



**GENERALNY INSPEKTOR
OCHRONY DANYCH
OSOBOWYCH**

Michał Serzycki

Warszawa, dnia 28 grudnia 2009 r.

DIS/DEC-1327/48391/09

dot. DIS-K-421/25/09

D E C Y Z J A

Na podstawie art. 104 § 1 i art. 105 § 1 ustawy z dnia 14 czerwca 1960 r. Kodeks postępowania administracyjnego (t.j. Dz. U. z 2000 r. Nr 98, poz. 1071 z późn. zm.) oraz art. 12 pkt 2, art. 18 ust. 1 pkt 1, art. 22 w związku z art. 26 ust. 1 pkt 4, art. 36 ust. 1, art. 40, art. 41 ust. 2 ustawy z dnia 29 sierpnia 1997 r. o ochronie danych osobowych (Dz. U. z 2002 r. Nr 101, poz. 926 z późn. zm.), oraz częścią C pkt XIII załącznika do 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. Nr 100, poz. 1024), po przeprowadzeniu postępowania administracyjnego w sprawie przetwarzania danych osobowych przez Spółkę,

I. Nakazuję Spółce usunięcie uchybień w procesie przetwarzania danych osobowych, poprzez:

- 1. Zapewnienie aby dane osób, które zamówiły czasopismo W za pośrednictwem strony internetowej A lub zarejestrowały się na ww. stronie internetowej (np. w „F”) były przechowywane w postaci uniemożliwiającej identyfikację osób, których dotyczą, po osiągnięciu celów przetwarzania, w terminie 14 dni od dnia, w którym niniejsza decyzja stanie się ostateczna.**
- 2. Zastosowanie środków technicznych i organizacyjnych zapewniających ochronę danych osobowych przetwarzanych w systemach informatycznych o nazwach P (służący do przetwarzania danych osób zamawiających prenumeratę czasopisma) i F (służący do**

przetwarzania danych osób rejestrujących się na stronie internetowej Spółki), odpowiednią do zagrożeń oraz kategorii danych objętych ochroną, w szczególności poprzez szyfrowanie danych przesyłanych przez sieć publiczną w ww. systemach w terminie 14 dni od dnia, w którym niniejsza decyzja stanie się ostateczna.

3. Zastosowanie środków kryptograficznej ochrony wobec danych wykorzystywanych do uwierzytelnienia do systemów informatycznych o nazwach: F oraz P, które są przesyłane w sieci publicznej za pośrednictwem strony internetowej A w terminie 14 dni od dnia, w którym niniejsza decyzja stanie się ostateczna.
4. Zgłoszenie zbioru danych osób zamawiających wiadomości newsletter za pośrednictwem strony internetowej A do rejestracji Generalnemu Inspektorowi Ochrony Danych Osobowych na formularzu „Zgłoszenie zbioru danych do rejestracji Generalnemu Inspektorowi Ochrony Danych Osobowych” stanowiącym załącznik do rozporządzenia Ministra Spraw Wewnętrznych i Administracji z dnia 11 grudnia 2008 r. w sprawie wzoru zgłoszenia zbioru danych do rejestracji Generalnemu Inspektorowi Ochrony Danych Osobowych (Dz. U. z 2008 r. nr 229, poz. 1536), w terminie od dnia, w którym niniejsza decyzja stanie się ostateczna.

II. W pozostałym zakresie postępowanie umarzam.

Uzasadnienie

Inspektorzy upoważnieni przez Generalnego Inspektora Ochrony Danych Osobowych przeprowadzili w Spółce kontrolę zgodności przetwarzania danych osobowych z przepisami o ochronie danych osobowych (sygn. DIS-K-421/25/09), tj. ustawą z dnia 29 sierpnia 1997 r. o ochronie danych osobowych (Dz. U. z 2002 r. Nr 101, poz. 926 z późn. zm.), zwaną dalej ustawą, oraz rozporządzeniem 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. Nr 100, poz. 1024), zwanym dalej rozporządzeniem. W toku kontroli odebrano od pracowników Spółki ustne wyjaśnienia, skontrolowano systemy informatyczne oraz dokonano oględzin pomieszczeń, w których odbywa się przetwarzanie danych osobowych. Stan faktyczny został szczegółowo opisany w protokole kontroli, który został podpisany przez Prezesa Zarządu Spółki.

Na podstawie tak zgromadzonego materiału dowodowego ustalono, że w procesie przetwarzania danych osobowych Spółka naruszyła przepisy o ochronie danych osobowych. Uchybienia te polegały na:

1. Niezapewnieniu aby dane osób, które zamówiły czasopismo W za pośrednictwem strony internetowej A lub zarejestrowały się na ww. stronie internetowej (np. w „F”) były przechowywane w postaci umożliwiającej identyfikację osób, których dotyczą, nie dłużej niż jest to niezbędne do osiągnięcia celu przetwarzania (art. 26 ust. 1 pkt 4 ustawy).
2. Niezastosowaniu środków technicznych i organizacyjnych zapewniających ochronę danych osobowych przetwarzanych w systemach informatycznych o nazwach P (służący do przetwarzania danych osób zamawiających prenumeratę czasopisma) i F (służący do przetwarzania danych osób rejestrujących się na stronie internetowej Spółki), odpowiednią do zagrożeń oraz kategorii danych objętych ochroną w szczególności poprzez szyfrowanie danych przesyłanych przez sieć publiczną (art. 36 ust. 1 ustawy).
3. Niezastosowaniu środków kryptograficznej ochrony wobec danych wykorzystywanych do uwierzytelnienia do systemów informatycznych: F oraz P, które są przesyłane w sieci publicznej za pośrednictwem strony internetowej A (część C pkt XIII załącznika do rozporządzenia).
4. Niezgłoszeniu zbioru danych osób zamawiających wiadomości newsletter za pośrednictwem strony internetowej A do rejestracji Generalnemu Inspektorowi Ochrony Danych Osobowych (art. 40 ustawy).
5. Niezgłoszeniu Generalnemu Inspektorowi Ochrony Danych Osobowych aktualizacji zbioru danych o nazwie „Baza klientów Działu” (art. 41 ust. 2 ustawy).

W związku z powyższym, Generalny Inspektor Ochrony Danych Osobowych wszczął z urzędu postępowanie administracyjne (sygn. DIS-K-421/25/09/28828), w celu wyjaśnienia okoliczności sprawy.

W odpowiedzi na zawiadomienie o wszczęciu postępowania administracyjnego Spółka pismem z dnia 18 sierpnia 2009 r. złożyła wyjaśnienia, w których poinformowała, że:

1. Określono sześcioletni termin przechowywania przetwarzanych danych osobowych.
2. Spółka wdrożyła system szyfrowania połączeń i transferu danych.
3. Dokonała aktualizacji zgłoszonego zbioru danych „Baza klientów działu”.
4. Zgłoszona aktualizacja obejmuje także zgłoszenie zbioru adresów e-mail użytkowników newsletterów.

Ponadto, do ww. pisma załączono kopię zgłoszenia zmian w zbiorze danych o nazwie „Baza klientów Działu”.

Po zapoznaniu się z całością materiału dowodowego zebranego w sprawie Generalny Inspektor Ochrony Danych Osobowych zważył co następuje:

Zgodnie z art. 26 ust. 1 pkt 4 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: przechowywane w postaci umożliwiającej identyfikację osób, których dotyczą, nie dłużej niż jest to niezbędne do osiągnięcia celu przetwarzania.

W toku kontroli ustalono, iż dane osób zamawiających czasopismo W za pośrednictwem strony internetowej A, są przetwarzane w celu realizacji zamówienia prenumeraty, a także w celu marketingowym, jeżeli osoba wyrazi zgodę na przetwarzanie danych w tym celu. Ponadto, dane są przetwarzane w związku z realizacją przepisów ustawy z dnia 29 września 1994 r. o rachunkowości (tekst jednolity: Dz. U. 2002 r. Nr 76 poz. 694 z późn. zm.). Ww. dane są przechowywane bezterminowo i są gromadzone od 1993 r. Dane nie były dotychczas usuwane.

W toku kontroli ustalono, iż dane osób rejestrujących się na stronie internetowej A są przetwarzane m.in. w celu marketingowym, jeżeli osoba wyrazi zgodę na przetwarzanie danych w tym celu. Ww. dane są przechowywane bezterminowo i są gromadzone od 2001 r. Dane nie były dotychczas usuwane.

Pismem z dnia z dnia 18 sierpnia 2009 r. Spółka złożyła wyjaśnienia, w których poinformowała, że został określony sześcioletni termin przetwarzania danych osób zamawiających czasopisma i rejestrujących się na stronie internetowej A.

Z uwagi na to, iż w toku prowadzonego postępowania Spółka nie wyjaśniła czy dane osób, które zamówiły czasopismo W za pośrednictwem strony internetowej A lub zarejestrowały się na ww. stronie internetowej są przechowywane w postaci uniemożliwiającej ich identyfikację po osiągnięciu celów przetwarzania danych (np. zakończenia prenumeraty, upływu terminów określonych w przepisach prawa do przechowywania danych osobowych), tj. po upływie okresu sześciu lat, uznać należy, iż w tym zakresie przedmiotowe uchybienie nie zostało usunięte.

Zgodnie z art. 36 ust. 1 ustawy administrator danych jest obowiązany zastosować środki techniczne i organizacyjne zapewniające ochronę przetwarzanych danych osobowych odpowiednią 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.

W toku czynności kontrolnych ustalono, że zastosowane środki mające służyć ochronie danych nie spełniają wymogów technicznych i organizacyjnych jakim powinny odpowiadać urządzenia i systemy informatyczne służące do przetwarzania danych osobowych określone w rozporządzeniu. Nie są szyfrowane dane przesyłane przez sieć publiczną w systemach informatycznych o nazwach: P (służący do przetwarzania danych osób zamawiających prenumeratę czasopisma) i F (służący do przetwarzania danych osób rejestrujących się na stronie internetowej Spółki).

Pismem z dnia z dnia 18 sierpnia 2009 r. Spółka złożyła wyjaśnienia, w których poinformowała, że wdrożono system szyfrowania połączeń i transferu danych. Z uwagi na to, iż Spółka nie przesłała żadnych dowodów potwierdzających złożone wyjaśnienia uznać należy, iż ww. uchybienie nie zostało usunięte.

Zgodnie z częścią C pkt XIII załącznika do rozporządzenia, administrator danych stosuje środki kryptograficznej ochrony wobec danych wykorzystywanych do uwierzytelnienia, które są przesyłane w sieci publicznej.

W toku czynności kontrolnych ustalono, że Spółka nie stosuje środków kryptograficznej ochrony wobec danych wykorzystywanych do uwierzytelnienia do systemu informatycznego o nazwie Forum oraz systemu informatycznego o nazwie P, które są przesyłane w sieci publicznej za pośrednictwem strony internetowej A.

Pismem z dnia 18 sierpnia 2009 r. Spółka złożyła wyjaśnienia, w których poinformowała, że wdrożono system szyfrowania połączeń i transferu danych. Z uwagi na to, iż Spółka nie przesłała żadnych dowodów potwierdzających złożone wyjaśnienia uznać należy, iż ww. uchybienie nie zostało usunięte.

Zgodnie z art. 40 ustawy administrator danych jest obowiązany zgłosić zbiór danych do rejestracji Generalnemu Inspektorowi, z wyjątkiem przypadków, o których mowa w art. 43 ust. 1 ustawy. Natomiast zgodnie z art. 7 pkt 1 ustawy ilekroć w ustawie jest mowa o zbiorze danych rozumie się przez to każdy posiadający strukturę zestaw danych o charakterze osobowym, dostępnych według określonych kryteriów, niezależnie od tego, czy zestaw ten jest rozproszony lub podzielony funkcjonalnie.

W toku kontroli ustalono, iż za pośrednictwem strony internetowej A istnieje możliwość podania adresu e-mail w celu otrzymywania od Spółki wiadomości newsletter. Adres ten jest podawany dobrowolnie przez osoby zainteresowane otrzymywaniem bezpłatnych treści redakcyjnych np. aktualności W. Otrzymywanie newslettera nie jest związane z rejestracją użytkownika w serwisie A. Jak ustalono w toku kontroli baza newsletterów nie jest połączona z bazą danych osób zarejestrowanych w serwisie i z bazą prenumeratorów. Zbiór adresów e-mail zarządzany jest przez system informatyczny D. Adresy te wykorzystywane są do wysyłania zamówionych informacji prasowych. Podstawą prawną przetwarzania ww. danych jest art. 23 ust. 1 pkt 5 ustawy, tj. gdy jest to niezbędne dla wypełniania prawnie usprawiedliwionych celów realizowanych przez administratorów danych albo odbiorców danych, a przetwarzanie nie narusza praw i wolności osoby, której dane dotyczą. Ww. adresy nie są udostępniane podmiotom zewnętrznym.

Wobec powyższego uznać należy, że adresy e-mail pozyskiwane za pośrednictwem strony internetowej A w celu otrzymywania wiadomości newsletter stanowią zbiór danych w rozumieniu

art. 7 pkt 1 ustawy, jednocześnie nie zachodzą przesłanki wskazane w art. 43 ust. 1 ustawy, zwalniające z obowiązku zgłoszenia zbioru do rejestracji Generalnemu Inspektorowi.

Pismem z dnia 18 sierpnia 2009 r. Spółka złożyła wyjaśnienia, w których poinformowała, że aktualizacja zbioru danych o nazwie „Baza klientów Działu” obejmuje także zgłoszenie zbioru adresów e-mail użytkowników newsletterów.

Z ww. wyjaśnień oraz z przesłanego przez Spółkę formularza „Zgłoszenia zbioru danych do rejestracji Generalnemu Inspektorowi Ochrony Danych Osobowych” dotyczącego wprowadzenia zmian w zbiorze danych o nazwie „Baza klientów Działu” wynika, iż Spółka złożyła na ww. formularzu dwa wnioski dotyczące: zgłoszenia zbioru danych osób zamawiających wiadomości newsletter, za pośrednictwem strony internetowej A oraz zgłoszenia zmian w zbiorze danych o nazwie „Baza klientów Działu”.

Zgodnie z art. 41 ustawy zgłoszenie zbioru danych do rejestracji powinno zawierać: 1) wniosek o wpisanie zbioru do rejestru zbiorów danych osobowych, 2) oznaczenie podmiotu prowadzącego zbiór i adres jego siedziby lub miejsca zamieszkania, w tym numer identyfikacyjny rejestru podmiotów gospodarki narodowej, jeżeli został mu nadany, oraz podstawę prawną upoważniającą do prowadzenia zbioru, a w przypadku podmiotu, o którym mowa w art. 31a, oznaczenie tego podmiotu i adres jego siedziby lub miejsce zamieszkania, 3) cel przetwarzania danych, 3a) opis kategorii osób, których dane dotyczą, oraz zakres przetwarzanych danych, 4) sposób zbierania oraz udostępniania danych, 4a) informację o odbiorcach lub kategoriach odbiorców, którym dane mogą być przekazywane, 5) opis środków technicznych i organizacyjnych zastosowanych w celach określonych w art. 36-39, 6) informację o sposobie wypełnienia warunków technicznych i organizacyjnych, określonych w przepisach, o których mowa w art. 39a, 7) informację dotyczącą ewentualnego przekazywania danych do państwa trzeciego (ust.1). Administrator danych jest obowiązany zgłaszać Generalnemu Inspektorowi każdą zmianę informacji, o której mowa w ust. 1, w terminie 30 dni od dnia dokonania zmiany w zbiorze danych. Do zgłaszania zmian stosuje się odpowiednio przepisy o rejestracji zbiorów danych (ust.2).

Z treści ww. przepisu wnika w szczególności co powinno zawierać zgłoszenie zbioru do rejestracji oraz, że zgłoszenie to może dotyczyć tylko jednego zbioru danych. Z uwagi na to, iż zbiór danych osób zamawiających wiadomości newsletter, za pośrednictwem strony internetowej A jest zbiorem odrębnym, który nie jest połączony z innym zbiorem danych, i w którym dane osobowe są przetwarzane na osobnej podstawie prawnej, Spółka jest zobowiązana zgłosić ten zbiór na **odrębnym formularzu** „Zgłoszenie zbioru danych do rejestracji Generalnemu Inspektorowi Ochrony Danych Osobowych” stanowiącym załącznik do rozporządzenia Ministra Spraw Wewnętrznych i Administracji z dnia 11 grudnia 2008 r. w sprawie wzoru zgłoszenia zbioru danych

do rejestracji Generalnemu Inspektorowi Ochrony Danych Osobowych (Dz. U. z 2008 r. nr 229, poz. 1536).

Stosownie do art. 105 § 1 Kodeksu postępowania administracyjnego, gdy postępowanie z jakiegokolwiek przyczyny stało się bezprzedmiotowe, organ administracji publicznej wydaje decyzję o jego umorzeniu. Przesłanką umorzenia postępowania na podstawie art. 105 § 1 k.p.a. jest bezprzedmiotowość postępowania „z jakiegokolwiek przyczyny”, czyli każdej przyczyny powodującej brak jednego z elementów materialnoprawnego stosunku prawnego w odniesieniu do jego strony podmiotowej lub przedmiotowej (wyrok NSA z 21 stycznia 1999 r. S.A./Sz 1029/97).

W toku postępowania Spółka usunęła pozostałe uchybienia w procesie przetwarzania danych osobowych, stanowiące przedmiot postępowania, poprzez:

1. Określenie terminu przetwarzania danych osób zamawiających czasopisma A za pośrednictwem strony internetowej A lub rejestrujących się na tej stronie.
2. Zgłoszenie Generalnemu Inspektorowi Ochrony Danych Osobowych aktualizacji zbioru danych o nazwie „Baza klientów Działu”.

Wobec powyższego, Generalny Inspektor Ochrony Danych Osobowych rozstrzygnął jak w sentencji.

Decyzja jest ostateczna. Na podstawie art. 21 ust. 1 ustawy o ochronie danych osobowych oraz art. 129 § 2 Kodeksu postępowania administracyjnego, strona niezadowolona z niniejszej decyzji może zwrócić się do Generalnego Inspektora Ochrony Danych Osobowych (adres: ul. Stawki 2, 00-193 Warszawa) z wnioskiem o ponowne rozpatrzenie sprawy, w terminie 14 dni od dnia doręczenia niniejszej decyzji.