GENERALNY INSPEKTOR OCHRONY DANYCH OSOBOWYCH

dr Wojciech R. Wiewiórowski

Warszawa, dnia 6 listopada 2014 r.

DIS/DEC- 1072/14/87525

dot.:[…]

D E C Y Z J A

Na podstawie art. 104 § 1 i art. 105 ustawy z dnia 14 czerwca 1960 r. Kodeks postępowania administracyjnego (Dz. U. z 2013 r., poz. 267), art. 12 pkt 2, art. 18 ust. 1 pkt 1, art. 22 w związku z art. 23 ust. 1, art. 39 ust. 1 ustawy z dnia 29 sierpnia 1997 r. o ochronie danych osobowych (Dz. U. z 2014, poz. 1182), po przeprowadzeniu postępowania administracyjnego w sprawie przetwarzania danych osobowych przez P. Sp. z o.o.,

I. Nakazuję P. Sp. z o.o., usunięcie uchybienia w procesie przetwarzania danych osobowych, poprzez zaprzestanie przetwarzania bez podstawy prawnej danych biometrycznych swoich klientów, w terminie 2 miesięcy 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 w P. Sp. z o.o., zwanej dalej także „Spółką”, kontrolę zgodności przetwarzania danych osobowych z przepisami o ochronie danych osobowych (sygn. kontroli: […]), tj. ustawą z dnia 29 sierpnia 1997 r. o ochronie danych osobowych (Dz. U. z 2014 r., poz. 1182), 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). Zakresem kontroli objęto przetwarzanie przez Spółkę danych biometrycznych – odcisków linii papilarnych – swoich

klientów. Stan faktyczny szczegółowo opisano w protokole kontroli, który został podpisany przez Członka Zarządu Spółki.

Na podstawie zgromadzonego podczas ww. kontroli materiału dowodowego ustalono, że w procesie przetwarzania danych osobowych Spółka, jako administrator danych, naruszyła przepisy o ochronie danych osobowych, polegające na:

1. Przetwarzaniu bez podstawy prawnej danych biometrycznych swoich klientów (art. 23 ust. 1 ustawy).

2. Niezawarciu w ewidencji osób upoważnionych do przetwarzania danych osobowych identyfikatorów użytkowników przetwarzających dane z wykorzystaniem systemu informatycznego, daty ustania upoważnienia, jak również zakresu upoważnienia (art. 39 ust. 1 ustawy).

W związku z powyższym Generalny Inspektor Ochrony Danych Osobowych wszczął z urzędu postępowanie administracyjne w celu wyjaśnienia okoliczności sprawy. W piśmie z dnia […] czerwca 2014 r. sygn. […], stanowiącym zawiadomienie o wszczęciu postępowania administracyjnego w przedmiotowej sprawie, Spółka została poinformowana o prawie czynnego udziału w każdym stadium postępowania, a przed wydaniem decyzji wypowiedzenia się, co do zebranych w toku kontroli dowodów i materiałów oraz zgłoszonych żądań.

Pełnomocnik Spółki w piśmie z dnia […] czerwca 2014 r. złożył wniosek o przedłużenie terminu wskazanego w zawiadomieniu o wszczęciu postępowania administracyjnego na złożenie wyjaśnień i ewentualnie innych dowodów do dnia […] lipca 2014 r. z uwagi na potrzebę kontaktu z członkami Zarządu Spółki oraz konieczność wyjaśnienia specjalistycznych zagadnień technicznych związanych ze stosowaną przez Spółkę procedurą weryfikacji uprawnień klientów wchodzących do klubów. Pismem z dnia […] czerwca 2014 r. sygn. […] Generalny Inspektor przychylił się do ww. wniosku.

W odpowiedzi na zawiadomienie o wszczęciu postępowania administracyjnego pełnomocnik Spółki w piśmie z dnia […] lipca 2014 r. złożył wyjaśnienia, w których poinformował, iż prowadzona w Spółce ewidencja osób upoważnionych do przetwarzania danych osobowych uwzględnia obecnie wszystkie elementy przewidziane w art. 39 ust. 1 ustawy (dodatkowo w załączeniu do pisma pełnomocnika Spółki z dnia […] lipca 2014 r. załączono wydruk ww. ewidencji). Ponadto, w piśmie z dnia […] lipca 2014 r. pełnomocnik Spółki odnosząc się do pkt 1 zawiadomienia o wszczęciu postępowania administracyjnego wyjaśnił m.in., iż:

1. Stosowanie systemu biometrycznej kontroli wstępu (dalej także „system”) do prowadzonych przez Spółkę klubów nie prowadzi do przetwarzania danych osobowych z uwagi na fakt, że dane te nie umożliwiają identyfikacji osoby bez poniesienia nadmiernych nakładów. Z uwagi na sposób funkcjonowania systemu biometrycznej kontroli wstępu, opartego na biometrycznych czytnikach

kontroli dostępu, kwestie przetwarzania danych biometrycznych klienta należy rozważyć przede wszystkim w odniesieniu do trwającej tysięczne ułamki sekund operacji wyliczenia kodu na podstawie pobranego wzorca biometrycznego, która to operacja odbywa się w biometrycznym czytniku kontroli - poza systemem informatycznym Spółki o nazwie „A". Ponadto: a) „system" nie przekazuje wzorców danych do systemu informatycznego Spółki i niezwłocznie usuwa je po dokonaniu porównania; b) „system", który dokonuje wyłącznie weryfikacji, nie posiada archiwum referencyjnego (nie dokonuje weryfikacji tożsamości na zasadzie badania zgodności wzorca biometrycznego z biometrycznymi danymi referencyjnymi zapisanymi w systemie informatycznym Spółki, bo takowych zapisanych w systemie nie ma); c) wzorce biometryczne mają charakter anonimowy, gdyż nie są powiązane z innymi danymi pozwalającymi na weryfikację/identyfikację osoby („system" nie przechowuje wzorców danych z innymi danymi jednostki); d) stosowane są zabezpieczenia wzorców biometrycznych przed nieuprawnionym dostępem osób trzecich, e) cechy biometryczne gromadzone incydentalnie przez Spółkę nie mogą zostać uznane za dane osobowe, gdyż nie identyfikują one osoby, której dane dotyczą.

3. W ocenie Spółki, w razie jednak przyjęcia, że dane biometryczne przetwarzane przez Spółkę stanowią dane osobowe i dochodzi do ich przetwarzania, należy uznać, że zbiór danych jest sporządzany przez Spółkę doraźnie, wyłącznie ze względów technicznych, a dane podlegają natychmiastowemu usunięciu (co ogranicza stosowanie ustawy o ochronie danych osobowych do rozdziału V).

4. Na wypadek uznania, że stosowanie przez Spółkę systemu biometrycznej kontroli wstępu prowadzi do przetwarzania danych osobowych, które nie jest objęte zakresem normy wyrażonej w art. 2 ust. 3 ustawy o ochronie danych osobowych, przetwarzanie (danych biometrycznych) jest dopuszczalne z uwagi na wyrażanie zgody na ich przetwarzanie przez klientów Spółki, tj. osoby, których dane dotyczą. Na podstawie regulaminów klubów Spółki, posiadanie opaski z kodem utworzonym na podstawie danych biometrycznych nie jest konieczne do korzystania z klubów fitness. Klient może otrzymać opaskę bez zapisanego na niej kodu i na takich samych zasadach korzystać z usług Spółki. W „Ogólnych warunkach członkostwa" wskazano, że wstęp do klubów Spółki jest możliwy za okazaniem karty członkowskiej, z czego wynika, że klienci Spółki nie muszą korzystać z opasek z mikroprocesorem, bo o prawie wstępu do klubów, zgodnie z regulaminami klubów Spółki, decyduje także posiadana karta. Klienci Spółki nie są zobowiązani do wyrobienia opaski z kodem i w związku z tym udostępniania swoich danych biometrycznych w celu wstępu do klubu. Klienci mogą wyrobić opaskę bez zapisywania na niej kodu (opaska taka nie otwiera bramki po przyłożeniu do czytnika, w celu wejścia do klubu; klient posiadający taką opaskę podchodzi do recepcji, gdzie po sprawdzeniu jego tożsamości, pracownik recepcji mechanicznie otwiera bramkę do klubu) utworzonego na podstawie wzorców biometrycznych, czy też

kontynuować korzystanie z karty członkowskiej na dotychczasowych zasadach. Przez przystąpienie do wyrobienia, a następnie korzystania z opaski z mikroprocesorem, klient wyraża zgodę na przetwarzanie danych biometrycznych w sposób świadomy, tj. posiadając wiedzę co do celu ich przetwarzania. Klient jest bowiem informowany o zasadach funkcjonowania „systemu" i tego, że Spółka stosuje go w celu kontroli wstępu do klubów. Kwestionowanie złożonych oświadczeń o wyrażeniu zgody na przetwarzanie danych osobowych jest błędne z uwagi na brak relacji podporządkowania w stosunku klient – Spółka oraz brak uprawnień organu ochrony danych osobowych w zakresie badania skuteczności wyrażenia zgody (co wynika zdaniem Spółki z uzasadnienia do wyroku Naczelnego Sądu Administracyjnego w Warszawie z dnia 1 grudnia 2009 r., I OSK 249/06).

5. Przy powyższym założeniu nie powstaje zbiór, który mógłby podlegać zgłoszeniu do rejestracji Generalnemu Inspektorowi Ochrony Danych Osobowych.

W związku z wyjaśnieniami przedstawionymi w piśmie z dnia […] lipca 2014 r. przez pełnomocnika Spółki zaistniała konieczność przeprowadzenia dodatkowych czynności kontrolnych. W tym celu w dniach od […] do […] 2014 r. inspektorzy upoważnieni przez Generalnego Inspektora Ochrony Danych Osobowych przeprowadzili w Spółce kolejną kontrolę zgodności przetwarzania danych osobowych z przepisami o ochronie danych osobowych (sygn. kontroli: […]). Zakresem kontroli objęto m.in. ustalenie podstawy prawnej przetwarzania danych biometrycznych klientów Spółki, w szczególności, czy pozyskiwana jest zgoda na przetwarzanie danych biometrycznych, a jeżeli tak, to czy zapewniono swobodę w jej udzieleniu. Stan faktyczny szczegółowo opisano w protokole kontroli, który został podpisany przez pełnomocników Spółki.

Pismem z dnia […] września 2014 r. Pełnomocnik Spółki przesłał kolejne wyjaśnienia wskazując m.in., że Spółka na żadnym etapie procesu kontroli dostępu do klubów fitness nie gromadzi i nie przechowuje danych w postaci „kodu alfanumerycznego" (przetworzony na algorytm zapis cechy biometrycznej – części skrajnych punktów linii papilarnych), a w procesie kontroli dostępu nigdy nie dochodzi do połączenia „kodu alfanumerycznego" z systemem informatycznym „A", w którym przetwarzane są dane osobowe klientów. W ww. piśmie Pełnomocnik Spółki zawnioskował o przedłużenie postępowania administracyjnego, w tym możliwość złożenia dodatkowych wniosków dowodowych przez Spółkę. Pismem z dnia […] września 2014 r. sygn. […], […] Generalny Inspektor uwzględnił ww. wniosek i wskazał, iż termin wydania decyzji administracyjnej w sprawie przetwarzania danych osobowych przez Spółkę zostaje przedłużony do dnia […] października 2014 r. Spółka nie złożyła jednak żadnych wniosków dowodowych.

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, 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 to niezbędne do wykonania określonych prawem zadań realizowanych dla dobra publicznego,

5) jest to niezbędne dla wypełnienia prawnie usprawiedliwionych celów realizowanych przez administratorów danych oraz odbiorców danych, a przetwarzanie nie narusza praw i wolności osoby, której dane dotyczą.

W toku kontroli sygn. […] ustalono, że w wybranych klubach prowadzonych przez Spółkę stosowany jest system biometrycznej kontroli wstępu do klubów w celu uproszczenia i przyspieszenia skutecznej weryfikacji klientów oraz podniesienia bezpieczeństwa. Wzorzec biometryczny odcisku palca klienta Spółki (informacje o pojedynczych punktach odcisku palca przekształcone algorytmem na postać cyfrową) zapisywany jest w chipie opaski, która jest wydawana klientowi. Zgodnie z wyjaśnieniami złożonymi w toku ww. kontroli opaska staje się własnością klienta i nie jest zwracana Spółce. W celu wejścia do klubu, klient przykłada do czytnika znajdującego się przy bramce wejściowej opaskę i palec, w celu weryfikacji, czy jest on właścicielem opaski i ma uprawnienia do korzystania z oferty Spółki. Czytnik sczytuje z opaski zapisany kod punktów biometrycznych i po przyłożeniu przez klienta palca do czytnika linii papilarnych sczytuje punkty biometryczne z palca, przetwarza je w kod i porównuje z kodem zapisanym na opasce. Jednocześnie wysyłany jest do systemu informatycznego o nazwie „A” (służącego do obsługi klientów Spółki) numer identyfikacyjny (ID) opaski celem zweryfikowania, czy klient posiada uprawnienia do korzystania z oferty klubu. W momencie przyłożenia opaski do czytnika znajdującego się przy bramce wejściowej, na komputerze znajdującym się w recepcji, wyświetla się informacja dotycząca klienta – członka klubu (m.in. zdjęcie). W systemie informatycznym o nazwie „A” nie są przechowywane dane biometryczne klientów, zapisany jest natomiast m.in. nr ID opaski. W toku kontroli sygn. […] ustalono również, że: a) w umowie członkowskiej zawieranej z klientem, na którą składają się formularz aplikacyjny o nazwie […] i „Ogólne warunki członkostwa”, brak jest zapisów odnośnie kontroli wejścia do klubów w oparciu o dane biometryczne; b) nie jest pozyskiwana od członków klubów zgoda na przetwarzanie danych

biometrycznych; c) gdy klient nie wyraża chęci korzystania z biometrycznej kontroli dostępu, wówczas taki klient również otrzymuje opaskę (jednakże bramka nie zadziała i osobę taką wpuszcza recepcjonista).

W toku kolejnej kontroli sygn. […] potwierdzono m.in., iż Spółka nie dysponuje pisemnymi oświadczeniami klientów (klubowiczów) o wyrażeniu zgody na przetwarzanie danych biometrycznych, gdyż zdaniem Spółki nie dochodzi w ogóle do przetwarzania przez Spółkę danych biometrycznych tych osób. W toku kontroli wyjaśniono również, że w związku z tym, że szczegóły systemu biometrycznej kontroli wstępu (wymagającego kodowania danej biometrycznej klienta w chipie wydanej mu opaski/ewentualnie nowej karty) były przedstawiane i tłumaczone klientom Spółki, Spółka stoi na stanowisku, że poprzez wybór nowego systemu kontroli wstępu klient wyrażał zgodę na przetwarzanie w tym zakresie jego danych osobowych. Jednocześnie w toku kontroli sygn. […] ustalono, iż zapoznanie się z „regulaminami klubów Spółki", o których mowa w piśmie Pełnomocnika Spółki z dnia […] lipca 2014 r. skierowanym do Generalnego Inspektora Ochrony Danych Osobowych, tj. „Regulaminem korzystania z klubów sportowych […]", „Regulaminem korzystania z basenów w klubach […]", „Regulaminem korzystania z sauny", „Zasadami korzystania z solarium w klubach […]", nie jest w żaden sposób potwierdzane przez klientów Spółki. Jednocześnie w umowie członkowskiej zawieranej z klientami brak jest odniesień co do obowiązywania ww. regulaminów.

Mając na uwadze materiał dowodowy zgromadzony w toku kontroli sygn. […] i sygn. […], jak również odnosząc się do informacji zawartych w pismach Spółki kierowanych do Generalnego Inspektora Ochrony Danych Osobowych należy stwierdzić, co następuje.

Nie można zgodzić się ze stanowiskiem Spółki, że stosowanie systemu biometrycznej kontroli wstępu w prowadzonych przez Spółkę klubach nie prowadzi do przetwarzania danych osobowych, z uwagi na fakt, że dane te nie umożliwiają identyfikacji osoby bez poniesienia nadmiernych nakładów.

Zgodnie bowiem z art. 6 ust. 1 ustawy o ochronie danych osobowych, w rozumieniu ustawy za dane osobowe uważa się wszelkie informacje dotyczące zidentyfikowanej lub możliwej do zidentyfikowania osoby fizycznej. Natomiast stosownie do ust. 2 powołanego przepisu, osobą możliwą do zidentyfikowania jest osoba, której tożsamość można określić bezpośrednio lub pośrednio, w szczególności przez powołanie się na numer identyfikacyjny albo jeden lub kilka specyficznych czynników określających jej cechy fizyczne, fizjologiczne, umysłowe, ekonomiczne, kulturowe lub społeczne.

Nie ulega wątpliwości, że klientami Spółki są osoby zidentyfikowane, ponieważ Spółka przetwarza ich dane osobowe w postaci papierowej, tj. umów członkowskich (formularz aplikacyjny o nazwie […] i „Ogólne warunki członkostwa"), a także w systemie informatycznym

Spółki o nazwie „A”. W tym kontekście należy wskazać, że przetworzona do postaci cyfrowej dana biometryczna jest informacją dotyczącą zidentyfikowanej osoby fizycznej (klienta) przez Spółkę. Informacja ta przetwarzana jest w systemie informatycznym Spółki opartym o czytniki biometryczne. Spółka wykorzystuje ww. informację w celu potwierdzenia, że osoba, która posługuje się opaską (z wprowadzonymi danymi biometrycznymi) jest klientem, któremu wydano tę opaskę i którego dane przetwarzane są przez Spółkę w systemie informatycznym o nazwie „A” w związku z zawartą umową członkowską. Należy podkreślić, że w pamięci czytnika należącego do Spółki, do chwili zakończenia operacji porównania wzorca biometrycznego, jest przetwarzana dana biometryczna klienta Spółki (czytnik linii papilarnych sczytuje punkty biometryczne z palca, przetwarza je w kod i porównuje z kodem zapisanym na opasce) i wobec tego faktu należy uznać, że Spółka przetwarza dane biometryczne swoich klientów w celu zapewnienia kontroli wstępu do wybranych klubów. Biorąc za podstawę definicję danych osobowych sformułowaną w myśl art. 6 ustawy o ochronie danych osobowych, należy uznać, że dane biometryczne klientów przetworzone do postaci zapisu cyfrowego, stanowią dane osobowe w rozumieniu powołanego przepisu. W wyniku zestawienia kodu cyfrowego zapisanego na opasce z kodem cyfrowym wygenerowanym on-line przez oprogramowanie czytnika w związku z przyłożeniem palca klienta możliwe jest bowiem potwierdzenie przez Spółkę tożsamości klienta i jego identyfikacja na podstawie zapisanego na karcie elektronicznej numeru ID.

Nie można zgodzić się również ze stanowiskiem Spółki, że zbiór danych jest sporządzany przez Spółkę doraźnie, wyłącznie ze względów technicznych, a dane podlegają natychmiastowemu usunięciu (co ogranicza stosowanie ustawy o ochronie danych osobowych do rozdziału V). W ocenie Generalnego Inspektora Ochrony Danych Osobowych Spółka przetwarza dane osobowe biometryczne swoich klientów i jest administratorem tych danych osobowych przetwarzanych w zbiorze danych osobowych klientów Spółki. W piśmiennictwie podnosi się, że art. 2 ust. 3 ustawy o ochronie danych osobowych może być rozumiany jako zawierający wyliczenie cech definicyjnych zbioru doraźnego, w sposób kumultatywny bądź też alternatywny. Według dominującego stanowiska przesłanka „doraźności” nie ma charakteru samodzielnego, spełnienie tej przesłanki jest konieczne, niemniej wymaga uzupełnienia poprzez względy natury technicznej, szkoleniowej lub dydaktycznej (Janusz Barta, Paweł Fajgielski, Ryszard Markiewicz, Ochrona danych osobowych Komentarz 4 Wydanie, Wolters Kluwer Polska Sp. z o.o., str. 317 – 318). Przy ocenie doraźności należy odwoływać się do okoliczności faktycznych towarzyszących przetwarzaniu danych dla określonych celów. W przypadku Spółki celem pozyskiwania przez Spółkę danych biometrycznych klientów w postaci cyfrowego obrazu linii papilarnych jest zapewnienie kontroli wstępu do klubów prowadzonych przez Spółkę. Ze względu na to, iż dane osobowe biometryczne przetwarzane są w zbiorze danych klientów Spółki i celem ich gromadzenia

jest zapewnienie kontroli wstępu do klubów, a także z uwagi na to, że zbiór danych nie jest tworzony jedynie ze względów technicznych, nie można uznać tego zbioru jako sporządzanego doraźnie (nie zmienia tego okoliczność, że okres przetwarzania danych biometrycznych jest relatywnie krótki, a same dane biometryczne wprowadzane są do zbioru danych klientów Spółki pojedynczo).

Natomiast w umowie członkowskiej zawieranej z klientem, na którą składają się: formularz aplikacyjny o nazwie […] i Ogólne warunki członkostwa", brak jest zapisów odnośnie kontroli wejścia do klubów w oparciu o dane biometryczne. Klient zawierając umowę członkowską ze Spółką godzi się, iż jego dane będą przetwarzane w celu jej realizacji wyłącznie w zakresie podanym i wynikającym z treści umowy. Z uwagi na fakt, iż dokumenty składające się na umowę członkowską obowiązującą w Spółce nie zawierają żadnych informacji wskazujących, iż wstęp do klubów Spółki będzie możliwy w oparciu o udostępnienie danych biometrycznych członka klubu i konieczne jest w związku z tym przetwarzanie tych danych przez Spółkę *(co więcej w pkt* […] *„Ogólnych warunków członkostwa" wskazano wyłącznie, że „Wstęp do Klubów* […] *jest możliwy tylko za okazaniem* […]*)*, nie można uznać, iż Spółka legitymuje się przesłanką przetwarzania danych osobowych - biometrycznych, o której mowa w art. 23 ust. 1 pkt 3 ww. ustawy. Warunki zawartych z klientami umów członkowskich, obejmujące sposób wstępu do klubów Spółki, nie przewidują zatem pozyskiwania przez Spółkę dodatkowych danych osobowych jakimi są dane biometryczne w związku z korzystaniem z usług świadczonych przez ww. kluby.

Nie można również uznać, że w obecnym stanie faktycznym Spółka legitymuje się przesłanką przetwarzania danych osobowych (biometrycznych) swoich klientów wskazaną w art. 23 ust. 1 ustawy o ochronie danych osobowych, tj. zgodą osoby, której dane dotyczą. Zgodnie z art. 7 pkt 5 ww. ustawy, wyrażenie zgody ma charakter oświadczenia woli, którego treścią jest zezwolenie na przetwarzanie danych osobowych składającego oświadczenie. Zgoda nie może być domniemana lub dorozumiana z oświadczenia woli o innej treści. W toku kontroli sygn. […], jak i w toku kontroli sygn. […] ustalono, że nie jest pozyskiwana od klientów zgoda na przetwarzanie ich danych biometrycznych, w tym pisemne oświadczenia klientów o wyrażeniu zgody (z uwagi na fakt, iż zadaniem Spółki dane te nie stanowią danych osobowych w rozumieniu ustawy o ochronie danych osobowych, a zatem Spółka nie staje się administratorem danych osobowych biometrycznych klienta). W toku kontroli sygn. […] ustalono również, że przed wprowadzeniem w klubach Spółki systemu biometrycznej kontroli wstępu przeprowadzono szkolenie w zakresie funkcjonowania tego systemu oraz potrzeby wyjaśniania klientom zasad jego funkcjonowania. W trakcie szkolenia przekazano menadżerom klubów m.in. informację, że cyt. „dane będą przetwarzane wyłącznie na opasce, która będzie stanowiła własność klienta". W trakcie szkolenia nie przekazano jego

uczestnikom informacji o konieczności wystąpienia (przez pracownika klubu) do klienta z pytaniem o wyrażenie zgody na przetwarzanie jego danych biometrycznych przez Spółkę. W świetle powyższych ustaleń nie można zgodzić się, iż z faktu zarejestrowania danych biometrycznych klienta (w opasce) należy założyć, że klient wyraża zgodę na przetwarzanie przez Spółkę jego danych biometrycznych. Bowiem z definicji „zgody osoby, której dane dotyczą" (art. 7 pkt 5 ustawy o ochronie danych osobowych) wynika wprost, że zgoda nie może być domniemana lub dorozumiana z oświadczenia woli o innej treści. W piśmiennictwie podkreśla się, że cyt. „Brzmienie komentowanego przepisu skłania do wniosku, iż zgoda nie może być wyrażona per facta concludentia. (...) W tym kontekście należy też opowiedzieć się za tym, że zgoda na przetwarzanie danych nie może być wyrażona poprzez milczenie lub inne tylko „pasywne" działanie (...)" (Janusz Barta, Paweł Fajgielski, Ryszard Markiewicz, Ochrona danych osobowych Komentarz 4 Wydanie, Wolters Kluwer Polska Sp. z o.o., str. 386 – 387). Odnosząc się natomiast do zarzutu podniesionego przez Spółkę co do braku uprawnień organu ochrony danych osobowych w zakresie badania skuteczności wyrażenia zgody (co wynika zdaniem Spółki z uzasadnienia do wyroku Naczelnego Sądu Administracyjnego w Warszawie z dnia 1 grudnia 2009 r., I OSK 249/06), należy stwierdzić, iż w toku postępowania administracyjnego nie stwierdzono jakichkolwiek oświadczeń woli w przedmiocie wyrażenia przez klientów Spółki zgody na przetwarzanie ich danych biometrycznych, w związku z tym taka ocena nie mogła być dokonana. Zdaniem Generalnego Inspektora Ochrony Danych Osobowych Spółka nie przetwarza danych osobowych biometrycznych na podstawie art. 23 ust. 1 pkt 1 ustawy o ochronie danych osobowych, bowiem zgoda nie może być domniemana lub dorozumiana z oświadczenia woli o innej treści.

W obecnym stanie faktycznym nie zachodzą również inne przesłanki wskazane w art. 23 ust. 1 ustawy stanowiące podstawę prawną przetwarzania tych danych.

Jednocześnie na podstawie złożonych przez Spółkę pisemnych wyjaśnień i załączonego wydruku ewidencji osób upoważnionych do przetwarzania danych osobowych, należy uznać, iż pozostałe uchybienie w procesie przetwarzania danych osobowych, stanowiące przedmiot niniejszego postępowania zostało usunięte, tj.: uzupełniono ww. ewidencję o datę ustania, zakres upoważnienia do przetwarzania danych osobowych oraz identyfikator (w przypadku przetwarzania danych w systemie informatycznym).

Stosownie do art. 105 § 1 Kodeksu postępowania administracyjnego, gdy postępowanie z jakiejkolwiek przyczyny stało się bezprzedmiotowe w całości albo w części, organ administracji publicznej wydaje decyzję o umorzeniu postępowania odpowiednio w całości albo w części. 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 materialnego stosunku prawnego w odniesieniu do jego strony podmiotowej lub przedmiotowej (wyrok NSA z 21 stycznia 1999 r. S.A./Sz1029/97).

Z uwagi na to, iż pozostałe uchybienie będące przedmiotem niniejszego postępowania administracyjnego zostało usunięte, postępowanie należało w tym zakresie umorzyć.

Mając powyższe na uwadze, w tym stanie faktycznym i prawnym, 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.).