GENERALNY INSPEKTOR
OCHRONY DANYCH
OSOBOWYCH
dr Wojciech R. Wiewiórowski

Warszawa, dnia 8 kwietnia 2011 r.

DIS/DEC-291/16553/11
dot. […]

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 (Dz. U. z 2000 r., Nr 98, poz. 1071 z późn. zm.), art. 12 pkt 2, art. 18 ust. 1 pkt 1 i art. 22 w związku z art. 7 pkt 5, art. 23 ust. 1 pkt 1, art. 24 ust. 1 pkt 2 i pkt 4, art. 36 ust. 2, art. 38 ustawy z dnia 29 sierpnia 1997 r. o ochronie danych osobowych (Dz. U. z 2002 r., Nr 101, poz. 926 z późn. zm.) oraz § 4, częścią A pkt IV ust. 2 zd. 1, częścią A pkt V, częścią B pkt VIII, 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. z2004 r., Nr 100, poz. 1024), po przeprowadzeniu postępowania administracyjnego w sprawie przetwarzania danych osobowych przez H. Sp. z o.o.,

I. Nakazuję H. Sp. z o.o. usunięcie uchybień w procesie przetwarzania danych osobowych, poprzez:

1) zapewnienie należytej kontroli w zakresie przekazywania danych osobowych pozyskanych z „Ankiet […]", dotyczącej podmiotu, który administruje systemem informatycznym zawierającym wskazane dane oraz fizycznej lokalizacji serwera i bazy danych tego systemu informatycznego, w terminie 30 dni od dnia, w którym niniejsza decyzja stanie się ostateczna,

2) uzupełnienie zawartego w „Polityce bezpieczeństwa danych osobowych Spółki H. Sp. z o.o." wykazu budynków, pomieszczeń lub części pomieszczeń, tworzących obszar, w którym

przetwarzane są dane osobowe oraz wykazu zbiorów danych osobowych wraz ze wskazaniem programów zastosowanych do przetwarzania danych osobowych o informacje dotyczące użytkowanego przez Spółkę systemu informatycznego o nazwie „A" (strony internetowej, za pośrednictwem której Spółka wprowadza dane osobowe z ankiet […]), w terminie 30 dni od dnia, w którym niniejsza decyzja stanie się ostateczna,

3) zmienianie nie rzadziej niż co 30 dni hasła logowania do systemu operacyjnego komputera użytkowanego przez pracownika Działu Rezerwacji, na którym w pliku o lokalizacji […] przetwarzane są ankiety […] zawierające dane osobowe klientów Spółki oraz hasła logowania do systemu informatycznego o nazwie „A" (strony internetowej, za pośrednictwem której Spółka wprowadza dane osobowe z wypełnionych przez klientów „Ankiet […]"), w terminie 30 dni od dnia, w którym niniejsza decyzja stanie się ostateczna,

4) zastosowanie środków ochrony kryptograficznej wobec danych zapisywanych w pliku o formacie „.pst" na dysku twardym komputera przenośnego, użytkowanego przez Prezesa Zarządu Spółki, nadesłane na elektroniczną skrzynkę pocztową o adresie: […] wraz z załączonymi plikami („Ankietami […]"), w terminie 30 dni od dnia, w którym niniejsza decyzja stanie się ostateczna,

5) zabezpieczenie za pomocą środków ochrony kryptograficznej teletransmisji danych przesyłanych przez Spółkę za pośrednictwem publicznej sieci internet do systemu informatycznego o nazwie „A" (strony internetowej, za pośrednictwem której Spółka wprowadza dane osobowe z ankiet […]), w terminie 30 dni od dnia, w którym niniejsza decyzja stanie się ostateczna.

II. W pozostałym zakresie postępowanie umarzam.

U z a s a d n i e n i e

Inspektorzy upoważnieni przez Generalnego Inspektora Ochrony Danych Osobowych przeprowadzili kontrolę sygn. akt […] w H. Sp. z o.o. (dalej: Spółka), w celu ustalenia zgodności przetwarzania danych osobowych z przepisami o ochronie danych osobowych, 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 pełnomocnika Spółki. Na podstawie tak zgromadzonego materiału dowodowego ustalono, że w procesie przetwarzania danych osobowych, H. Sp. z o.o. jako administrator danych, naruszyła przepisy o ochronie danych osobowych. Uchybienia te polegały na tym, że:

1) sposób sformułowania klauzuli zawierającej oświadczenie o wyrażeniu zgody na przetwarzanie danych osobowych przez Spółkę jak i R., a w szczególności na „prowadzenie ewidencji osobowej w celach marketingowych, w tym sprzedaży usług turystycznych i towarzyszących" oraz w celu „udostępniania danych osobowych podmiotom gospodarczym branży turystycznej i organizacjom turystycznym, w szczególności do dokonania rezerwacji w ośrodku […]", nie zapewniał osobie wypełniającej ten formularz opcjonalność w kwestii wyboru podmiotu przetwarzającego dane jak i celu przetwarzania danych (art. 23 ust. 1 pkt 1, art. 7 pkt 5 ustawy),

2) klienci, którzy wzięli udział w prezentacji organizowanej przez Spółkę i zdecydowali się na wzięcie udziału w wyjeździe testowym na […] do jednego z ośrodków prowadzonych przez C., nie byli informowani, podanie których danych w „Ankiecie […]" jest dobrowolne (nie wynika to także z umowy zawartej przez Spółkę z C.; ponadto, klienci nie byli informowani, iż dane będą przekazywane C. (art. 24 ust. 1 pkt 2 i pkt 4 ustawy),

3) „Polityka bezpieczeństwa danych osobowych Spółki H." nie zawiera informacji dotyczących użytkowanego przez Spółkę systemu informatycznego o nazwie „A" (strony internetowej, za pośrednictwem której Spółka wprowadza dane osobowe z ankiet […]); na stronie 3 zawierała informacje niezgodne ze stanem faktycznym, tj. w punkcie […] Spółka wskazała, że dostęp do skrzynki mailowej, do której klienci Spółki wysyłają ankiety […], posiada jedynie Kierownik Działu Rezerwacji, gdyż dostęp do ww. skrzynki pocztowej posiadają trzy osoby (art. 36 ust. 2 ustawy w związku z § 4 rozporządzenia),

4) kontrolowana jednostka nie zapewniła należytej kontroli w zakresie, komu dane osobowe są przekazywane, gdyż Pan P. M. prowadzący działalność gospodarczą pod nazwą „I", świadczący usługi informatyczne dla Spółki, w tym, nadzorujący proces przetwarzania w postaci elektronicznej danych osobowych pozyskiwanych za pośrednictwem „Ankiety […]", nie posiadał wiedzy w zakresie wskazania fizycznej lokalizacji serwera oraz bazy danych systemu informatycznego (zawierającej dane osobowe pozyskane z ankiet […]) oraz podmiotu, który administruje ww. systemem informatycznym (art. 38 ustawy),

5) hasło logowania do systemu operacyjnego komputera użytkowanego przez Pana S. N. - pracownika Działu […], na którym w pliku o lokalizacji […] przetwarzane są ankiety […]

zawierające dane osobowe klientów Spółki oraz hasło logowania do systemu informatycznego o nazwie „A" (strony internetowej, za pośrednictwem której Spółka wprowadza dane osobowe z wypełnionych przez klientów „Ankiet […]"), nie były zmieniane co najmniej raz na 30 dni (część A pkt IV ust. 2 zd. 1 załącznika do rozporządzenia),

6) hasło logowania do systemu informatycznego o nazwie „A" (strony internetowej, za pośrednictwem której Spółka wprowadza dane osobowe z wypełnionych przez klientów „Ankiet […]") nie składało się co najmniej z 8 znaków, zawierających małe, wielkie litery oraz cyfry lub znaki specjalne (część B pkt VIII załącznika do rozporządzenia),

7) dane zapisane podczas pobierania maili nadesłanych na skrzynkę pocztową o nazwie […] korespondencja elektroniczna wraz z załączonymi plikami („Ankietami […]") zapisywana w pliku o formacie „.pst" na dysku twardym komputera przenośnego, użytkowanego przez Pana A. O. - Prezesa Zarządu Spółki, nie zostały zabezpieczone za pomocą środków kryptograficznej ochrony (część A pkt V załącznika do rozporządzenia),

8) teletransmisja danych przesyłanych przez Spółkę za pośrednictwem publicznej sieci internet do systemu informatycznego o nazwie „A" (strony internetowej, za pośrednictwem której Spółka wprowadza dane osobowe z ankiet […]) nie została zabezpieczona za pomocą środków kryptograficznej ochrony, np. bezpiecznego protokołu https (pkt XIII część C załącznika do rozporządzenia).

W związku z powyższym Generalny Inspektor Ochrony Danych Osobowych wszczął z urzędu postępowanie administracyjne w celu wyjaśnienia okoliczności sprawy (pismo sygn. […].

W odpowiedzi na ww. skierowane pismo informujące o wszczęciu postępowania administracyjnego, pełnomocnik Spółki pismami z dnia […] i […] marca 2011 r. złożył wyjaśnienia w sprawie wskazanych uchybień, informując o następujących okolicznościach:

1) Spółka dokonała zmian w „Ankiecie […]", które objęły treść klauzuli dotyczącej wyrażenia zgody na przetwarzanie danych osobowych oraz zakres pytań, na które odpowiedź jest obowiązkowa,

2) H. Sp. z o.o. dokonała stosownych zmian w Polityce bezpieczeństwa, tak, aby było w niej ujęte korzystanie przez Spółkę z systemu „A" oraz faktyczny krąg osób upoważnionych do dostępu do skrzynki poczty elektronicznej: […],

3) Spółka dostosowała stosowanie haseł do wymogów części B pkt VIII załącznika do rozporządzenia, w tym hasła do systemu informatycznego „A",

4) H. Sp. z o.o. zatrudniła informatyka celem zabezpieczenia za pomocą środków ochrony kryptograficznej danych zapisanych na komputerze przenośnym użytkowanym przez Prezesa Spółki oraz przesyłania danych za pośrednictwem sieci Internet do systemu informatycznego o nazwie „A".

Do pisma z dnia […] marca 2011 r. załączono formularz „Ankiety […]" oraz kopię „Polityki bezpieczeństwa danych osobowych spółki H. Sp. z o.o."

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

Zgodnie z art. 36 ust. 2 ustawy, administrator danych prowadzi dokumentację opisującą sposób przetwarzania danych oraz środki, o których mowa w ust. 1. W myśl § 3 ust. 1 rozporządzenia, na dokumentację, o której mowa w § 1 pkt 1, składa się polityka bezpieczeństwa i instrukcja zarządzania systemem informatycznym służącym do przetwarzania danych osobowych, zwana dalej „instrukcją. Zgodnie z ust. 2, dokumentację, o której mowa w § 1 pkt 1, prowadzi się w formie pisemnej. Natomiast, zgodnie z ust. 3, dokumentację, o której mowa w § 1 pkt 1, wdraża administrator danych.

Stosownie do § 4 pkt 1 i pkt 2 rozporządzenia, polityka bezpieczeństwa, o której mowa w § 3 ust. 1, zawiera w szczególności: wykaz budynków, pomieszczeń lub części pomieszczeń, tworzących obszar, w którym przetwarzane są dane osobowe; wykaz zbiorów danych osobowych wraz ze wskazaniem programów zastosowanych do przetwarzania tych danych.

W toku czynności kontrolnych ustalono, że kontrolowana jednostka opracowała i wdrożyła dokumentację stanowiącą politykę bezpieczeństwa oraz instrukcję zarządzania systemem informatycznym służącym do przetwarzania danych osobowych. Stwierdzono, że „Polityka bezpieczeństwa danych osobowych Spółki H." nie zawiera informacji dotyczących użytkowanego przez Spółkę systemu informatycznego o nazwie A" (strony internetowej, za pośrednictwem której Spółka wprowadza dane osobowe z ankiet […]). W piśmie z dnia z dnia […] marca 2011 r. Spółka wyjaśniła, że dokonała stosownych zmian w polityce bezpieczeństwa, w zakresie dotyczącym systemu informatycznego o nazwie „A" oraz zakresie dotyczącym osób upoważnionych do dostępu do skrzynki pocztowej […]. Analiza polityki bezpieczeństwa, potwierdziła, że Spółka dokonała właściwej korekty osób upoważnionych do dostępu do skrzynki pocztowej […]. Z analizy polityki bezpieczeństwa wynika również, w odniesieniu do systemu informatycznego o nazwie „A", iż wypełniony został wymóg, o którym mowa w §4 pkt 3, pkt 4, pkt 5 rozporządzenia. Jednak w odniesieniu do wymogu, o którym mowa w § 4 pkt 1, pkt 2 rozporządzenia należy stwierdzić, że zawarty w ww. dokumencie wykaz budynków, pomieszczeń lub części pomieszczeń, tworzących

obszar, w którym przetwarzane są dane osobowe, nie uwzględnia systemu informatycznego o nazwie A" (w szczególności miejsca lokalizacji bazy danych ww. systemu informatycznego), a także, iż wykaz zbiorów danych osobowych wraz ze wskazaniem programów zastosowanych do przetwarzania danych osobowych nie uwzględnia systemu informatycznego o nazwie „A".

Zgodnie z art. 38 ustawy, administrator danych jest obowiązany zapewnić kontrolę nad tym, jakie dane osobowe, kiedy i przez kogo zostały do zbioru wprowadzone oraz komu są przekazywane.

W toku czynności kontrolnych ustalono, że P. P. M. w zakresie prowadzonej działalności gospodarczej pod nazwą „I", świadczy usługi informatyczne dla Spółki, w tym, nadzoruje proces przetwarzania w postaci elektronicznej danych osobowych pozyskiwanych za pośrednictwem „Ankiety […]". Jak wynika z ustaleń kontroli, P. P. M. nie posiada wiedzy w zakresie fizycznej lokalizacji serwera oraz bazy danych ww. systemu informatycznego (zawierającej dane osobowe pozyskane z ankiet […]) oraz podmiotu, który administruje ww. systemem informatycznym. Przesłane przez Spółkę wyjaśnienia oraz załączone dowody nie potwierdzają, aby uchybienie w tym zakresie zostało usunięte. Mając na uwadze powyższe, należy stwierdzić, że kontrolowana jednostka nie zapewniła należytej kontroli w zakresie komu dane osobowe są przekazywane.

Zgodnie z częścią A pkt IV ust. 2 zd. 1 załącznika do rozporządzenia, w przypadku, gdy do uwierzytelniania użytkowników używa się hasła, jego zmiana następuje nie rzadziej niż co 30 dni.

W związku z przetwarzaniem przez Spółkę danych z wykorzystaniem publicznej sieci internet powinny być zastosowane środki bezpieczeństwa na poziomie wysokim. W toku czynności kontrolnych ustalono, że zmiana hasła logowania do systemu informatycznego o nazwie „A" (strony internetowej, za pośrednictwem której Spółka wprowadza dane osobowe z wypełnionych przez klientów ankiet […]) następuje rzadziej niż co 30 dni.

W myśl wymogu zawartego w części A pkt V załącznika do rozporządzenia, osoba użytkująca komputer przenośny zawierający dane osobowe zachowuje szczególną ostrożność podczas jego transportu, przechowywania i użytkowania poza obszarem, o którym mowa w § 4 pkt 1 rozporządzenia, w tym stosuje środki ochrony kryptograficznej wobec przetwarzanych danych osobowych.

Ustalono, że podczas pobierania maili nadesłanych na skrzynkę pocztową o nazwie […], korespondencja elektroniczna wraz z załączonymi plikami („Ankietami […]") zapisywana jest w pliku o formacie „.pst" na dysku twardym komputera lokalnego, użytkowanego przez pracownika Działu […], oraz na dysku twardym komputera przenośnego, użytkowanego przez Prezesa Zarządu Spółki. Dane zapisane na komputerze przenośnym, użytkowanym przez Prezesa Zarządu Spółki, nie zostały zabezpieczone za pomocą środków kryptograficznej ochrony.

Stosownie do pkt XIII części C załącznika do rozporządzenia, administrator danych obowiązany jest zabezpieczyć teletransmisję danych, w tym stosować środki kryptograficznej ochrony wobec danych wykorzystywanych do uwierzytelnienia, które są przesyłane w sieci publicznej.

W toku postępowania ustalono, że teletransmisja danych przesyłanych przez Spółkę za pośrednictwem publicznej sieci internet do systemu informatycznego o nazwie „A" (strony internetowej, za pośrednictwem której Spółka wprowadza dane osobowe z ankiet […]) nie została zabezpieczona za pomocą środków kryptograficznej ochrony, np. bezpiecznego protokołu https.

Ze złożonych przez H. Sp. z o.o. wyjaśnień w piśmie z dnia […] marca 2011 r. wynika, że Spółka zatrudniła informatyka celem dokonania przez niego prac polegających na zabezpieczeniu laptopa oraz teletransmisji danych za pomocą środków kryptograficznej ochrony. Wyjaśnienia w tym zakresie nie potwierdzają jednak, iż został przywrócony stan zgodny z prawem.

Stosownie do art. 105 § 1 Kodeksu postępowania administracyjnego, gdy postępowanie z jakiejkolwiek 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 jakiejkolwiek przyczyny", czyli z 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./Sz1029/97).

Na podstawie całokształtu materiału dowodowego należy uznać, iż w toku postępowania administracyjnego zostały usunięte pozostałe uchybienia w procesie przetwarzania danych osobowych, stanowiące przedmiot postępowania, poprzez:

1) zmodyfikowanie klauzuli o wyrażeniu zgody na przetwarzanie danych osobowych,

2) realizację obowiązku informacyjnego, o którym mowa w art. 24 ust. 1 pkt 2 i pkt 4 ustawy, tj. o odbiorcach danych i o dobrowolności podania danych,

3) uzupełnienie „Polityki bezpieczeństwa danych osobowych Spółki H." o informacje o osobach upoważnionych do dostępu do skrzynki pocztowej […], 4) uzupełnienie Polityki bezpieczeństwa danych osobowych Spółki H." o informacje dotyczące systemu informatycznego o nazwie „A" w zakresie, o którym mowa w § 4 pkt 3, pkt 4, pkt 5 rozporządzenia, tj. opisu struktury zbiorów danych wskazujący zawartość poszczególnych pól informacyjnych i powiązania między nimi, sposobu przepływu danych pomiędzy poszczególnymi systemami, określenia środków technicznych i organizacyjnych niezbędnych dla zapewnienia poufności, integralności i rozliczalności przetwarzanych danych,

5) dostosowanie haseł wykorzystywanych w procesie logowania do systemu operacyjnego użytkowanego przez pracownika Działu […] komputera, na którym w pliku o lokalizacji […] przetwarzane są „Ankiety […]" zawierające dane osobowe klientów Spółki, do wymogu, o którym mowa w części B pkt VIII załącznika do rozporządzenia, tj. składają się co najmniej z 8 znaków, zawierają małe i wielkie litery oraz cyfry lub znaki specjalne.

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.