



**GENERALNY INSPEKTOR
OCHRONY DANYCH
OSOBOWYCH**

dr Wojciech R. Wiewiórowski

Warszawa, dnia 20 czerwca 2014 r.

DOLiS-035- 1245 /14

AGENCJA REKLAMY

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, jednostek organizacyjnych niebędących osobami prawnymi oraz innych podmiotów 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 z dnia 29 sierpnia 1997 roku o ochronie danych osobowych.

Niniejszym informuję Panią, że Generalny Inspektor Ochrony Danych Osobowych powziął informację o tym, że pracownicy Pani firmy przesyłają na adresy poczty elektronicznej różnych osób informacje handlowe, udostępniając jednocześnie przy tej okazji wszystkim odbiorcom wysyłanej wiadomości listę mailingową zawierającą dane osobowe innych adresatów 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. 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.

Administrator danych osobowych jest ponadto zobowiązany m. in. do przestrzegania przepisów ustawy o ochronie danych osobowych w zakresie zasad zabezpieczenia danych osobowych. Art. 36 ust. 1 w/w 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, zabranieniem 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.

Informacyjnie wskazuję także, że w oparciu o przepisy 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.

Jednocześnie przypominam, że ustawa nakłada na administratora określone obowiązki, w tym zobowiązuje go, aby: 1) dopełnił – ustanowionego w art. 40 ustawy o ochronie danych osobowych - obowiązku zgłoszenia zbioru danych do rejestracji Generalnemu Inspektorowi Ochrony Danych Osobowych (GIODO) - zgłoszenie zbioru danych do rejestracji jest regułą, od której wyjątki wymienione zostały w art. 43 ust. 1 pkt. 1-11 ustawy o ochronie danych osobowych. Katalog tych wyjątków jest zamknięty i nie może być interpretowany rozszerzająco. Oceny tego, czy zbiór należy zgłosić do rejestracji, administrator danych dokonuje sam, przy czym zwolnienie zbioru danych z rejestracji jest możliwe tylko wówczas, gdy przesłanka uprawniająca do odstąpienia od rejestracji dotyczy wszystkich danych zawartych w zbiorze, 2) stosował odpowiednie zabezpieczenia, o których stanowią przepisy

rozdziału 5 ustawy o ochronie danych osobowych oraz rozporządzenie 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 – administrator jest bowiem zobowiązany zastosować środki techniczne i organizacyjne zapewniające przetwarzanym danym odpowiednią ochronę, a przede wszystkim zabezpieczyć dane przed ich udostępnieniem osobom nieupoważnionym, zebraniem przez osobę nieuprawnioną, przetwarzaniem z naruszeniem ustawy oraz utratą, uszkodzeniem lub zniszczeniem (art. 36 ust. 1 ustawy o ochronie danych osobowych), 3) dopełnił obowiązku informacyjnego ustanowionego w art. 24 ust. 1 oraz art. 25 ust. 1 ustawy o ochronie danych osobowych, chyba że administrator danych jest z niego zwolniony – w przypadku zbierania danych bezpośrednio od osoby, której dotyczą (art. 24) administrator musi poinformować ją o swojej nazwie i adresie, celu zbierania, odbiorcach danych (także tych przewidywanych), prawie dostępu do danych i prawie ich poprawiania, a także o dobrowolności albo obowiązku ich podania (a gdy obowiązek ten istnieje – o jego podstawie prawnej). W przypadku zbierania danych nie od osoby, której one dotyczą (art. 25), administrator – zaraz po utrwaleniu danych – musi poinformować osobę, której one dotyczą, o swojej nazwie i adresie, celu i zakresie zbierania danych, a zwłaszcza o ich odbiorcach, źródle, z którego dane pozyskał, prawie dostępu do danych i prawie ich poprawiania, a także o prawie żądania zaprzestania przetwarzania danych lub wniesienia sprzeciwu wobec przetwarzania danych, 4) dokładał szczególnej staranności w celu ochrony interesów osób, których dane dotyczą, poprzez zapewnienie, aby dane były przetwarzane zgodnie z prawem, zbierane dla oznaczonych, zgodnych z prawem celów i niepoddawane dalszemu przetwarzaniu niezgodnemu z tymi celami, merytorycznie poprawne i adekwatne w stosunku do celów, w jakich są przetwarzane, przechowywane w postaci umożliwiającej identyfikację osób, których dotyczą, nie dłużej niż jest to niezbędne do osiągnięcia celu przetwarzania (o czym stanowi art. 26 ust. 1 pkt. 1 – 4 ustawy o ochronie danych osobowych), 5) respektował prawa osób, których dane dotyczą – prawa te wymienione są w rozdziale 4 ustawy o ochronie danych osobowych i dotyczą kontroli procesu przetwarzania danych.

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.