwierdzić, że istnieje możliwość identyfikacji osoby będącej użytkownikiem danego adresu, podobnie jak na podstawie adresu IP użytkownika komputera. Elementarnym kryterium ułatwiającym uznanie adresu e-mail za daną osobową będzie w szczególności jego treść (np. zawierająca imię lub skrót imienia i nazwisko). Nie zawsze jednak adres ten prowadzi do identyfikacji osoby fizycznej. Może bowiem dotyczyć on również podmiotów nie będących osobami fizycznymi. Adres poczty elektronicznej należy zatem traktować jako informację, która potencjalnie może być daną osobową, ale z uwzględnieniem wszelkich okoliczności występujących w konkretnym przypadku.

Jednym z podstawowych, wynikającymi z ustawy o ochronie danych osobowych obowiązków ciążących na administratorze danych i warunkującym legalność ich przetwarzania jest obowiązek zastosowania środków technicznych i organizacyjnych zapewniających ochronę przetwarzanych danych osobowych odpowiednią do zagrożeń oraz kategorii danych objętych ochroną, o których mowa w rozdziale 5 ustawy o ochronie danych osobowych, zaś w przypadku przetwarzania danych w systemie informatycznym – w przepisach rozporządzenia Ministra Spraw Wewnętrznych i Administracji z dnia 29 kwietnia 2004 r. w sprawie dokumentacji przetwarzania danych osobowych oraz warunków technicznych i organizacyjnych, jakim powinny odpowiadać urządzenia i systemy informatyczne służące do przetwarzania danych osobowych (Dz. U. z 2004 r., Nr 100, poz. 1024). Tytułem przykładu należy wskazać, że art. 36 ust. 1 ww. ustawy 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, innymi słowy, osoba do której skierowana jest korespondencja, która przesyłana jest także do innych odbiorców, co do zasady, nie powinna mieć możliwości zapoznawania się z danymi pozostałych adresatów wiadomości. Generalny Inspektor Ochrony Danych Osobowych jednocześnie wskazuje, że istnieją proste środki, które pozwalają na ukrycie innych adresatów wiadomości e-mail poprzez zastosowanie chociażby tzw. pola UDW (tj. „ukryte do wiadomości", ang. BCC). Pozwala to zapobiec udostępnieniu danych osobowych osobom do tego nieuprawnionym.

Niezależnie od powyższego wskazuję, że zgodnie z art. 36a ust. 1 ustawy o ochronie danych osobowych, administrator danych może powołać administratora bezpieczeństwa informacji, którego zadaniem jest: zapewnianie przestrzegania przepisów o ochronie danych osobowych (art. 36a ust. 2 pkt 1 ustawy o ochronie danych osobowych) oraz prowadzenie rejestru zbiorów danych przetwarzanych przez administratora danych (zgodnie z art. 36a ust. 2 pkt 2 ustawy o ochronie danych osobowych). Powołanie ABI jest zatem fakultatywne, niemniej jednak poprzez osobę ABI administrator danych pozyskuję osobę, która ze względu na posiadaną wiedzę z zakresu ochrony danych osobowych będzie mogła zadbać nie tylko o należyte zabezpieczenie danych osobowych, ale także o kompleksowe zapewnienie u administratora danych przestrzeganie przepisów o ochronie danych osobowych. W przypadku niepowołania administratora bezpieczeństwa informacji zadania określone w art. 36a ust. 2 pkt 1, z wyłączeniem obowiązku sporządzania sprawozdania, o którym mowa w art. 36a ust. 2 pkt 1 lit. a, wykonuje administrator danych (art. 36b).

Podkreślenia wymaga, iż administrujący danymi musi brać pod uwagę możliwość poniesienia odpowiedzialności nie tylko administracyjnej, ale i karnej. Stosownie bowiem do treści art. 51 ust. 1 ustawy o ochronie danych osobowych, kto administrując zbiorem danych lub będąc obowiązanym do ochrony danych osobowych udostępnia je lub umożliwia dostęp do nich osobom nieupoważnionym, podlega grzywnie, karze ograniczenia wolności albo pozbawienia wolności do lat 2. Odpowiedzialność ta rozszerzona została w art. 52 ustawy, zgodnie z którym penalizowane jest także nieumyślne naruszenie obowiązku zabezpieczenia danych przed ich zabraniem przez osobę nieupoważnioną, uszkodzeniem lub zniszczeniem. Jak twierdzi A. Drozd, „przestępstwo stypizowane w art. 52 może popełnić każda osoba, na której ciąży obowiązek zabezpieczenia danych osobowych przed ich zabraniem przez osobę nieuprawnioną, uszkodzeniem lub zniszczeniem. Będzie to w szczególności osoba fizyczna występująca w roli administratora danych albo przetwarzającego" (A. Drozd, Ustawa o ochronie danych osobowych. Komentarz. Wzory pism i przepisy. Warszawa 2007, Wydawnictwo Prawnicze LexisNexis, Wydanie III, s. 325).

W kwestii zagadnień dotyczących ochrony danych osobowych organ ds. ochrony danych osobowych zachęca do zapoznania się z serwisem ABI-Informator (https://abi.giodo.gov.pl/).

Mając na uwadze powyższe zwracam się o podjęcie stosownych działań mających na celu wyeliminowanie na przyszłość podobnych działań oraz o poinformowanie 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 o działaniach podjętych w związku z okolicznościami wskazanymi w niniejszym piśmie. Wskazuję także, że treść wystąpienia wraz z udzieloną odpowiedzią mogą zostać umieszczone na stronie internetowej Generalnego Inspektora Ochrony Danych Osobowych.