



**GENERALNY INSPEKTOR
OCHRONY DANYCH
OSOBOWYCH**

Michał Serzycki

Warszawa, dnia 27 maja 2009 r.

DIS-DEC-444/19255/09

dot. DIS-K-421/39/09

D E C Y Z J A

Na podstawie art. 104 § 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. 23 ust. 1 pkt 1, art. 24 ust. 1, art. 36 ust. 1 i 2, art. 38 i 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 A pkt IV ust. 2, częścią B pkt VIII i 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 H.,

I. Nakazuję H jako administratorowi danych, usunięcie uchybień w procesie przetwarzania danych osobowych, poprzez:

- 1. Przetwarzanie danych osobowych pozyskanych przez H za pośrednictwem infolinii, na podstawie zgody wyrażonej przez osoby, których dane dotyczą, w terminie miesiąca od dnia, w którym niniejsza decyzja stanie się ostateczna.**
- 2. Dopełnienie wobec osób, których dane osobowe H pozyskał za pośrednictwem infolinii, obowiązku informacyjnego wskazanego w art. 24 ust. 1 ustawy o ochronie danych osobowych, w terminie miesiąca od dnia, w którym niniejsza decyzja stanie się ostateczna.**
- 3. Zabezpieczenie za pomocą środków kryptograficznej ochrony teletransmisji danych osobowych przesyłanych przez klientów H do systemu informatycznego o nazwie CRM, za pośrednictwem formularzy znajdujących się na stronie internetowej o adresie w terminie miesiąca od dnia, w którym niniejsza decyzja stanie się ostateczna.**

- 4. Zabezpieczenie za pomocą środków kryptograficznej ochrony** teletransmisji danych osobowych przesyłanych pomiędzy serwerem systemu informatycznego o nazwie „Faktury H” a Biurami Sprzedaży H. w terminie miesiąca od dnia, w którym niniejsza decyzja stanie się ostateczna.
- 5. Uzupełnienie polityki bezpieczeństwa o zgodne ze stanem faktycznym następujące elementy:** 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 terminie miesiąca od dnia, w którym niniejsza decyzja stanie się ostateczna.
- 6. Uwzględnienie w polityce bezpieczeństwa informacji dotyczących systemów informatycznych o nazwach:** „Faktury H.”, „Symfonia”, „Navision” oraz „TRX”, w terminie miesiąca od dnia, w którym niniejsza decyzja stanie się ostateczna.
- 7. Zapewnienie kontroli nad tym, jakie dokumenty zawierające dane osobowe są przekazywane między Biurem Sprzedaży Spółki a zakładem głównym Spółki** w terminie 14 dni od dnia, w którym niniejsza decyzja stanie się ostateczna.
- 8. Dokonanie aktualizacji zgłoszenia zbioru danych osobowych o nazwie „H”** (zgłoszenie nr R 002084/07), w zakresie zmienionej firmy administratora danych, w terminie 14 dni od dnia, w którym niniejsza decyzja stanie się ostateczna.
- 9. Zapewnienie, aby hasła służące uwierzytelnianiu dostępu użytkowników do systemów informatycznych o nazwach:** „TRX”, „Faktury H.” oraz „CRM”, były zmieniane nie rzadziej niż co 30 dni, w terminie miesiąca od dnia, w którym niniejsza decyzja stanie się ostateczna.
- 10. Zapewnienie, aby hasła służące uwierzytelnianiu dostępu użytkownikom do systemów informatycznych o nazwach:** „Faktury H.” oraz „CRM” składały się co najmniej z 8 znaków, w terminie miesiąca od dnia, w którym niniejsza decyzja stanie się ostateczna.
- 11. Zastosowanie środków kryptograficznej ochrony wobec danych, które są przesyłane w sieci publicznej, wykorzystywanych do uwierzytelnienia w systemie informatycznym o nazwie „Faktury H.”,** w terminie miesiąca od dnia, w którym niniejsza decyzja stanie się ostateczna.

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

Inspektorzy upoważnieni przez Generalnego Inspektora Ochrony Danych Osobowych, przeprowadzili kontrolę (sygn. DIS-K-421/39/09) w H. (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 również 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 również 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 osoby reprezentujące Spółkę.

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

1. Przetwarzaniu bez podstawy prawnej danych osobowych pozyskanych przez H. za pośrednictwem infolinii (art. 23 ust. 1 ustawy).
2. Niedopełnieniu wobec osób, których dane osobowe H. pozyskała za pośrednictwem infolinii, obowiązku informacyjnego, wskazanego w art. 24 ust. 1 ustawy o ochronie danych osobowych.
3. Niezabezpieczeniu za pomocą środków kryptograficznej ochrony teletransmisji danych osobowych przesyłanych przez klientów H. do systemu informatycznego o nazwie „CRM”, za pośrednictwem ogólnie dostępnych formularzy znajdujących się na stronie internetowej o adresie (art. 36 ust. 1 ustawy).
4. Niezabezpieczeniu za pomocą środków kryptograficznej ochrony teletransmisji danych przesyłanych pomiędzy serwerem systemu informatycznego o nazwie „Faktury H.” a Biurami Sprzedaży H. (art. 36 ust. 1 ustawy).
5. Nieuwzględnieniu w polityce bezpieczeństwa informacji dotyczących systemów informatycznych o nazwach: „Faktury H.”, „Symfonia”, „Navision” oraz „TRX” (art. 36 ust. 2 ustawy).
6. Nieuzupełnieniu polityki bezpieczeństwa o zgodne ze stanem faktycznym następujące elementy: 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 (art. 36 ust. 2 ustawy).
7. Niedokonaniu aktualizacji zgłoszenia zbioru danych o nazwie „H.” (zgłoszenie nr R 002084/07) w zakresie zmiany firmy administratora danych (art. 41 ust. 2 ustawy).
8. Niezapewnieniu kontroli nad tym, jakie dokumenty są przekazywane między Biurem Sprzedaży Spółki a zakładem głównym Spółki mieszczącym (art. 38 ustawy).

9. Niezapewnieniu, aby hasła służące uwierzytelnianiu dostępu do systemów informatycznych o nazwach: „TRX”, „Faktury H.” oraz „CRM”, zmieniane były nie rzadziej niż co 30 dni (część A pkt IV ust. 2 załącznika do rozporządzenia).
10. Niezapewnieniu, aby hasła służące uwierzytelnianiu dostępu do systemów informatycznych o nazwach: „Faktury H.” oraz „CRM” składały się co najmniej z 8 znaków (część B pkt VIII załącznika do rozporządzenia).
11. Niezastosowaniu środków kryptograficznej ochrony wobec danych, które są przesyłane w sieci publicznej, wykorzystywanych do uwierzytelnienia w systemie informatycznym o nazwie „Faktury H.” (część C pkt XIII załącznika do rozporządzenia).

W związku z powyższym, w dniu 9 kwietnia 2009 r. Generalny Inspektor Ochrony Danych Osobowych, wszczął z urzędu postępowanie administracyjne w niniejszej sprawie w celu wyjaśnienia okoliczności sprawy (sygn. pisma DIS-K-421/39/09/12896), administrator danych został poinformowany o prawie czynnego udziału w każdym stadium postępowania, a przed wydaniem decyzji wypowiedzenia się co do zebranych dowodów i materiałów oraz zgłoszonych żądań. Spółka nie skorzystała z możliwości złożenia wyjaśnień oraz nie przedstawiła dowodów potwierdzających usunięcie wskazanych uchybień.

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

Zgodnie z art. 23 ust. 1 ustawy o ochronie danych osobowych, przetwarzanie danych jest dopuszczalne tylko wtedy, gdy: 1) osoba, której dane dotyczą, wyrazi na to zgodę, chyba że chodzi o usunięcie dotyczących jej danych, 2) jest to niezbędne dla zrealizowania uprawnienia lub spełnienia obowiązku wynikającego z przepisu prawa, 3) jest to konieczne do realizacji umowy, gdy osoba, której dane dotyczą, jest jej stroną lub gdy jest to niezbędne do podjęcia działań przed zawarciem umowy na żądanie osoby, której dane dotyczą, 4) jest niezbędne do wykonania określonych prawem zadań realizowanych dla dobra publicznego, 5) jest to niezbędne dla wypełnienia prawnie usprawiedliwionych celów realizowanych przez administratorów danych albo odbiorców danych, a przetwarzanie nie narusza praw i wolności osoby, której dane dotyczą.

W literaturze podkreśla się, że, „podmiot przetwarzający dane (administrator danych) powinien wykazać się co najmniej jedną z przesłanek, o których mowa w art. 23 ust. 1 ustawy o ochronie danych osobowych, aby jego działanie mogło być uznane za zgodne z prawem (A. Mednis, „Ustawa o ochronie danych osobowych – komentarz”, Warszawa 1999, str. 49).

W toku czynności kontrolnych ustalono, że jednym ze źródeł pozyskiwania przez Spółkę danych osobowych klientów jest infolinia. Dzwoniąc na numer telefonu infolinii (0801 900 200)

osoba zainteresowana zawarciem umowy pośrednictwa może podać dane osobowe w zakresie: imię, nazwisko i numer telefonu. Klient nie wyraża telefonicznie odrębnej zgody na przetwarzanie przez Spółkę dotyczących go danych osobowych.

Przetwarzanie przez Spółkę danych osobowych klientów jest konieczne do realizacji umowy, gdy osoba, której dane dotyczą, jest jej stroną lub gdy jest to niezbędne do podjęcia działań przed zawarciem umowy na żądanie osoby, której dane dotyczą (art. 23 ust. 1 pkt 3 ustawy o ochronie danych osobowych). Pozyskanie danych osobowych potencjalnego klienta Spółki za pośrednictwem infolinii nie jest jednak działaniem niezbędnym do podjęcia działań przed zawarciem umowy pośrednictwa w obrocie nieruchomościami. Ten etap kontaktu z potencjalnym klientem nie zawsze skutkuje podpisaniem ww. umowy. Przesłanką legalizującą przetwarzanie przez H. danych osobowych klientów pozyskanych za pośrednictwem infolinii, powinna być zgoda osoby, której dane dotyczą (art. 23 ust. 1 pkt 1 ustawy o ochronie danych osobowych).

Wobec powyższego, należy uznać, że Spółka przetwarza bez podstawy prawnej dane osób, które podają swoje dane za pośrednictwem infolinii.

Zgodnie z art. 24 ust. 1 ustawy o ochronie danych osobowych, w przypadku zbierania danych osobowych od osoby, której one dotyczą, administrator danych jest obowiązany poinformować tę osobę o: 1) adresie swojej siedziby i pełnej nazwie, a w przypadku gdy administratorem danych jest osoba fizyczna - o miejscu swojego zamieszkania oraz imieniu i nazwisku, 2) celu zbierania danych, a w szczególności o znanych mu w czasie udzielania informacji lub przewidywanych odbiorcach lub kategoriach odbiorców danych, 3) prawie dostępu do treści swoich danych oraz ich poprawiania, 4) dobrowolności albo obowiązku podania danych, a jeżeli taki obowiązek istnieje, o jego podstawie prawnej. Przepisu ust. 1 nie stosuje się, jeżeli: 1) przepis innej ustawy zezwala na przetwarzanie danych bez ujawniania faktycznego celu ich zbierania, 2) osoba, której dane dotyczą, posiada informacje, o których mowa w ust. 1.

W toku postępowania ustalono, że w przypadku pozyskiwania danych osobowych klientów za pośrednictwem infolinii nie jest realizowany przez Spółkę obowiązek informacyjny wynikający z art. 24 ustawy o ochronie danych osobowych.

W związku z powyższym należy stwierdzić, iż Spółka narusza przepisy art. 24 ustawy o ochronie danych osobowych, nie dopełniając obowiązku informacyjnego wobec osób, których dane dotyczą.

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.

Teletransmisja danych osobowych przesyłanych przez klientów H. do systemu informatycznego CRM za pośrednictwem ogólnie dostępnych formularzy znajdujących się na stronie internetowej nie została zabezpieczona za pomocą środków kryptograficznej ochrony (np. protokołu ssl). Podobnie, teletransmisja danych realizowana przez użytkowników systemu informatycznego o nazwie „Faktury H.” pomiędzy serwerem ww. systemu informatycznego a Biurem Sprzedaży nie została zabezpieczona za pomocą środków kryptograficznej ochrony (np. protokołu ssl).

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.

W toku kontroli ustalono, że Spółka opracowała i wdrożyła dokumentację stanowiącą politykę bezpieczeństwa. Należy zauważyć, że przedłożona polityka bezpieczeństwa zawiera informacje, które różnią się od stanu faktycznego stwierdzonego w toku czynności kontrolnych, w szczególności: za niezgodne należy uznać informacje zawarte w pkt. 7.1 ww. dokumentu („wykaz budynków i pomieszczeń”) oraz pkt 7.2 (identyfikacja zbiorów danych osobowych). Ponadto, zauważyć należy, że polityka bezpieczeństwa nie uwzględnia systemów informatycznych o nazwie: „Faktury H.”, „Symfonia”, „Navision” oraz „TRX”.

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.

Jak ustalono w toku postępowania, wymiana korespondencji między zakładem głównym Spółki mieszczącym a Biurem Sprzedaży Spółki, odbywa się za pośrednictwem podmiot świadczącego usługi poczty kurierskiej. Na korespondencję przesyłaną z ww. Biura do zakładu głównego Spółki składają się umowy pośrednictwa, kopie umów przedwstępnych lub umów kupna – sprzedaży, a także faktury VAT. Ww. dokumenty pakowane są do jednej koperty i wysyłane raz dziennie. Koperty oznaczane są wyłącznie informacją dotyczącą adresata oraz rodzaju przesyłanych dokumentów (bez wskazywania konkretnych numerów). Prowadzony przez asystentkę wykaz jest uzupełniany w rubryce „wysłano” o informację o przekazaniu kurierowi jednego egzemplarza

umowy pośrednictwa do centrali Spółki poprzez wpisanie słowa „tak”. Nie jest prowadzony odrębny rejestr zawierający datę wysyłki, ani pokwitowanie odbioru przez kuriera.

W toku czynności kontrolnych ustalono, że nadawca przesyłki nie sprawuje kontroli nad tym, które dokumenty (zawierające dane osobowe konkretnych osób) w danym dniu przekazał do zakładu głównego Spółki. Biuro Sprzedaży Spółki nie dysponuje też, poza ww. wykazem, żadnymi innymi narzędziami, które pozwalałyby dokładnie określić, które dokumenty zostały danego dnia przekazane do zakładu głównego Spółki za pośrednictwem kuriera.

Istotne znaczenie ma również fakt, że w stosunku do korespondencji wychodzącej na zewnątrz Spółki prowadzona jest pocztowa książka nadawcza, do której wpisywana jest korespondencja wychodząca przesyłana listem poleconym. Korespondencja przekazywana drogą pocztową jest odmiennie traktowana, niż korespondencja przekazywana za pośrednictwem kuriera. Tym samym należy uznać, że nieewidencjonowanie tej ostatniej przez Biuro Sprzedaży Spółki stoi w sprzeczności z przytoczonym powyżej art. 38 ustawy, zgodnie z którym administrator danych jest obowiązany zapewnić kontrolę nad tym, jakie dane osobowe, kiedy i przez kogo zostały do zbioru wprowadzone oraz komu są przekazywane.

Zgodnie z art 41 ust. 2 ustawy o ochronie danych osobowych, administrator jest obowiązany zgłaszać Generalnemu Inspektorowi Ochrony Danych Osobowych każdą zmianę informacji, o której mowa w ust. 1 tego artykułu.

Zbiór danych osobowych klientów Spółki w dniu 13 czerwca 2007 r. został zgłoszony do rejestracji Generalnemu Inspektorowi Ochrony danych Osobowych, gdy Spółka działała pod firmą „J” która została później zmieniona na „H.” Pomimo tego, iż Postanowieniem z dnia 7 sierpnia 2008 r. Sądu Rejonowego, XII Wydział Gospodarczy Krajowego Rejestru Sądowego została zmieniona firma Spółki z „J” na „H” Spółka nie zaktualizowała informacji podanych w zgłoszeniu zbioru danych o nazwie „H” i tym samym nie dopełniła obowiązku wynikającego z art. 41 ust. 2 ustawy o ochronie danych osobowych.

Zgodnie z częścią A pkt IV ust. 2 załącznika do rozporządzenia, w przypadku, gdy do uwierzytelniania użytkowników używa się hasła, jego zmiana następuje nie rzadziej niż co 30 dni. Hasło składa się z co najmniej 6 znaków.

W toku czynności kontrolnych ustalono, że hasło uwierzytelnienia użytkowników do systemów informatycznych o nazwie: „TRX”, „H” oraz „CRM” zmieniane jest rzadziej niż co 30 dni.

Zgodnie z częścią C pkt XIII załącznika do rozporządzenia (Dz. U. z 2004 r. Nr 100, poz. 1024), administrator danych stosuje środki kryptograficznej ochrony wobec danych wykorzystywanych do uwierzytelnienia, które są przesyłane w sieci publicznej.

W toku czynności kontrolnych ustalono, że w odniesieniu do systemu informatycznego „Faktury H.” administrator danych nie zastosował środków kryptograficznej ochrony wobec danych wykorzystywanych do uwierzytelnienia, które są przesyłane w sieci publicznej.

Zgodnie z częścią B pkt VIII załącznika do rozporządzenia, w przypadku, gdy do uwierzytelniania użytkowników używa się hasła, składa się ono co najmniej z 8 znaków, zawiera małe i wielkie litery oraz cyfry lub znaki specjalne.

W toku postępowania ustalono, że hasło uwierzytelnienia użytkowników do systemów informatycznych: „Faktury H.” oraz „CRM” nie składa się z co najmniej 8 znaków. Jednocześnie polityka bezpieczeństwa oraz instrukcja zarządzania systemem informatycznym służącym do przetwarzania danych osobowych, zawierają procedurę dotyczącą minimalnej długości hasła logowania, która nie jest zgodna z wytycznymi, o których mowa w części B pkt VIII załącznika do rozporządzenia (Dz. U. Nr 11, poz. 95, z późn. zm.).

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.