GENERALNY INSPEKTOR OCHRONY DANYCH OSOBOWYCH
dr Wojciech R. Wiewiórowski

Warszawa, dnia 14 maja 2012 r.

DIS/DEC-415/12/29650
dot. […]

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 i art. 7 pkt 5, art. 24 ust 1 pkt 1, pkt 3, pkt 4, art. 27 ust. 1 i ust. 2 pkt 1, art. 36 ust. 1, art. 36 ust. 2, art. 37, art. 39 ust. 1, art. 40 ustawy z dnia 29 sierpnia 1997 r. o ochronie danych osobowych (Dz. U. z 2002 r. Nr 101, poz. 926 z późn. zm.), § 3 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 W. Sp. z o. o,

nakazuję W. Sp. z o. o., usunięcie uchybień w procesie przetwarzania danych, poprzez:

1. Zapewnienie swobody w kwestii wyrażenia przez klientów zgody na przetwarzanie danych osobowych poprzez wyodrębnienie oświadczenia o wyrażeniu zgody na przetwarzanie danych od innych oświadczeń zawartych w treści formularza „Zgłoszenie członkostwa", w terminie od dnia, w którym niniejsza decyzja stanie się ostateczna.

2. Dopełnianie wobec klientów obowiązku informacyjnego w zakresie podania adresu siedziby W. Sp. z o. o., informacji o prawie dostępu do treści swoich danych oraz ich poprawiania oraz informacji że dane są niezbędne celem zawarcia umowy, w terminie od dnia, w którym niniejsza decyzja stanie się ostateczna.

3. Przetwarzanie danych o stanie zdrowia klientów na podstawie zgody wyrażonej na piśmie przez osoby, których dane dotyczą, w terminie od dnia, w którym niniejsza decyzja stanie się ostateczna.

4. Zgłoszenie do rejestracji Generalnemu Inspektorowi Ochrony Danych Osobowych zbioru danych osobowych klientów Spółki w terminie 7 dni od dnia, w którym niniejsza decyzja stanie się ostateczna.

5. Zabezpieczenie danych osobowych klientów zawartych w dokumentacji przechowywanej w recepcji Spółki przed ich udostępnieniem osobom nieupoważnionym, w terminie 7 dni od dnia, w którym niniejsza decyzja stanie się ostateczna.

6. Zabezpieczenie danych osobowych klientów zawartych w dokumentacji przechowywanej w pomieszczeniu […] przed ich udostępnieniem osobom nieupoważnionym, w terminie 7 dni od dnia, w którym niniejsza decyzja stanie się ostateczna.

7. Zastosowanie środków kryptograficznej ochrony danych podczas przesyłania danych osobowych wprowadzanych przez klientów do formularza kontaktowego zamieszczonego na stronie internetowej […] skrzynkę poczty elektronicznej w siedzibie Spółki, w terminie 30 dni od dnia, w którym niniejsza decyzja stanie się ostateczna.

8. Zastosowanie środków kryptograficznej ochrony danych podczas przesyłania za pośrednictwem sieci Internet danych osobowych przetwarzanych w systemie informatycznym o nazwie „A" , w terminie 30 dni od dnia, w którym niniejsza decyzja stanie się ostateczna.

9. Opracowanie i wdrożenie polityki bezpieczeństwa w terminie 30 dni od dnia, w którym niniejsza decyzja stanie się ostateczna.

10. Opracowanie i wdrożenie instrukcji zarządzania systemem informatycznym służącym do przetwarzania danych osobowych w terminie 30 dni od dnia, w którym niniejsza decyzja stanie się ostateczna.

11. Nadanie upoważnień do przetwarzania danych osobom dopuszczonym w W. Sp. z o. o. do przetwarzania danych osobowych, w terminie 7 dni od dnia, w którym niniejsza decyzja stanie się ostateczna.

12. Opracowanie ewidencji osób upoważnionych do przetwarzania danych w terminie 7 dni 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 w W. Sp. z o. o., zwaną dalej również Spółką., kontrolę zgodności przetwarzania danych osobowych z przepisami o ochronie danych osobowych sygn. akt […], 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 ustne wyjaśnienia od pracowników Spólki oraz skontrolowano systemy informatyczne służące do przetwarzania 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 W. Sp. z o. o., jako administrator danych, naruszyła przepisy o ochronie danych osobowych. Uchybienia te polegały na:

1. Niezapewnieniu swobody w kwestii wyrażenia przez klientów zgody na przetwarzanie danych osobowych w treści formularza „Zgłoszenie członkostwa" (art. 23 ust. 1 pkt 1 ustawy).
2. Niedopełnieniu wobec klientów obowiązku informacyjnego w zakresie podania adresu siedziby W. Sp. z o. o., informacji o prawie dostępu do treści swoich danych oraz ich poprawiania oraz informacji, że dane są niezbędne celem zawarcia umowy (art. 24 ust 1 pkt 1, pkt 3, pkt 4 ustawy).
3. Przetwarzaniu danych o stanie zdrowia (zbieranych w przypadku indywidualnych treningów przez trenerów) pomimo braku pisemnej zgody osób, których te dane dotyczą (art. 27 ust. 2 pkt 1 ustawy).
4. Niezgłoszeniu do rejestracji Generalnemu Inspektorowi Ochrony Danych Osobowych zbioru danych osobowych klientów Spółki (art. 40 ustawy).
5. Niewystarczającym zabezpieczeniu danych osobowych klientów przed ich udostępnieniem osobom nieupoważnionym, poprzez przechowywanie na otwartym kontuarze recepcji segregatorów z dokumentacją trenerów, w tym wypełnionych „Formularzy […] oraz formularzy zgłoszeniowych i bieżącej dokumentacji […] (na której również widnieją imiona, nazwiska i nr telefonów klientów) (art. 36 ust. 1 ustawy).
6. Niewystarczającym zabezpieczeniu dokumentacji archiwalnej zawierającej dane osobowe klientów Spółki, przechowywanej w pomieszczeniu […], przed jej udostępnieniem osobom nieupoważnionym (art. 36 ust. 1 ustawy).
7. Niezastosowaniu środków kryptograficznej ochrony danych podczas przesyłania danych osobowych ze strony internetowej […] na skrzynkę poczty elektronicznej, do której dostęp możliwy jest w siedzibie Spółki (art. 36 ust. 1 ustawy).

8. Niezastosowaniu środków kryptograficznej ochrony danych podczas przesyłania za pośrednictwem sieci Internet danych osobowych przetwarzanych w systemie informatycznym o nazwie „A” (art. 36 ust. 1 ustawy).
9. Nieopracowaniu polityki bezpieczeństwa oraz instrukcji zarządzania systemem informatycznym służącym do przetwarzania danych osobowych (art. 36 ust. 2 ustawy,§ 3 rozporządzenia).
10. Dopuszczeniu do przetwarzania danych osobowych osób, którym nie nadano upoważnień do przetwarzania danych osobowych (art. 37 ust. 1 ustawy).
11. Nieopracowaniu ewidencji osób upoważnionych w Spółce do przetwarzania danych (art. 39 ust. 1 ustawy).

W związku z powyższym, Generalny Inspektor Ochrony Danych Osobowych wszczął z urzędu postępowanie administracyjne w niniejszej sprawie w celu wyjaśnienia okoliczności sprawy. Pismem z dnia […] marca 2011 r. zawiadamiającym o wszczęciu postępowania administracyjnego w przedmiotowej sprawie sygn. […], 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. Pomimo to, Spółka nie złożyła wyjaśnień oraz nie przedstawił dowodów potwierdzających usunięcie wskazanych uchybień.

Generalny Inspektor Ochrony Danych Osobowych po przeprowadzeniu analizy całokształtu materiału dowodowego zebranego w niniejszej sprawie zważył, co następuje:

Zgodnie z art. 23 ust. 1 pkt. 1 ustawy, przetwarzanie danych jest dopuszczalne tylko wtedy, gdy: osoba, której dane dotyczą, wyrazi na to zgodę, chyba że chodzi o usunięcie dotyczących jej danych. W myśl art. 7 pkt 5 ustawy, ilekroć w ustawie jest mowa o: zgodzie osoby, której dane dotyczą - rozumie się przez to oświadczenie woli, którego treścią jest zgoda na przetwarzanie danych osobowych tego, kto składa oświadczenie; zgoda nie może być domniemana lub dorozumiana z oświadczenia woli o innej treści; zgoda może być odwołana w każdym czasie.

Jak ustalono w toku kontroli podstawą prawną przetwarzania danych klientów jest zgoda na przetwarzanie danych wyrażona w treści formularza „Zgłoszenie członkostwa” oraz realizacja umowy, której stroną jest klient. W treści ww. formularza zgoda na przetwarzanie danych osobowych znajduje się wśród innych oświadczeń m.in. w zakresie zapoznania się i akceptacji warunków członkostwa w klubie i cennika, pod którymi klient składa jeden podpis.

Z tych względów należy uznać, że w takiej sytuacji klient nie ma swobody wyrażenia lub nie zgody na przetwarzania swoich danych, bowiem wyrażając zgodę na zawarcie umowy lub też akceptując warunki członkostwa wyraża zgodę na: „przesyłanie informacji związanych z

funkcjonowaniem Klubu i zaproszeń na imprezy organizowane dla członków Klubu na podany przeze mnie adres kontaktowy, e-mail, bądź numer telefonu.”.

Zgodnie z art. 24 ust. 1 pkt 1, pkt 3, pkt 4 ustawy, w przypadku zbierania danych osobowych od osoby, której one dotyczą, administrator danych jest obowiązany poinformować tę osobę o: adresie swojej siedziby i pełnej nazwie, a w przypadku gdy administratorem danych jest osoba fizyczna - o miejscu swojego zamieszkania oraz imieniu i nazwisku, prawie dostępu do treści swoich danych oraz ich poprawiania, dobrowolności albo obowiązku podania danych, a jeżeli taki obowiązek istnieje, o jego podstawie prawnej.

W toku kontroli ustalono, że obowiązek informacyjny wobec klientów realizowany jest w zakresie wskazanym w treści formularza „Zgłoszenia członkostwa”. W treści przedmiotowego formularza wskazano nazwę Spółki, ale nie podano adresu jej siedziby, ponadto formularz nie zawiera informacji o prawie dostępu do treści swoich danych oraz ich poprawiania, jak również, że dane są niezbędne celem zawarcia umowy.

Zgodnie z art. 27 ust. 1 ustawy, 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. Przetwarzanie danych, o których mowa w ust. 1, jest jednak dopuszczalne, jeżeli: osoba, której dane dotyczą, wyrazi na to zgodę na piśmie, chyba że chodzi o usunięcie dotyczących jej danych (art. 27 ust. 2 pkt 1 ustawy).

W toku kontroli ustalono, że w Spółce przetwarzane są dane o stanie zdrowia, w przypadku indywidualnych treningów przez trenerów, które nie są wpisywane do systemu informatycznego. Wobec powyższego należy uznać, że Spółka powinna pozyskiwać pisemną zgodę od osób, których dane dotyczą na przetwarzanie ich danych o stanie zdrowia, brak jest bowiem pomimo celowości przetwarzania takich danych, podstaw prawnych do ich przetwarzania.

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. W myśl art. 7 pkt 1, 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 Spółce przetwarzane są dane klientów, które są zbierane przy pomocy formularzy tj. […]. Formularze te stanowią dokumentację klientów, przechowywaną w biurze […] oraz w […]. Dokumentacja klientów jest przechowywana w segregatorach, ułożona kolejno wg daty. Ponadto, dane klientów przetwarzane są w systemie informatycznym o nazwie „A”, który służy do

ewidencjonowania użytkowników klubu […]. Należy zatem uznać, że Spółka prowadzi zbiór danych osobowych, w rozumieniu art. 7 pkt 1 ustawy, którego nie zgłosiła do rejestracji Generalnemu Inspektorowi Ochrony Danych Osobowych. Zbiór ten nie podlega wyłączeniu z rejestracji, bowiem nie spełnia przesłanek, o których mowa w art. 43 ust. 1 ustawy.

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, zabraniem przez osobę nieuprawnioną, przetwarzaniem z naruszeniem ustawy oraz zmianą, utratą, uszkodzeniem lub zniszczeniem.

Jak ustalono, recepcja w Spółce znajduje się w otwartej części pomieszczeń zajmowanych przez Spółkę i wydzielona jest kontuarem. W recepcji przechowywane są segregatory z dokumentacją trenerów, w tym wypełnione „Formularze […]". Ponadto, w odrębnym segregatorze przechowywane są […] zawierające również dane osobowe klientów (imię, nazwisko, nr telefonu). W […] przechowywane są także formularze […] z ostatnich trzech dni oraz bieżąca dokumentacja […], na której widnieją: imiona, nazwiska i numery telefonów klientów. Sprzątaniem pomieszczeń zajmuje się personel sprzątający […], po godzinach pracy […]. W świetle powyższych ustaleń należy stwierdzić, że administrator danych w sposób niewystarczający zabezpieczył dane osobowe klientów, przed ich udostępnieniem osobom nieupoważnionym, bowiem dostęp do dokumentacji zawierającej dane osobowe klientów przechowywanej w […] może mieć personel sprzątający.

Ponadto, dokumentacja klientów z lat ubiegłych jest przechowywana w pomieszczeniu […] zajmowanym przez jednego z pracowników […]. W pomieszczeniu są otwarte regały, na których przechowywane są segregatory z dokumentacją klientów (formularze), dokumentacją […] oraz […]. Część dokumentacji (formularze […], wypełnione formularze […]) jest ułożona na biurku i szafkach. Klucze do pomieszczenia są przechowywane w recepcji.

W świetle powyższych ustaleń należy stwierdzić, że przedmiotowa dokumentacja nie została w sposób wystarczający zabezpieczona przed jej udostępnieniem osobom nieupoważnionym.

W toku kontroli ustalono także, że Spółka na stronie internetowej udostępniała formularz kontaktowy. Na formularzu kontaktowym klient musi wprowadzić następujące dane osobowe: nazwisko, adres email oraz numer telefonu. Ustalono, że formularz wysyłany jest siecią Internet do Spółki w postaci poczty elektronicznej i dostarczany jest na skrzynkę poczty elektronicznej, do której dostęp możliwy jest w siedzibie Spółki. Przesyłanie danych osobowych w powyższy sposób nie jest zabezpieczone środkami kryptograficznej ochrony danych (dowód stanowi załącznik […] do protokołu kontroli).

Nadto jak ustalono, przesyłanie danych przetwarzanych w Spółce przy użyciu aplikacji klienckiej w systemie informatycznym o nazwie „A", a następnie przesyłanych na serwer za pośrednictwem sieci Internet nie jest zabezpieczone za pomocą środków ochrony kryptograficznej.

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. Dokumentacja, o której jest mowa wyżej, zgodnie z ust. 3, powinna być wdrożona przez administratora danych.

W toku kontroli ustalono, że w Spółce nie opracowano dokumentacji opisującej proces przetwarzania danych osobowych, tj. polityki bezpieczeństwa i instrukcji zarządzania systemem informatycznym służącym do przetwarzania danych osobowych.

Zgodnie z art. 37 ustawy, do przetwarzania danych mogą być dopuszczone wyłącznie osoby posiadające upoważnienie nadane przez administratora danych.

W toku kontroli ustalono, że w Spółce nie są nadawane upoważnienia do przetwarzania danych osobowych.

Zgodnie z art. 39 ust. 1 ustawy, administrator danych prowadzi ewidencję osób upoważnionych do ich przetwarzania, która powinna zawierać: 1) imię i nazwisko osoby upoważnionej, 2) datę nadania i ustania oraz zakres upoważnienia do przetwarzania danych osobowych, 3) identyfikator, jeżeli dane są przetwarzane w systemie informatycznym.

W toku czynności kontrolnych ustalono, że w Spółce nie jest prowadzona ewidencja osób upoważnionych do przetwarzania danych osobowych.

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

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.

W razie niewykonania decyzji w terminie zostanie wobec podmiotu zobowiązanego do jej wykonania wszczęte postępowanie egzekucyjne na podstawie przepisów ustawy z dnia 17 czerwca 1966 r. o postępowaniu egzekucyjnym w administracji (Dz. U. z 2005 r. Nr 229, poz. 1954, z późn. zm.).