



**GENERALNY INSPEKTOR
OCHRONY DANYCH
OSOBOWYCH**

dr Wojciech R. Wiewiórowski

Warszawa, dnia 19 sierpnia 2011 r.

DOLiS-035- 2399/11/PW/

Sz.P.

gen. insp. Andrzej Matejuk

Komendant Główny Policji

Komenda Główna Policji

ul. Puławska 148/150

02-624 Warszawa

WYSTĄPIENIE

na podstawie art. 19a ust. 1 ustawy z dnia 29 sierpnia 1997 r. o ochronie danych osobowych (t.j. Dz.U. z 2002 r. Nr 101, poz. 926, z późn. zm.) – zgodnie z którym w celu realizacji zadań, o których mowa w art. 12 pkt 6, Generalny Inspektor może kierować do organów państwowych, organów samorządu terytorialnego, państwowych i komunalnych jednostek organizacyjnych, podmiotów niepublicznych realizujących zadania publiczne, osób fizycznych i prawnych, jednostek organizacyjnych niebędących osobami prawnymi oraz innych podmiotów wystąpienia zmierzające do zapewnienia skutecznej ochrony danych osobowych – zwracam się do Pana Generala o unaocznienie podległym komendantom wojewódzkim konieczności przestrzegania przepisów o ochronie danych osobowych, w szczególności w procesie udostępniania informacji publicznej.

Generalny Inspektor Ochrony Danych Osobowych pozyskał informację, iż na stronie w Biuletynie Informacji Publicznej Komendy Wojewódzkiej Policji w Kielcach, w związku ze sprawozdaniem z działalności kontrolnej w 2010 roku znalazły się informacje zawierające dane osobowe osób zatrzymanych.

Na wstępie wyjaśniam, iż wszystkie czynności podejmowane w związku z przetwarzaniem danych osobowych powinny przebiegać w zgodzie z obowiązującymi w tym zakresie przepisami, w tym ustawy z dnia 29 sierpnia 1997 r. o ochronie danych osobowych (Dz. U. 2002 r. Nr 101, poz. 926 z późn. zm.), zwanej dalej ustawą i wydanych na jej podstawie aktów wykonawczych.

Należy zwrócić uwagę na art. 27 ust. 1 ustawy o ochronie danych osobowych, wskazujący, które dane ustawodawca uznał za szczególnie chronione. Zgodnie z tym przepisem zabrania się przetwarzania danych ujawniających pochodzenie rasowe lub etniczne, poglądy polityczne, przekonania religijne lub filozoficzne, przynależność wyznaniową, partyjną lub związkową, jak również danych o stanie zdrowia, kodzie genetycznym, nałogach lub życiu seksualnym oraz danych dotyczących skazań, orzeczeń o ukaraniu i mandatów karnych, a także innych orzeczeń wydanych w postępowaniu sądowym lub administracyjnym.

Zgodnie z art. 6 ustawy o ochronie danych 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. Informacji nie uważa się za umożliwiającą określenie tożsamości osoby, jeżeli wymagałoby to nadmiernych kosztów, czasu lub działań.

Podniesienia wymaga, że ustawa o ochronie danych osobowych definiuje przetwarzanie danych jako 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 (art. 7 pkt 2 ustawy). Niezbędnym warunkiem legalności każdej czynności mieszczącej się w pojęciu przetwarzania danych, w tym ich udostępniania, jest spełnienie którejkolwiek z przesłanek dopuszczalności przetwarzania danych wymienionych w art. 23 ust. 1 lub art. 27 ust. 2 ustawy. Przetwarzanie danych jest więc dopuszczalne m. in. wówczas, gdy jest to niezbędne dla zrealizowania uprawnienia lub spełnienia obowiązku wynikającego z przepisu prawa (art. 23 ust. 1 pkt 2 ustawy). Powołana przesłanka ma zasadnicze znaczenie dla okoliczności przetwarzania danych osobowych przez organy władzy publicznej – upoważnione do działania wyłącznie na podstawie i w granicach prawa (art. 7 Konstytucji RP oraz art. 6 Kodeksu postępowania administracyjnego).

Należy stwierdzić, iż co prawda ustawa o dostępie do informacji publicznej nakazuje udostępnianie każdej informacji o sprawach publicznych, to zgodnie z jej art. 5, prawo do informacji publicznej podlega ograniczeniu w zakresie i na zasadach określonych w przepisach o ochronie informacji niejawnych oraz ochronie innych tajemnic ustawowo chronionych oraz ze względu na prywatność osoby fizycznej lub tajemnicę przedsiębiorcy. Ograniczenie to nie dotyczy informacji o osobach pełniących funkcje publiczne, mających związek z pełnieniem tych funkcji, w tym

o warunkach powierzenia i wykonywania funkcji, oraz w przypadku, gdy osoba fizyczna lub przedsiębiorca rezygnują z przysługującego im prawa.

Wskazuję, że Trybunał Konstytucyjny wielokrotnie w wydanych orzeczeniach wyrażał pogląd, iż prawo dostępu do informacji nie ma charakteru bezwzględnego, a jego granice wyznaczone są m.in. przez konieczność respektowania praw i wolności innych podmiotów, w tym przez konstytucyjnie gwarantowane prawo do ochrony życia prywatnego. Nie negując konieczności zapewnienia transparentności i możliwości weryfikowania działalności Policji przez społeczeństwo, podkreślić należy, iż w demokratycznym państwie prawnym konieczne jest także respektowanie prawa do prywatności i ochrony danych osobowych. Zgodnie z art. 47 Konstytucji Rzeczypospolitej Polskiej, każdy ma prawo do ochrony prawnej życia prywatnego, rodzinnego, czci i dobrego imienia oraz do decydowania o swoim życiu osobistym. Polska ustawa zasadnicza podkreśla przy tym, w swym art. 233 ust. 1, że prawo to nie może doznawać ograniczeń także w stanach nadzwyczajnych. Skoro zatem przepisy Konstytucji RP chronią przedmiotowe prawo w sytuacji zagrożenia, to tym bardziej nie mogą wprowadzać w tym zakresie ograniczeń wówczas, kiedy płynące z powyższego „korzyści” nie są wystarczające dla uznania zasadności ingerencji o takim charakterze (wyrok z dnia 20 marca 2006 r., sygn. akt K 17/2005). Trybunał Konstytucyjny podkreślił również, iż, cyt.: „(...) Nie można (...) tracić z pola widzenia faktu, że prawo do prywatności ma charakter szczególny w systemie praw i wolności konstytucyjnych (...)”

Ponadto, art. 51 Konstytucji RP stanowi, że nikt nie może być obowiązany inaczej niż na podstawie ustawy do ujawniania informacji dotyczących jego osoby (ust. 1); władze publiczne nie mogą pozyskiwać, gromadzić i udostępniać innych informacji o obywatelach niż niezbędne w demokratycznym państwie prawnym (ust. 2); każdy ma prawo dostępu do dotyczących go urzędowych dokumentów i zbiorów danych. Ograniczenie tego prawa może określić ustawa (ust. 3); każdy ma prawo do żądania sprostowania oraz usunięcia informacji nieprawdziwych, niepełnych lub zebranych w sposób sprzeczny z ustawą (ust. 4); zasady i tryb gromadzenia oraz udostępniania informacji określa ustawa (ust. 5). Wskazać przy tym należy również na ustanowioną w art. 31 ust. 1 Konstytucji RP zasadę, dopuszczającą ograniczenia w zakresie korzystania z konstytucyjnych wolności i praw ustanawiane tylko w ustawie i tylko wtedy, gdy są konieczne w demokratycznym państwie dla jego bezpieczeństwa lub porządku publicznego, bądź dla ochrony środowiska, zdrowia i moralności publicznej, albo wolności i praw innych osób. Ograniczenia te nie mogą naruszać istoty wolności i praw.

Obowiązek poszanowania prawa do prywatności wynika również z faktu, iż Rzeczpospolita Polska, jako państwo członkowskie Unii Europejskiej, jest stroną europejskiej Konwencji o ochronie praw człowieka i podstawowych wolności, sporządzonej w Rzymie w dniu 4 listopada 1950 r., która w swym art. 8 ustanawia prawo do poszanowania życia prywatnego i rodzinnego, swojego mieszkania i swojej korespondencji.

Stosownie do art. 36 ust. 1 ustawy o ochronie danych osobowych administrator danych jest obowiązany zastosować środki techniczne i organizacyjne zapewniające ochronę przetwarzanych danych osobowych odpowiednie do zagrożeń oraz kategorii danych objętych ochroną, a w szczególności powinien zabezpieczyć dane przed ich udostępnieniem osobom nieupoważnionym, zabranieniem przez osobę nieuprawnioną, przetwarzaniem z naruszeniem ustawy oraz zmianą, utratą, uszkodzeniem lub zniszczeniem. Poprzez stwierdzenie „odpowiednie środki techniczne” rozumie się przyjęcie takich rozwiązań, które będą skuteczne, a zatem zapewnią przetwarzanie danych osobowych zgodnie z zasadami ich ochrony, w szczególności w przedmiocie zabezpieczenia danych w sytuacjach wskazanych zarówno w przepisie art. 36 ust. 1, jak i powołanych przepisów karnych ustawy. Z pomocą tych zabezpieczeń administrator danych powinien wyeliminować wystąpienie potencjalnych zagrożeń bądź zminimalizować ryzyko ich wystąpienia. Określone przez administratora danych zasady, środki i rozwiązania organizacyjne mające zapewnić danym bezpieczeństwo muszą być przestrzegane przez wszystkie osoby, które zgodnie z art. 37 ustawy o ochronie danych osobowych, zostały upoważnione do przetwarzania danych przez administratora danych. Tylko bowiem osoby upoważnione mogą mieć dostęp do danych osobowych a jakiegokolwiek udostępnianie tych danych musi również znajdować stosowną podstawę prawną. Dostosowanie środków i rozwiązań służących do przetwarzania danych do wymogów powołanych przepisów leży w gestii administratora danych i powinno uwzględniać sposób przetwarzania danych.

Dlatego należy wskazać, że komendant jako organ zobowiązany do udostępnienia informacji publicznych w trybie ustawy o dostępie do informacji publicznej, w przypadku, gdy informacja należy do informacji prawnie chronionych powinien zachować ją w poufności, do czego wprost zobowiązuje go art. 5 ustawy o dostępie do informacji publicznej.

W związku z powyższym, uprzejmie proszę Pana Generała o podjęcie działań mających na celu zapobieżenie zaistnieniu w przyszłości podobnych przypadków udostępniania danych osobowych osobom nieupoważnionym.

Jednocześnie wskazuję, że zgodnie z art. 19a ust. 3 ustawy o ochronie danych osobowych, podmiot, do którego zostało skierowane wystąpienie lub wnioski, o których mowa w ust. 1 i 2, jest obowiązany ustosunkować się do tego wystąpienia lub wniosku na piśmie w terminie 30 dni od daty jego otrzymania.

Informuję przy tym, iż treść niniejszego wystąpienia wraz z udzieloną odpowiedzią opublikowane będą na stronie internetowej Generalnego Inspektora Ochrony Danych Osobowych www.giodo.gov.pl