GENERALNY INSPEKTOR OCHRONY DANYCH OSOBOWYCH

dr Wojciech R. Wiewiórowski

Warszawa, dnia 3 sierpnia 2011 r.

DIS/DEC-651/37118/11

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. 7 pkt 5, art. 23 ust. 1 pkt 1, art. 37, art. 39 ust. 1 pkt 2, 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.), § 4 pkt 1 i pkt 2, § 7 ust. 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), oraz częścią B pkt VIII załącznika do ww. rozporządzenia, po przeprowadzeniu postępowania administracyjnego w sprawie przetwarzania danych osobowych przez Klub […] S.S.A,

n a k a z u j ę

Klubowi […] S.S.A., usunięcie uchybień w procesie przetwarzania danych osobowych, poprzez:

1. **Zapewnienie osobom, od których pozyskiwane są dane osobowe za pomocą dokumentu o nazwie "Wniosek o wydanie Karty […]", opcjonalności w kwestii wyrażenia zgody na przetwarzanie dotyczących ich danych osobowych, odrębnie dla celów marketingowych i promocyjnych oraz odrębnie na przekazywanie ww. danych innym podmiotom, w terminie 30 dni od dnia, w którym niniejsza decyzja stanie się ostateczna.**
2. **Zapewnienie osobom, od których pozyskiwane są dane osobowe za pomocą dokumentu o nazwie "Wniosek o wydanie Karty […]", opcjonalności w kwestii wyrażenia zgody na przetwarzanie dotyczących ich danych osobowych w celach marketingowych**

i promocyjnych, odrębnie dla Klubu […] S.S.A. oraz odrębnie dla E. Sp. z o.o., w terminie 30 dni od dnia, w którym niniejsza decyzja stanie się ostateczna.

3. **Wskazanie pełnych nazw i adresów siedzib partnerów marketingowych i promocyjnych, którym przekazywane będą dane osobowe pozyskane za pomocą dokumentu o nazwie "Wniosek o wydanie Karty […]", w terminie 30 dni od dnia, w którym niniejsza decyzja stanie się ostateczna.**
4. **Zgłoszenie Generalnemu Inspektorowi Ochrony Danych Osobowych aktualizacji informacji dotyczących zbioru danych osobowych o nazwie „B." (księga rejestrowa nr […]) w zakresie: podstawy prawnej przetwarzania danych, celu przetwarzania danych, zakresu przetwarzanych danych oraz informacji o odbiorcach, którym dane są przekazywane, w terminie 30 dni od dnia, w którym niniejsza decyzja stanie się ostateczna.**
5. **Zapewnienie, aby hasła używane do uwierzytelniania użytkowników w systemie informatycznym o nazwie „A", służącym do przetwarzania danych osobowych pozyskanych za pomocą dokumentu o nazwie "Wniosek o wydanie Karty […]", składały się co najmniej z 8 znaków, zawierały małe i wielkie litery oraz cyfry lub znaki specjalne, w terminie 3 miesięcy od dnia, w którym niniejsza decyzja stanie się ostateczna.**
6. **Uzupełnienie polityki bezpieczeństwa dotyczącej systemu informatycznego o nazwie „A." o wykaz budynków, pomieszczeń lub części pomieszczeń, tworzących obszar, w którym przetwarzane są dane osobowe oraz wykaz zbiorów danych osobowych wraz ze wskazaniem programów zastosowanych do przetwarzania tych danych, w terminie 30 dni od dnia, w którym niniejsza decyzja stanie się ostateczna.**
7. **Nadanie upoważnień do przetwarzania danych osobowych osobom dopuszczonym do przetwarzania ww. danych, w terminie 30 dni od dnia, w którym niniejsza decyzja stanie się ostateczna.**
8. **Uzupełnienie ewidencji osób upoważnionych do przetwarzania danych osobowych o datę ustania upoważnienia do przetwarzania danych osobowych, w terminie 30 dni od dnia, w którym niniejsza decyzja stanie się ostateczna.**
9. **Zapewnienie, aby systemy informatyczne o nazwach „A" i „B", służące do przetwarzania danych osobowych pozyskanych za pomocą dokumentu o nazwie "Wniosek o wydanie Karty […]", umożliwiały dla każdej osoby, której dane osobowe są przetwarzane w ww. systemach informatycznych, sporządzenie i wydrukowanie raportu zawierającego w powszechnie zrozumiałej formie informacje, o których mowa w § 7 ust. 1 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, w terminie 3 miesięcy 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 Klubie […] S.S.A., zwanym dalej Klubem, kontrolę zgodności przetwarzania danych osobowych z przepisami o ochronie danych osobowych (sygn. […]), 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 i 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 Klubu, 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 Klub.

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

1. Zamieszczeniu na dokumencie o nazwie "Wniosek o wydanie Karty […]" niewłaściwie sformułowanej klauzuli zgody na przetwarzanie danych osobowych. Nieprawidłowość konstrukcji ww. klauzuli polega na umieszczeniu w niej łącznie dwóch oświadczeń woli o wyrażeniu zgody na przetwarzanie danych osobowych w różnych celach. Skutkiem powyższego osoby, od których pozyskiwane są dane osobowe za pomocą dokumentu o nazwie "Wniosek o wydanie Karty […]" zostały pozbawione opcjonalności w kwestii wyrażenia zgody na przetwarzanie dotyczących ich danych osobowych dla celów marketingowych i promocyjnych oraz na przekazywanie tych danych innym podmiotom. Ponadto, zgoda na przetwarzanie danych osobowych dla celów marketingowych i promocyjnych pozyskiwana jest łącznie na rzecz Klubu oraz E. Sp. z o.o. W ten sposób osoby, od których pozyskiwane są dane osobowe zostały pozbawione możliwości wyboru, na rzecz którego z ww. podmiotów pragną wyrazić zgodę na przetwarzanie dotyczących ich danych osobowych dla celów marketingowych i promocyjnych. Jednocześnie, poprzez nieprecyzyjne określenie podmiotów, którym

przekazywane będą dane osobowe pozyskane za pomocą dokumentu o nazwie "Wniosek o wydanie Karty […]" uniemożliwiono osobom, od których ww. dane są pozyskiwane, podjęcie swobodnej decyzji dotyczącej tego, komu zostaną przekazane ww. dane osobowe (art. 23 ust. 1 pkt 1 w związku z art. 7 pkt 5 ustawy).

2. Niezgłoszeniu Generalnemu Inspektorowi Ochrony Danych Osobowych aktualizacji informacji dotyczących zbioru danych osobowych o nazwie „B.” (księga rejestrowa nr […]) w zakresie: podstawy prawnej przetwarzania danych, celu przetwarzania danych, zakresu przetwarzanych danych oraz informacji o odbiorcach, którym dane są przekazywane (art. 41 ust. 2 ustawy).
3. Niezapewnieniu, aby hasła używane do uwierzytelniania użytkowników w systemie informatycznym o nazwie „A” składały się co najmniej z 8 znaków, zawierały małe i wielkie litery oraz cyfry lub znaki specjalne (część B pkt VIII załącznika do rozporządzenia).
4. Niezawarciu w polityce bezpieczeństwa dotyczącej systemu informatycznego o nazwie „B” 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 tych danych (§ 4 pkt 1 i pkt 2 rozporządzenia).
5. Dopuszczeniu do przetwarzania danych osobowych osób, którym nie nadano upoważnień do przetwarzania ww. danych (art. 37 ustawy).
6. Niezawarciu w ewidencji osób upoważnionych do przetwarzania danych osobowych daty ustania upoważnienia do przetwarzania danych osobowych (art. 39 ust. 1 pkt 2 ustawy).
7. Niezapewnieniu, aby systemy informatyczne o nazwach "A" i "B", umożliwiały sporządzenie i wydrukowanie raportu zawierającego w powszechnie zrozumiałej formie informacje, o których mowa w § 7 ust. 1 rozporządzenia (§ 7 ust. 3 rozporządzenia).

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

W odpowiedzi na zawiadomienie o wszczęciu postępowania administracyjnego Klub nie złożył dodatkowych wyjaśnień oraz nie przedstawił innych dowodów mogących potwierdzić usunięcie uchybień w procesie przetwarzania danych osobowych.

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

Zgodnie z art. 23 ust. 1 pkt 1 ustawy, przetwarzanie danych jest dopuszczalne wtedy, gdy osoba, której dane dotyczą, wyrazi na to zgodę, chyba że chodzi o usunięcie dotyczących jej danych. Jednocześnie należy wskazać, iż zgodnie z 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.

W toku kontroli ustalono, że za pomocą formularza o nazwie „Wniosek o wydanie Karty […]" pozyskiwana jest od osób składających ww. wnioski zgoda na przetwarzanie dotyczących ich danych osobowych, w celach marketingowych i promocyjnych, przez Klub oraz przez E. Sp. z o.o., zwaną dalej również E. Sp. z o.o. Pozyskiwanie zgody na przetwarzanie danych osobowych w ww. celach wynika z faktu prowadzenia przez Klub akcji marketingowych na rzecz podmiotów, z którymi w tym zakresie współpracuje. W ten sam sposób pozyskiwana jest również zgoda na przekazywanie ww. danych partnerom marketingowym i promocyjnym Klubu i E. Sp. z o.o. Pozyskiwanie zgody na przetwarzanie danych osobowych w ww. celach odbywa się poprzez zaznaczenie przez wnioskodawcę pola wyboru przy klauzuli o treści: „*Wyrażam zgodę na przetwarzanie danych osobowych zawartych we wniosku w celach marketingowych i promocyjnych przez klub S.S.A.; E. Sp. z o.o., oraz przekazywanie tych danych partnerom marketingowym i promocyjnym tych podmiotów, a w szczególności na otrzymywanie informacji handlowych od wszystkich tych podmiotów. Zostałem poinformowany o prawie dostępu do treści moich danych osobowych, prawie ich poprawiania oraz o dobrowolności podania przeze mnie moich danych osobowych*".

Mając na uwadze powyższe ustalenia należy stwierdzić, iż zastosowana przez Klub forma pozyskiwania zgody na przetwarzanie danych osobowych narusza przepisy ustawy o ochronie danych osobowych, bowiem decyzja w sprawie wyrażenia zgody na przetwarzanie danych osobowych powinna mieć charakter swobodny i samodzielny, tzn. że w przypadku różnych celów przetwarzania danych osobowych należy pozyskiwać oddzielną zgodę na każdy z tych celów, w przypadku wyrażania zgody na przetwarzanie danych osobowych przez różne podmioty należy pozyskać odrębną zgodę na przetwarzanie danych przez każdy z tych podmiotów, jak również należy precyzyjnie określić krąg podmiotów, którym dane będą przekazywane. Stanowisko uznające za niezgodne z prawem łączenie oświadczeń woli dotyczących zgody na przetwarzanie danych osobowych znajduje swoje potwierdzenie w orzecznictwie NSA. W wyroku z dnia 11 kwietnia 2003 r. (sygn. II S.A. 3942/02) Naczelny Sąd Administracyjny stwierdził, iż *„(...) w przypadku oświadczenia woli dotyczącego różnych celów przetwarzania (danych osobowych) (...), zgoda winna być wyrażona wyraźnie pod każdym z tych celów przetwarzania"*. Należy stwierdzić, iż w opisanej sytuacji, sposób skonstruowania klauzuli zgody na przetwarzanie danych osobowych nie zapewnia osobom składającym "Wniosek o wydanie Karty […]" opcjonalności w kwestii wyrażenia zgody na przetwarzanie ich danych osobowych dla celów marketingowych i promocyjnych oraz na przekazywanie ich danych innym podmiotom. Ponadto,

nie zapewniono opcjonalności wyrażenia zgody na przetwarzanie danych osobowych w celach marketingowych i promocyjnych przez Klub i przez E. Sp. z o.o. Jednocześnie, nieprecyzyjne określenie podmiotów, którym dane będą przekazywane, nie zapewnia możliwości podjęcia przez wnioskodawcę swobodnej decyzji komu zostaną przekazane dotyczące go dane osobowe.

Zgodnie z art. 41 ust. 2 ustawy, 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.

Jak ustalono, Klub zgłosił do rejestracji Generalnemu Inspektorowi Ochrony Danych Osobowych zbiór danych osobowych o nazwie „B." (księga rejestrowa nr […]). Analiza ww. księgi rejestrowej ujawniła rozbieżności pomiędzy informacjami w niej zawartymi, a stanem faktycznym ustalonym w wyniku przeprowadzonej kontroli. Wskazane rozbieżności dotyczyły:

a) podstawy prawnej przetwarzania danych - nie wskazano, iż dane osobowe przetwarzane są w celu wypełnienia obowiązków wynikających z przepisów ustawy z dnia […] marca 2009 r. o bezpieczeństwie imprez masowych (Dz. U. z 2009 r., Nr 62, poz. 504),
b) celu przetwarzania danych - jak ustalono, dane są przetwarzane również w celu zapewnienia identyfikacji osób uczestniczących w imprezie sportowej,
c) zakresu przetwarzanych danych - w zgłoszeniu zbioru do rejestracji nie wskazano takich danych jak: wizerunek twarzy, seria i numer innego niż dowód osobisty dokumentu potwierdzającego tożsamość, adres e-mail i nr telefonu,
d) informacji o odbiorcach, którym dane są przekazywane - w zgłoszeniu zbioru do rejestracji nie wskazano, że dane osobowe przekazywane są E. S.A., w imieniu której działa E. Sp. z o.o., jako podmiot, o którym mowa w art. 31 ust 1 ustawy.

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.

Jak ustalono w toku kontroli hasła używane do uwierzytelniania użytkowników w systemie informatycznym o nazwie „A", służącym do przetwarzania danych osobowych, nie zawierają wielkich liter.

Zgodnie z § 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 oraz wykaz zbiorów danych osobowych wraz ze wskazaniem programów zastosowanych do przetwarzania tych danych.

W toku kontroli ustalono, że w Klubie prowadzona jest dokumentacja przetwarzania danych osobowych tj. polityka bezpieczeństwa i instrukcja zarządzania systemem informatycznym służącym do przetwarzania danych osobowych. Dokumentacja ta składa się z dwóch części – pierwsza z nich odnosi się do systemu informatycznego o nazwie „A”, a druga do systemu informatycznego o nazwie "B", który przez producenta nazwany jest aplikacją „C”. Należy również wskazać, iż polityka bezpieczeństwa systemu "B" jest dokumentem opracowanym przez firmę E. Sp. z o.o., odnoszącym się do aplikacji nazwanej „C”. Dokument ten przedstawia zasady bezpiecznej eksploatacji systemu z punktu widzenia dostawcy systemu i jednocześnie jej administratora, a nie administratora danych, którym jest Klub. Polityka bezpieczeństwa odnosząca się do systemu "B" nie zawiera: 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 tych danych.

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

W toku kontroli ustalono, iż do przetwarzania danych dopuszczone zostały osoby nie posiadające upoważnień nadanych przez administratora danych**.**

Zgodnie z art. 39 ust. 1 pkt 2 ustawy, administrator danych prowadzi ewidencję osób upoważnionych do ich przetwarzania, która powinna zawierać datę nadania i ustania oraz zakres upoważnienia do przetwarzania danych osobowych.

W toku kontroli ustalono, iż prowadzona w Klubie ewidencja osób upoważnionych do przetwarzania danych nie zawiera daty ustania upoważnienia.

Zgodnie z § 7 ust. 3 rozporządzenia, dla każdej osoby, której dane osobowe są przetwarzane w systemie informatycznym, system zapewnia sporządzenie i wydrukowanie raportu zawierającego w powszechnie zrozumiałej formie informacje, o których mowa w ust. 1.

W toku kontroli ustalono, iż systemy informatyczne o nazwach „A” i „B”, w których przetwarzane są dane osobowe, nie zapewniają dla każdej osoby, której dane osobowe są przetwarzane w systemie informatycznym sporządzenia i wydrukowania raportu zawierającego w powszechnie zrozumiałej formie informacje, o których mowa w ust. 1.

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.