



**WYROK**

**W IMIENIU RZECZYPOSPOLITEJ POLSKIEJ**

Dnia 16 grudnia 2015 r.

Wojewódzki Sąd Administracyjny w Warszawie  
w składzie następującym:

Przewodniczący Sędzia WSA – Stanisław Marek Pietras (spraw.)

Sędzia WSA – Andrzej Kołodziej

Sędzia WSA – Janusz Walawski

Protokolant – specjalista Aleksandra Weiher

po rozpoznaniu na rozprawie w dniu 10 grudnia 2015 r.

sprawy ze skargi P.

na decyzję Generalnego Inspektora Ochrony Danych Osobowych

z dnia 4 lutego 2015 r. nr DIS/DEC-71/15/8533

w przedmiocie przetwarzania danych osobowych



– oddala skargę –

Na oryginale właściwe podpisy  
Za zgodność z oryginałem

## UZASADNIENIE

Inspektorzy upoważnieni przez Generalnego Inspektora Ochrony Danych Osobowych, przeprowadzili w Pr

, kontrolę zgodności przetwarzania danych osobowych z przepisami o ochronie danych osobowych, której zakresem objęto przetwarzanie przez spółkę danych biometrycznych w postaci odcisków linii papilarnych swoich klientów, zaś stan faktyczny szczegółowo opisano w protokole kontroli, który został podpisany przez członka Zarządu Spółki.

Na podstawie zgromadzonego podczas 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. niezawarcia w ewidencji osób upoważnionych do przetwarzania danych osobowych identyfikatorów użytkowników przetwarzających dane z wykorzystaniem systemu informatycznego, daty ustanienia 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 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 odnosząc się do pkt 1 zawiadomienia o wszczęciu postępowania administracyjnego wyjaśnił m.in., iż 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 „P...”. Ponadto „system” nie przekazuje wzorców danych do systemu informatycznego spółki i niezwłocznie usuwa je po dokonaniu porównania, „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, 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, stosowane są zabezpieczenia wzorców biometrycznych przed nieuprawnionym dostępem osób trzecich, cechy biometryczne gromadzone incydentalnie przez spółkę nie mogą zostać uznane za dane osobowe, gdyż nie identyfikują one osoby, której dane dotyczą. Ponadto w ocenie spółki, w razie jednak przyjęcia, że dane biometryczne przetwarzane przez spółkę stanowią dane osobowe i dochodzi do ich przetwarzania, to 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). Natomiast 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 o tym, 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. 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 i w tym celu w dniach od do września 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, a 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, zaś 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 „P”, w którym przetwarzane są dane osobowe klientów. W powyższym piśmie zawnioskowano o przedłużeniu postępowania administracyjnego, w tym możliwość złożenia dodatkowych wniosków dowodowych przez spółkę, zaś Generalny Inspektor uwzględnił powyższy wniosek i wskazał, iż termin wydania decyzji administracyjnej w sprawie przetwarzania danych osobowych przez spółkę zostaje przedłużony do dnia października 2014 r., jednakże spółka nie złożyła żadnych wniosków dowodowych.

W tej sytuacji Generalny Inspektor Ochrony Danych Osobowych decyzją z dnia 6 listopada 2014 r. nr DIS/DEC-1072/14/87525, działając na podstawie art. 104 § 1 i art. 105 k.p.a., art. 12 pkt 2, art. 18 ust. 1 pkt 1, art. 22 w zw. 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):

I. nakazał P

, 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 umorzono.

W uzasadnieniu – powołując się na opisany powyżej stan faktyczny – podano, że 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 rozpoznawanej sprawie ustalono zaś, 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 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 czytuje z opaski zapisany kod punktów biometrycznych i po przyłożeniu przez klienta palca do czytnika linii papilarnych czytuje punkty biometryczne z palca, przetwarza je w kod i porównuje z kodem zapisanym na opasce. Jednocześnie wysyłany jest do systemu informatycznego o nazwie „P” (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 „F” nie są przechowywane dane biometryczne klientów, zapisany jest natomiast m.in. nr ID opaski. W toku kontroli ustalono również, że: a) w umowie członkowskiej zawieranej z klientem, na którą składają się formularz aplikacyjny o nazwie „P” i „Formularz Aplikacyjny” 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 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 nią danych biometrycznych tych osób. W toku kontroli wyjaśniono również, że w związku z tym, iż szczegóły systemu biometrycznej kontroli wstępu (wymagającego kodowania danej biometrycznej klienta w chipie wydanej mu opaski/ewentualnie nowej karty) były przedstawiane i tłumaczone klientom, to 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 ustalono, iż zapoznanie się z „Regulaminem korzystania z klubów sportowych J. ....”, „Regulaminem korzystania z basenów w klubach J. ....”, „Regulaminem korzystania z sauny”, „Zasadami korzystania z solarium w klubach J. ....”, nie jest w żaden sposób potwierdzane przez klientów spółki. Jednocześnie w umowie członkowskiej zawieranej z klientami brak jest odniesień co do obowiązywania powyższych regulaminów. Zatem – mając na uwadze powyższe ustalenia – 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 „P. .... Formularz Aplikacyjny” i „Ogólne warunki członkostwa”), a także w systemie informatycznym spółki o nazwie „P. ....”. W tym kontekście wskazano, 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 powyższą 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 „P. ....” w związku z zawartą umową członkowską. Podkreślono, że w pamięci czytnika należącego do spółki, do chwili zakończenia operacji porównania wzorca biometrycznego, jest przetwarzana dana biometryczna klienta spółki (czytnik linii papilarnych czytuje punkty biometryczne z palca, przetwarza je w kod i porównuje z

kodek 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 art. 6 ustawy o ochronie danych osobowych uznano, 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 kodek 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), bowiem 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 kumulatywny 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 „P Formularz Aplikacyjny” 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 3.1 „Ogólnych warunków członkostwa” wskazano wyłącznie, że wstęp do Klubów jest możliwy tylko za okazaniem karty członkowskiej (...), nie można uznać, iż spółka legitymuje się przesłanką przetwarzania danych osobowych – biometrycznych, o której mowa w art. 23 ust. 1 pkt 3 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 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, a w toku kontroli 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 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. Z definicji bowiem „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 „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 wskazano, 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. Zatem 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 uznano, że 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 zaś do art. 105 § 1 k.p.a., gdy postępowanie z jakiegokolwiek 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 jakiegokolwiek przyczyny”, czyli z każdej przyczyny powodującej brak jednego z elementów

materialnego stosunku prawnego w odniesieniu do jego strony podmiotowej lub przedmiotowej. Z uwagi na to, iż pozostałe uchybienie będące przedmiotem niniejszego postępowania administracyjnego zostało usunięte, postępowanie należało w tym zakresie umorzyć.

We wniosku z dnia 3 grudnia 2014 r. do Generalnego Inspektora Ochrony Danych Osobowych o ponowne rozpatrzenie sprawy w zakresie punktu I decyzji, wniesiono o jego uchylenie oraz umorzenie postępowania w sprawie przetwarzania danych osobowych przez spółkę z tym zakresie, zarzucając naruszenie art. 2 ust. 1 w zw. z art. 6 i 7 pkt 1 oraz art. 2 ust. 3 i art. 23 ust. 1 pkt 3, a ponadto art. 23 ust. 1 pkt 1 w zw. z art. 7 pkt 5 ustawy o ochronie danych osobowych. W uzasadnieniu podano, że:

1. ze stanu faktycznego przyjętego za podstawę wydania zaskarżonej decyzji nie wynika, aby spółka przetwarzała dane osobowe swoich klientów w postaci danych biometrycznych. Z ustalonego stanu faktycznego wynika jedynie, że podczas kontroli wstępu do klubów prowadzonych przez spółkę, spółka przetwarza dane osobowe klienta w postaci jego numeru karty identyfikacyjnej, który jest skorelowany z systemem informatycznym spółki o nazwie „P”.
2. organ nie wykazał, w jaki sposób stosowanie biometrycznego systemu kontroli wstępu, prowadzi do powstania zbioru danych osobowych w rozumieniu ustawy o ochronie danych osobowych (a więc posiadającego strukturę zestawu danych o charakterze osobowym, dostępnych według określonych kryteriów).
3. organ nie wskazał z jakich okoliczności stanu faktycznego wynika, że dane biometryczne nie są przetwarzane przez spółkę w warunkach art. 2 ust. 3 ustawy o ochronie danych osobowych, zgodnie z którym, w odniesieniu do zbiorów danych osobowych sporządzanych doraźnie, wyłącznie ze względów technicznych, szkoleniowych lub w związku z dydaktyką w szkołach wyższych, a po ich wykorzystaniu niezwłocznie usuwanych albo poddanych anonimizacji, mają zastosowanie jedynie przepisy rozdziału 5 ustawy o ochronie danych osobowych zatytułowanego „Zabezpieczenie danych osobowych”.
4. organ błędnie ustalił, że klienci nie wyrażają zgody na wykonywanie operacji na ich danych biometrycznych.
5. dokonując oceny zaistnienia przesłanki legitymizującej przetwarzanie danych w postaci konieczności realizacji umowy organ nie uwzględnił nowej treści „Ogólnych

warunków członkostwa", którymi posługuje się Spółka od dnia      października 2014 r.:

„3.1 Wstęp do Klubów P      następuje przy użyciu karty albo opaski członkowskiej, stanowiącej własność Członka.

3.2 W celu zapewnienia bezpieczeństwa, a w szczególności ograniczenia dostępu do pomieszczeń Klubów P      osobom nieupoważnionym, kontrola wstępu do Klubów P      może odbywać się z wykorzystaniem biometrycznego systemu weryfikacji, przy pomocy opaski członkowskiej zawierającej kod alfanumeryczny utworzony na podstawie danych biometrycznych Członka. P      nie gromadzi ani nie przechowuje danych biometrycznych. Kod alfanumeryczny zapisany jest wyłącznie na opasce i jest chroniony przed nieuprawnionym dostępem przez osoby trzecie przez zastosowanie mechanizmów kryptograficznych.

3.3 Do korzystania z karty albo opaski członkowskiej uprawniony jest wyłącznie Członek, o ile nie zastrzeżono inaczej. W przypadku utraty lub zniszczenia karty albo opaski i konieczności wystawienia nowej, Członek zobowiązany jest do wniesienia dodatkowej opłaty, zgodnie z cennikiem obowiązującym w Klubie. Każda karta i opaska członkowska posiada numer ID umożliwiający weryfikację uprawnień członkowskich w systemie informatycznym P      ”.

Jako dowód spółka załączyła na potwierdzenie złożonych wyjaśnień do wniosku o ponowne rozpatrzenie sprawy formularz o nazwie „      Formularz aplikacyjny” oraz „Ogólne warunki członkostwa”.

W związku z tym, iż załączony dowód dotyczył innego podmiotu niż spółka

Generalny Inspektor pismem z dnia      stycznia 2015 r. nr DIS-K-421/7/14, DIS-K-421/124/14/1715/15 wystąpił do spółki o przesłanie właściwego formularza aplikacyjnego wraz z ogólnymi warunkami członkostwa i dokument taki został przesłany do za pismem z dnia :      stycznia 2015 r.

Generalny Inspektor Ochrony Danych Osobowych decyzją z dnia 4 lutego 2015 r. nr DIS/DEC-71/15/8533, mając za podstawę art. 138 § 1 pkt 1 k.p.a., utrzymał w mocy zaskarżoną decyzję. W uzasadnieniu – powołując się na opisany powyżej stan faktyczny oraz argumentację zawartą w zaskarżonej decyzji – podano, że nie można zgodzić się z opinią spółki, iż „operacja (przetwarzania danych biometrycznych klienta) odbywa się w czytniku, poza jakimkolwiek systemem informatycznym Spółki”. Nie można także zgodzić się z zarzutem, iż z ustalonego (w



toku ww. kontroli) stanu faktycznego nie wynika, aby spółka przetwarzała dane osobowe swoich klientów w postaci danych biometrycznych, natomiast „wynika jedynie, że podczas kontroli wstępu, spółka przetwarza dane osobowe klienta w postaci jego numeru karty identyfikacyjnej, który jest skorelowany z systemem P. i którego przetwarzanie jest ujawnione w rejestrze prowadzonym przez Organ”. Stosownie do definicji systemu informatycznego wskazanej w art. 7 pkt 2a ustawy o ochronie danych osobowych, przez system informatyczny rozumie się zespół współpracujących ze sobą urządzeń, programów, procedur przetwarzania informacji i „narzędzi” programowych zastosowanych w celu przetwarzania danych. Uwzględniając ww. definicję przy ocenie stanu faktycznego stwierdzono, iż na system informatyczny spółki składają się systemy „P. . . . Admin”, system biometrycznej kontroli dostępu, urządzenia (w tym stacje komputerowe, urządzenia zapisujące dane biometryczne, czytniki danych biometrycznych, nośniki danych biometrycznych – opaski wydawane klientom spółki), opracowane i wdrożone procedury. Dlatego nie można zgodzić się z argumentacją, że przetwarzanie danych biometrycznych klientów odbywa się poza jakimkolwiek systemem informatycznym spółki, gdyż czytniki biometryczne (podobnie jak opaski wydawane na własność klientom spółki) są elementem systemu informatycznego spółki. Spółka przetwarza dane osobowe klientów (m.in. imię, nazwisko, adres, nr PESEL) zarówno w postaci papierowej, tj. umów członkowskich (formularz o nazwie „P. . . . Formularz Aplikacyjny” i „Ogólne warunki członkostwa”), jak i w systemie informatycznym o nazwie „P. . . . Klientami Spółki są zatem osoby zidentyfikowane. Przetworzona do postaci cyfrowej dana biometryczna takiego klienta jest więc informacją dotyczącą zidentyfikowanej osoby fizycznej. Mając na względzie, iż zgodnie z art. 6 ust. 1 ustawy o ochronie danych osobowych, za dane osobowe uważa się wszelkie informacje dotyczące zidentyfikowanej lub możliwej do zidentyfikowania osoby fizycznej, to również przetworzona do postaci zapisu cyfrowego dana biometryczna klienta jest daną osobową. Informacja ta przetwarzana jest w systemie informatycznym spółki opartym o czytniki biometryczne i wykorzystywana w celu potwierdzenia, że osoba, która posługuje się opaską (z wprowadzonymi danymi biometrycznymi) jest klientem, któremu tę opaskę wydano i którego dane przetwarzane są przez Spółkę w systemie informatycznym o nazwie „P. . . . w związku z zawartą umową członkowską. Każdorazowo przy wejściu do klubu spółki w pamięci czytnika należącego do spółki, do chwili zakończenia

operacji porównania wzorca biometrycznego, jest przetwarzana dana biometryczna klienta Spółki, gdyż czytnik linii papilarnych czytuje punkty biometryczne z przyłożonego do czytnika palca, przetwarza je w kod i porównuje z kodem zapisanym na opasce. W wyniku zestawienia kodu cyfrowego zapisanego na opasce z kodem cyfrowym wygenerowanym on-line przez oprogramowanie czytnika w związku z przyłożeniem palca możliwe jest potwierdzenie tożsamości klienta i jego identyfikacja na podstawie zapisanego numeru ID opaski. Nie można również podzielić argumentacji spółki wskazującej na brak przetwarzania danych osobowych klientów spółki (danych biometrycznych) w zbiorze danych osobowych prowadzonym przez spółkę, bowiem spółka zgłosiła do rejestracji zbiór danych osobowych o nazwie „P” i w zbiorze tym przetwarzane są dane osobowe klientów spółki, m.in. w systemie „P” (poprzednia nazwa systemu to „P.”).

Spółka nie wskazała informacji o pozyskiwaniu danych biometrycznych członków klubu, kierując się tym, iż dane biometryczne wprowadzane m.in. do czytników biometrycznych nie są możliwe do powiązania przez Spółkę z innymi danymi osobowymi tych członków klubu, w szczególności przetwarzanymi w systemie informatycznym o nazwie „P”. Miała również na uwadze fakt, iż dane biometryczne nie są przechowywane w tych czytnikach (jak i w urządzeniach umożliwiających zapisanie danych biometrycznych na chipie opaski). Wbrew opinii spółki przetwarzana dana biometryczna powiązana jest z danymi osobowymi klienta spółki przetwarzanymi w systemie o nazwie „P”, poprzez numer ID. Dana biometryczna zindywidualizowanego klienta w postaci zapisu cyfrowego jest pozyskiwana do zbioru danych osobowych klientów spółki (zgłoszonego do rejestracji Generalnemu Inspektorowi). Dane osobowe klientów przetwarzane przez spółkę (m.in. w systemie „P”) wraz z ich danymi biometrycznymi tworzą posiadający strukturę zestaw danych o charakterze osobowym, dostępnych według określonych kryteriów, a więc zbiór danych w rozumieniu art. 7 pkt 1 ustawy o ochronie danych osobowych. Nie zachodzą zatem okoliczności, które przemawiałyby za uznaniem zbioru danych osobowych klientów spółki, w którym przetwarzane są dane biometryczne, za sporządzony w warunkach art. 2 ust. 3 ustawy o ochronie danych osobowych, zaś w zaskarżonej decyzji przedstawiono stanowisko, dlaczego nie można uznać tego zbioru jako sporządzonego doraźnie. W dalszej części wskazano, że nie uwzględniono nowej treści „Ogólnych warunków członkostwa”, którymi posługuje się spółka od dnia

października 2014 r., bowiem dowody w tym zakresie nie wpłynęły do Biura Generalnego Inspektora Ochrony Danych Osobowych przed jej wydaniem pomimo uwzględnienia wniosku pełnomocnika spółki zawartego w piśmie z dnia września 2014 r. dotyczącego możliwości złożenia przez spółkę kolejnych wniosków dowodowych. W dniu grudnia 2014 r. wpłynął do Biura Generalnego Inspektora Ochrony Danych Osobowych wniosek o ponowne rozpatrzenie sprawy, do którego załączono jako dowód formularz aplikacyjny i ogólne warunki członkostwa dotyczące innego podmiotu niż Spółka, tj. Dlatego

pismem z dnia stycznia 2015 r. Generalny Inspektor zwrócił się do pełnomocnika Spółki o przesłanie dowodu w postaci właściwego formularza aplikacyjnego wraz z ogólnymi warunkami członkostwa. Dowód taki wpłynął do Biura Generalnego Inspektora drogą elektroniczną w dniu stycznia 2015 r. Spółka w pkt 3.2. ogólnych warunków członkostwa informuje klientów, iż w celu zapewnienia bezpieczeństwa, a w szczególności ograniczenia dostępu do pomieszczeń klubów spółki osobom nieupoważnionym, kontrola wstępu i może odbywać się z wykorzystaniem biometrycznego systemu weryfikacji, przy pomocy opaski członkowskiej zawierającej kod alfanumeryczny utworzony na podstawie danych biometrycznych członka. Jednakże w kolejnym zdaniu informuje, że „nie gromadzi ani nie przechowuje danych biometrycznych”, jednakże informacja ta nie jest zgodna ze stanem faktycznym stwierdzonym w toku kontroli, ponieważ każdorazowo przy wejściu do klubu dane biometryczne klientów wprowadzane są do czytników spółki (będących częścią systemu informatycznego Spółki), a więc są gromadzone przez spółkę. Po analizie powyższych dokumentów składających się na umowę członkowską obowiązującą w spółce od dnia października 2014 r. stwierdzono, że warunki zawartych z klientami umów członkowskich, obejmujące sposób wstępu do klubów spółki, nie przewidują pozyskiwania (przetwarzania) przez spółkę dodatkowych danych osobowych, jakimi są dane biometryczne w związku z korzystaniem z usług świadczonych przez ww. kluby (nadal brak jest postanowienia wskazującego, iż wstęp do klubów spółki będzie się odbywał w oparciu o udostępnianie danych biometrycznych spółce). Brak takiego postanowienia skutkuje tym, iż klient sądzi, że spółka nie przetwarza jego danych osobowych biometrycznych i nie staje się również ich administratorem. Dlatego nie można uznać, że spółka przetwarzając dane osobowe biometryczne ww. klientów legitymuje się podstawą prawną do ich przetwarzania, o jakiej mowa w art. 23 ust. 1 pkt 3 ustawy o ochronie danych

osobowych. Na podstawie materiału dowodowego zgromadzonego w sprawie należy również dodatkowo wskazać, że dokumenty składające się na umowę członkowską obowiązującą w spółce przed październikiem 2014 r. nie zawierają żadnych postanowień wskazujących, że wstęp do klubów spółki będzie możliwy także w oparciu o udostępnienie danych biometrycznych członka klubu i w takim przypadku konieczne jest przetwarzanie tych danych przez spółkę. Zatem w odniesieniu do klientów, którzy zawarli ze spółką umowę przed październikiem 2014 r., spółka również nie posiada podstawy prawnej przetwarzania ich danych osobowych biometrycznych, wskazanej w art. 23 ust. 1 pkt 3 ustawy o ochronie danych osobowych. Ponadto nie sposób podzielić stanowiska Spółki, że „ewentualne” przetwarzanie danych (biometrycznych) jest legitymizowane wyrażeniem zgody przez klientów spółki (art. 23 ust. 1 pkt 1 ustawy o ochronie danych osobowych). Zatem ponownie wskazano, że w trakcie przeprowadzonych w spółce kontroli ustalono, iż nie jest pozyskiwana od klientów zgoda na przetwarzanie ich danych biometrycznych, w tym pisemne oświadczenia klientów o wyrażeniu takiej zgody (ze względu na fakt, iż zdaniem 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). Ponadto w toku kontroli sygn. DIS-K- ustalono, że przed wprowadzeniem w klubach Spółki systemu w trakcie szkolenia pracowników nie przekazano informacji o konieczności wystąpienia (przez pracownika klubu) do klienta z pytaniem o wyrażenie zgody na przetwarzanie jego danych biometrycznych przez spółkę. Zatem nie można zgodzić się, iż z faktu zarejestrowania danych biometrycznych klienta (w opasce przekazywanej na własność klientowi) należy założyć, że klient wyraża zgodę na przetwarzanie przez spółkę jego danych osobowych i w toku postępowania administracyjnego nie stwierdzono, aby spółka odbierała jakiegokolwiek oświadczenie woli w przedmiocie wyrażenia przez klientów spółki zgody na przetwarzanie ich danych biometrycznych. Stąd też spółka nie przetwarza danych biometrycznych swoich klientów na podstawie art. 23 ust. 1 pkt 1 ustawy, zaś okoliczność pozyskania zgody przez czynności dorozumiane nie może stanowić podstawy prawnej przetwarzania danych o czym stanowi art. 7 pkt 5 ustawy o ochronie danych osobowych.

W skardze do Wojewódzkiego Sądu Administracyjnego w Warszawie, skarżąca P. wniosła o uchylenie zaskarżonej decyzji



w całości i poprzedzającej ją decyzji w pkt I oraz zwrot kosztów postępowania według norm przepisanych zarzucając:

1. naruszenie art. 6 ust. 3 w zw. z ust. 1 i ust. 2 ustawy z dnia 29 sierpnia 1997 r. o ochronie danych osobowych (Dz. U. z 2014 r., poz. 1182, dalej jako "Ustawa") poprzez ich błędne zastosowanie i przyjęcie, że stosowanie biometrycznej kontroli wstępu do prowadzonych przez skarżącą klubów prowadzi do przetwarzania danych osobowych, tj. informacji dotyczących zidentyfikowanych lub możliwych do zidentyfikowania osób fizycznych, których tożsamość można określić na podstawie tych informacji bezpośrednio lub pośrednio, podczas gdy te dane biometryczne nie umożliwiają określenia tożsamości osoby bez poniesienia nadmiernych kosztów i tym samym nie stanowią danych osobowych w rozumieniu ustawy;

2. naruszenie art. 2 ust. 3 ustawy poprzez jego błędną wykładnię i przyjęcie, że – w przypadku uznania, iż dane biometryczne w okolicznościach sprawy stanowią dane osobowe w rozumieniu ustawy – skarżąca przetwarza te dane biometryczne w zbiorze danych osobowych innym niż sporządzanym doraźnie (co wyłącza zastosowanie do nich przepisów ustawy za wyjątkiem rozdziału V Ustawy), choć ocena zgromadzonego w sprawie materiału dowodowego jednoznacznie wskazuje na dorażność przetwarzania tych danych biometrycznych ze względów technicznych związanych ze sposobem funkcjonowania biometrycznego systemu kontroli wstępu do prowadzonych przez skarżącego klubów;

3. naruszenie art. 23 ust. 1 pkt 3 Ustawy oraz art. 23 ust. 1 pkt 1 w zw. z art. 7 pkt 5 ustawy poprzez ich błędną wykładnię i przyjęcie, że – w przypadku uznania, że dane biometryczne w okolicznościach sprawy stanowią dane osobowe w rozumieniu ustawy, a skarżąca dane takie przetwarza w zbiorze danych osobowych innym niż sporządzanym doraźnie – skarżąca nie legitymuje się żadną z podstaw prawnych do przetwarzania takich danych wskazanych w tych przepisach ustawy, tj. koniecznością do realizacji umowy, gdy osoba, której dane dotyczą, jest jej stroną ani też że osoba taka wyraziła zgodę na przetwarzanie tych danych, podczas gdy zgodnie ze zgromadzonym w sprawie materiałem dowodowym wzorzec umowny, na podstawie którego zawierana jest umowa z osobą, której dane dotyczą, wyraźnie przewiduje możliwość wykorzystania biometrycznego systemu kontroli wstępu dla takiej osoby, a skorzystanie z niego warunkowane jest zgodą takiej osoby, która nie jest domniemana lub dorozumiana z oświadczenia woli takiej osoby o innej treści.

W uzasadnieniu podano, że sam kod alfanumeryczny przetworzony z zapisu odcisku palca i zapisany na opasce nie pozwala na podanie informacji o tożsamości osoby, do której ona należy. Ustalenie na jego podstawie tożsamości osoby wiązałoby się z trudnymi do oszacowania lecz znacznymi i nieproporcjonalnymi kosztami. To numer identyfikacyjny (ID) opaski, który jest wysyłany do systemu informatycznego Spółki (P...), za pomocą którego przetwarzane są przez spółkę dane osobowe w zbiorze danych, stanowi daną umożliwiającą identyfikację określonej osoby, a tym samym daną osobową. Funkcja kodu alfanumerycznego jest zatem ograniczona wyłącznie do weryfikacji przez porównanie danych właściciela opaski z danymi osoby posługującej się tą opaską. Innymi słowy, funkcja czytników biometrycznych ogranicza się jedynie do potwierdzenia, że osoba, która próbuje wejść do klubu spółki, jest właścicielem opaski. Pomiedzy czytnikami a systemami informatycznymi spółki służącymi do przetwarzania danych osobowych (które to dane pozwalają w sposób jednoznaczny na zidentyfikowanie danej osoby), nie dochodzi zaś do przepływu danych biometrycznych, które zasilająby zestaw danych osobowych o takiej osobie, które przetwarza spółka w zbiorze danych. Ponadto w toku sczytywania danych biometrycznych, a następnie przetwarzania w kod alfanumeryczny przez czytnik biometrycznej weryfikacji, nie powstaje relewantny dla stosowania ustawy (z wyłączeniem jej rozdziału V) zbiór danych osobowych. Dane biometryczne bowiem (przy przyjęciu, że stanowią dane osobowe w rozumieniu ustawy) są sczytywane pojedynczo i po chwili niezwłocznie usuwane i wbrew twierdzeniom organu, dane te zarazem są zbierane wyłącznie ze względów technicznych związanych ze sposobem funkcjonowania mechanizmu biometrycznej kontroli wstępu. Zatem z uwagi na incydentalny i doraźny charakter przetwarzania pojedynczych danych biometrycznych przez spółkę, które następnie niezwłocznie podlegają usunięciu, i nie prowadzą do:

1. powstania zestawu danych, bo dane nie są przechowywane w żadnej postaci – nawet nieuporządkowanej,
2. wobec braku istnienia zestawu, nie może on być uporządkowany;
3. wobec niezwłocznego usuwania z czytników biometrycznych poszczególnych danych nie są one dostępne dla spółki.

W dalszej części wskazano, że w przypadku uznania, iż dane biometryczne w okolicznościach sprawy stanowią dane osobowe w rozumieniu ustawy, a skarżąca dane takie przetwarza w zbiorze danych osobowych innym niż sporządzanym

doraźnie (czemu skarżący zaprzecza), nietrafne jest twierdzenie organu, jakoby spółka przetwarzała ww. dane bez podstaw prawnych z ustawy. Od dnia października 2014 r. spółka posługuje się nowym formularzem aplikacyjnym oraz nowymi "Ogólnymi warunkami członkostwa" ("OWU"), które zawierają postanowienia precyzujące, że kontrola wstępu do klubów spółki może odbywać się za pomocą biometrycznego systemu weryfikacji i specjalnej opaski członkowskiej i w tym miejscu wskazano treść pkt 3.1 – 3.3. Nie sposób się zgodzić ze stanowiskiem organu, że samo sformułowanie „P nie gromadzi ani nie przechowuje danych biometrycznych” przesądza o braku spełnienia warunków tej przesłanki legalizującej przetwarzanie ww. danych. Mianowicie z tego powodu, że opis mechanizmu funkcjonowania biometrycznej weryfikacji kontroli dostępu jest w pełni zgodny z ustalonym w stanie faktycznym. W sposób jasny i zrozumiały ww. postanowienia OWU wyjaśniają istotę działania mechanizmu biometrycznego. Osoba, której dane dotyczą, ma zatem pełną wiedzę o tym, w jaki sposób jej dane biometryczne będą przetwarzane w tym procesie. Istotą zaś cytowanego przez organ fragmentu postanowienia pkt. 3.2 było zapewnienie takiej osoby, że spółka nie przetwarza tych danych dla jakichkolwiek innych celów aniżeli kontrola wejścia. Ponadto uwzględnienie w OWU alternatywnego mechanizmu kontroli wejść do klubów, na które osoba, której te dane dotyczą, dobrowolnie godzi się, i która jest objęta zgodą obu stron stosunku zobowiązaniowego, w pełni realizuje przesłankę z art. 23 ust. 1 pkt 3 ustawy. Nawet przy przyjęciu (czemu skarżący zaprzecza), że cytowane przez organ w decyzji sformułowanie ww. postanowienia OWU nie jest zgodne – zdaniem Organu – z kwalifikacją prawną czynności na danych biometrycznych przeprowadzanych przez spółkę, to osoba, której te dane dotyczą, działa z pełnym rozeznanem odnośnie do istoty tego mechanizmu i świadomie obejmuje swoim oświadczeniem woli taki właśnie sposób realizowania umowy ze spółką opartej na wzorcu umownym, tj. OWU. Dalej stwierdzono, że zgoda wyrażana przez klientów nie jest w żadnym wypadku dorozumiana z oświadczenia woli o innej treści i organ nie wykazał z jakiego to oświadczenia woli skarżący domniemuje zgody na przetwarzanie danych biometrycznych oraz podkreślono, że nie sposób zgodzić się ze stanowiskiem organu popartym zacytowanym fragmentem jednego z komentarzy, jakoby udzielenie zgody nie mogło w żadnych okolicznościach nastąpić w drodze czynności w pełni świadomej, dobrowolnej i wyrażonej, lecz konkludentnej czynności osoby, której dane dotyczą. W ocenie skarżącej takie stanowisko jest nazbyt rygorystyczne i

dalece odbiega od literalnego brzmienia przepisu art. 7 pkt. 5 Ustawy. Wyrażając wolę wyrobienia opaski oraz udostępniając spółce w tym celu odciski palców (wyłącznie dla ich zapisania na opasce), klienci spółki w sposób jednoznaczny wyrażają zatem zgodę na ich udostępnienie i mają świadomość komu (spółce), w jakim zakresie (odcisków punktów skrajnych) oraz w jakim celu (wyrobienia opaski służącej kontroli wstępu), to czynią.

W odpowiedzi na skargę Generalny Inspektor Ochrony Danych Osobowych wniósł o jej oddalenie, a wskazując na dotychczasowe ustalenia faktyczne i prawne dodał, że nie podziela stanowiska spółki, że stosowanie systemu biometrycznej kontroli wstępu w prowadzonych klubach nie prowadzi do przetwarzania danych osobowych, z uwagi na to, że dane te nie umożliwiają określenia tożsamości osoby bez poniesienia nadmiernych nakładów, jak również nie podzielił dwóch pozostałych zarzutów podtrzymując argumentację, jak w zaskarżonej decyzji.

Wojewódzki Sąd Administracyjny w Warszawie zważył, co następuje:

Zgodnie z brzmieniem art. 1 § 1 i 2 ustawy z dnia 25 lipca 2002 r. – Prawo o ustroju sądów administracyjnych (Dz. U. Nr 153, poz. 1269 ze zm.), sąd administracyjny sprawuje wymiar sprawiedliwości m.in. poprzez kontrolę działalności administracji publicznej pod względem zgodności z prawem.

Skarga analizowana pod tym kątem podlega oddaleniu, bowiem została ona wydana zgodnie z prawem. Zgodnie z art. 23 ust. 1 ustawy o ochronie danych osobowych (tekst jedn. z 2014 r. poz. 1182 ze zm.), 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 ządanie 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.

Natomiast stosownie do treści art. 6 ust. 1 ustawy, w rozumieniu ustawy za dane osobowe uważa się wszelkie informacje dotyczące zidentyfikowanej lub możliwej do zidentyfikowania osoby fizycznej, a 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 ust. 2). Z kolei według art. 2 ust. 1, ustawa określa zasady postępowania przy przetwarzaniu danych osobowych oraz prawa osób fizycznych, których dane osobowe są lub mogą być przetwarzane w zbiorach danych, zaś w myśl ust. 2, ustawę stosuje się do przetwarzania danych osobowych:

- 1) w kartotekach, skorowidzach, księgach, wykazach i w innych zbiorach ewidencyjnych;
- 2) w systemach informatycznych, także w przypadku przetwarzania danych poza zbiorem danych.

Niezależnie od powyższego, w myśl art. 7 pkt 1, ilekroć w ustawie jest mowa o zbiorze danych, to 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, zaś wedle pkt 2 przetwarzanie danych, to jakiegokolwiek operacje wykonywane na danych osobowych, takie jak zbieranie, utrwalanie, przechowywanie, opracowywanie, zmienianie, udostępnianie i usuwanie, a zwłaszcza te, które wykonuje się w systemach informatycznych. Zaś co się tyczy systemu informatycznego, to w pkt 2a rozumie się przez to zespół współpracujących ze sobą urządzeń, programów, procedur przetwarzania informacji i narzędzi programowych zastosowanych w celu przetwarzania danych, a mówiąc 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 (pkt 5).

W rozpoznawanej sprawie tymczasem, jak ustalono w toku kontroli przeprowadzonej przez Generalnego Inspektora Ochrony Danych Osobowych i co

organ dokładnie opisał w uzasadnieniu zaskarżonej decyzji, w wybranych klubach Spółki zastosowano system biometrycznej kontroli wstępu do klubów w celu uproszczenia i przyspieszenia skutecznej weryfikacji klientów oraz podniesienia bezpieczeństwa. Wzorzec biometryczny odcisku palca klienta w postaci informacji o pojedynczych punktach odcisku palca, zostały przekształcone algorytmem na postać cyfrową i zapisano jest w chipie opaski będącej w posiadaniu klienta, którą wymieniony wchodząc do klubu przykład do czytnika znajdującego się przy bramce wejściowej, podobnie jak i palec. Operacja ta ma za zadanie dokonać weryfikacji, czy klient jest właścicielem opaski i w konsekwencji czy posiada uprawnienia do wejścia. W trakcie tego procesu, czytnik czytuje z opaski zapisany kod punktów biometrycznych i po przyłożeniu przez klienta palca do czytnika z liniami papilarnymi, czytuje punkty biometryczne z palca, po czym przetwarza je w kod i porównuje z kodem zapisanym na opasce. Jednocześnie wysyłany jest do systemu informatycznego „P...”, numer identyfikacyjny (ID) opaski celem zweryfikowania, czy klient posiada uprawnienia do korzystania z oferty klubu. W momencie przyłożenia opaski do czytnika, na monitorze znajdującym się w recepcji, wyświetla się informacja dotycząca klienta, w tym m.in. jego zdjęcie, członka Klubu (m.in. zdjęcie). W podanym wyżej systemie nie są jednak przechowywane dane biometryczne klientów, ale jest zapisany m.in. nr ID opaski. Dodać w tym miejscu należy, że w umowie zawieranej z klientem, na którą składają się formularz aplikacyjny o nazwie „P... Formularz Aplikacyjny” i „Ogólne warunki członkostwa”, brak jest zapisów odnośnie kontroli wejścia do klubów w oparciu o dane biometryczne. Zatem nie jest pozyskiwana od członków klubów zgoda na przetwarzanie danych biometrycznych. Jednakże gdy klient nie wyrazi zgody na korzystania z biometrycznej kontroli dostępu, to również otrzymuje opaskę, przy czym jest wpuszczany przez recepcjonistę. Ponadto jak ustalono w trakcie kontroli, Spółka nie dysponuje pisemnymi oświadczeniami klientów o wyrażeniu zgody na przetwarzanie danych osobowych biometrycznych, a zapoznanie się z „Regulaminem korzystania z klubów sportowych...”, „Regulaminem korzystania z basenów w klubach...”, „Regulaminem korzystania z sauny”, „Zasadami korzystania z solarium w klubach...”, nie jest potwierdzane przez klientów Spółki, zaś w umowie członkowskiej zawieranej z klientami, brak jest odniesień co do obowiązywania takich regulaminów.

Zatem analiza przedstawionego powyżej stanu faktycznego nie pozwala – zdaniem Sądu – na przyjęcie tezy zaprezentowanej przez Spółkę, że przetwarzanie danych biometrycznych w czytniku, odbywa się poza systemem informatycznym oraz że nie dochodzi w ten sposób do przetwarzania danych osobowych w postaci danych biometrycznych. Z tego mianowicie powodu, że na system informatyczny Spółki, o którym mowa w cytowanym już wyżej przepisie art. 7 pkt 2a, składają się – jak słusznie zauważył organ – systemy „P...”, „... Admin”, system biometrycznej kontroli dostępu, m.in. urządzenia w postaci stacji komputerowej, urządzenia zapisujące dane biometryczne, czytniki danych biometrycznych, nośniki danych biometrycznych, tj. opaski wydawane klientom Spółki oraz opracowane i stosowane procedury. Wszak czytnik wraz z opaską będące elementami systemu, służą bezspornie do identyfikacji klientów, które są osobami zidentyfikowanymi poprzez przetwarzanie m.in. imienia, nazwiska, adresu nr PESEL zarówno w postaci papierowej, tj. umów członkowskich, jak i w systemie informatycznym „P...”. Zatem przetworzona do postaci cyfrowej dana biometryczna klienta, służy do jego zidentyfikowania poprzez porównanie wzorca biometrycznego i pozwala na dostęp do usług Spółki, a w konsekwencji spełnia przesłanki z cytowanego już wyżej przepisu art. 6 ust. 1 ustawy.

Należy również stwierdzić, że niezależnie od przetwarzania danych w systemie informatycznym, również w przypadku przetwarzania danych poza zbiorem danych, administrator także musi się legitymować jedną z przesłanek o których mowa w cytowanym już wyżej przepisie art. 23 ust. 1 ustawy.

Tymczasem Spółka zgłosiła do rejestracji zbiór danych osobowych o nazwie „P...” i w zbiorze tym przetwarzane są dane osobowe klientów Spółki, m.in. w systemie „P...”, jednakże nie wskazano informacji o pozyskiwaniu wskazanych już wyżej danych biometrycznych, a przecież dana biometryczna jest powiązana z danymi osobowymi klienta poprzez numer ID i jest pozyskiwana do zbioru danych osobowych klientów Spółki, bowiem dane osobowe klientów przetwarzane przez Spółkę (m.in. w systemie „P...”) wraz z ich danymi biometrycznymi tworzą posiadający strukturę zestaw danych o charakterze osobowym, dostępnych według określonych kryteriów, a więc zbiór danych w rozumieniu cytowanego już wyżej art. 7 pkt 1 ustawy.

Należy w tym miejscu wskazać, że w myśl art. 2 ust. 3 ustawy, w odniesieniu do zbiorów danych osobowych sporządzanych doraźnie, wyłącznie ze względów

technicznych, szkoleniowych lub w związku z dydaktyką w szkołach wyższych, a po ich wykorzystaniu niezwłocznie usuwanych albo poddanych anonimizacji, mają zastosowanie jedynie przepisy rozdziału 5. Jednakże – zdaniem Sądu – nie można powyższego zbioru uznać jako doraźny, bowiem dane osobowe biometryczne przetwarzane są w zbiorze danych osobowych klientów Spółki zgłoszonym do rejestracji i w związku z zapewnieniem kontroli wstępu do klubów. Zatem nie ma on charakteru technicznego mimo relatywnie krótkiego okresu przetwarzania i wprowadzania tych danych do zbioru pojedynczo, podczas wchodzenia klienta do klubu, a wobec powyższego nie można uznać tego zbioru jako sporządzanego doraźnie. Nie zmienia tego okoliczność, że same dane biometryczne wprowadzane są do zbioru danych osobowych klientów Spółki pojedynczo, tj. każdorazowo przy wejściu klienta Spółki do klubu w związku z przyłożeniem do czytnika palca i opaski.

Ponadto stwierdzić należy, że w pkt 3.2. ogólnych warunków członkostwa informuje się klientów, iż w celu zapewnienia bezpieczeństwa, a w szczególności ograniczenia dostępu do pomieszczeń klubów Spółki osobom nieupoważnionym, kontrola wstępu i może odbywać się z wykorzystaniem biometrycznego systemu weryfikacji, przy pomocy opaski członkowskiej zawierającej kod alfanumeryczny utworzony na podstawie danych biometrycznych członka. Jednakże w kolejnym zdaniu podaje się, że „nie gromadzi ani nie przechowuje danych biometrycznych”. Jednakże – co już wyżej wykazano – poprzez wprowadzenie danych biometrycznych do czytników będących elementem systemu informatycznego, gromadzi się powyższe dane. Analiza powyższych dokumentów potwierdza, że nadal brak jest informacji wskazującej, iż wstęp do klubów będzie się odbywał w oparciu o udostępnianie danych biometrycznych, a to powoduje, że klient sądzi, iż Spółka nie przetwarza jego danych osobowych biometrycznych i nie staje się również ich administratorem. Zatem nie sposób uznać, aby Spółka przetwarzając dane osobowe biometryczne klientów, legitymowała się podstawą prawną do ich przetwarzania, o jakiej mowa w art. 23 ust. 1 pkt 3 ustawy. Również dokumenty składające się na umowę członkowską obowiązującą w Spółce przed października 2014 r. nie zawierają żadnych postanowień wskazujących, że wstęp do klubów jest możliwy w oparciu o udostępnienie danych biometrycznych w takim przypadku konieczne jest przetwarzanie tych danych przez Spółkę. Zatem w odniesieniu do tych klientów, Spółka również nie posiada podstawy prawnej przetwarzania ich danych osobowych



biometrycznych, wskazanej w art. 23 ust. 1 pkt 3 ustawy o ochronie danych osobowych.

Niezależnie od powyższego wskazać należy, że Spółka nie pozyskiwała od klientów pisemnej zgody na przetwarzanie ich danych biometrycznych, w tym pisemnego oświadczenia o wyrażeniu takiej zgody i nie sposób się zgodzić, że z faktu zarejestrowania danych biometrycznych w opasce przekazywanej na własność klientowi, klient ów wyraża zgodę na przetwarzanie przez Spółkę jego danych osobowych. Wszak stosownie do cytowanego już wyżej art. 7 pkt 5 ustawy, zgoda nie może być wyrażona przez pewne czynności dorozumiane, zaś uzyskanie zgody w ten sposób nie daje podstawy prawnej do przetwarzania danych. Powyższe stanowisko nie jest odosobnione, bowiem znajduje swoje potwierdzenie w doktrynie, gdzie np. w komentarz do art. 174 (pkt 1) ustawy z dnia 16 lipca 2004 r. Prawo telekomunikacyjne (Dz. U. z 2014 r., poz. 243 z późn. zm.), w myśl którego jeżeli przepisy tej ustawy wymagają wyrażenia zgody przez abonenta lub użytkownika końcowego, zgoda ta nie może być domniemana lub dorozumiana z oświadczenia woli o innej treści, stwierdza się, że „(...) Pierwszym wymogiem dla zgody, wynikającym ze sformułowania zakazu domniemywania zgody bądź jej dorozumienia, jest konieczność jasnego, wyraźnego, nienasuującego wątpliwości pozytywnego oświadczenia woli przy tak samo wyraźnym jednoznacznym określeniu przedmiotu, którego zgoda dotyczy. Dla wyrażenia zgody w rozumieniu art. 174 nie znajduje zastosowania przepis art. 60 k.c. wskazujący, że oświadczenie woli może być wyrażone przez każde zachowanie ujawniające wolę w sposób dostateczny” (Krzysztof Kawalek, Maciej Rogalski, Prawo telekomunikacyjne Komentarz Warszawa 2010, Wolters Kluwer Polska Sp. z o.o., str. 894). Takie same stanowisko zawarto w Komentarzu do ustawy o ochronie danych osobowych Janusza Barta, Pawła Fajgielskiego i Ryszard Markiewicz (wydanie 4, Wolters Kluwer Polska Sp. z o.o., 384 i 386 – 387).

Tytułem uzupełnienia odnosząc się do argumentacji skarżącej o braku możliwości ustalenia w rozpoznawanej sprawie tożsamości danej osoby na podstawie tylko kodu alfanumerycznego stwierdzić należy, że w myśl art. 6 ustawy, pojęcie danych osobowych obejmuje wszelkie informacje dotyczące osoby fizycznej, o ile możliwe jest zidentyfikowanie tej osoby. Z kolei za osobę możliwą do zidentyfikowania uważana jest osoba, której tożsamość można określić bezpośrednio lub pośrednio, w szczególności przez powołanie się m.in. na jej cechy fizyczne, do

których bez wątpienia zalicza się dane biometryczne np. w postaci linii papilarnych palca (ust. 2). Skoro zaś tak, to należy rozstrzygnąć czy, a jeżeli tak, to kiedy taka informacja umożliwia określenie tożsamości danej osoby. Niewykluczone jest i co utrzymuje Spółka, sama dana biometryczna – oceniając powyższą kwestię tylko hipotetycznie – faktycznie może nie wskazywać na konkretną osobę. Jednakże nie oznacza to, że w ten sposób w ogóle zamyka się drogę do ustalenia tożsamości osoby, z którą ta informacja jest związana. Wszak można to uczynić poprzez dotarcie do odpowiedniej bazy, niekoniecznie będącej w posiadaniu skarżącej, w której są zbierane powyższe dane biometryczne i następnie powiązać te dane z odpowiednio osobą. Reasumując, „w zasadzie każda wiadomość o jakimś zdarzeniu, o jakiejś sytuacji z udziałem człowieka może zostać uznana za wiadomość zindywidualizowaną, gdyż – co najmniej teoretycznie – zawsze istnieje możliwość określenia tożsamości tego człowieka. W tym stanie rzeczy pojawia się dalsze, zasadnicze pytanie, czy danymi osobowymi są tylko takie dane, które od razu, ze względu na swoją treść, pozwalają określić tożsamość osoby (jak się określa: osoby zainteresowanej), czy również takie dane, przy których co prawda takie bezpośrednie odniesienie do osoby nie istnieje, niemniej podanie jej tożsamości jest możliwe. Przychylenie się do drugiej możliwości wywołuje dalsze pytania. Odnoszą się one do stopnia nakładów potrzebnych do ustalenia tożsamości. Innymi słowy, chodzi o to, czy do danych osobowych powinno się zaliczać tylko takie dane (informacje), przy których określenie tożsamości jest proste (względnie nie przysparza znacznych trudności) i dostępne dla przeciętnej osoby. Alternatywą byłoby przyjęcie, że przesłanką danych osobowych jest w ogóle możliwość określenia tożsamości, choćby wymagało to szczególnych nakładów, przygotowania, wiedzy, kompetencji”. (Komentarz do ustawy o ochronie danych osobowych, Janusz Barta, Paweł Fajgielski, Ryszard Markiewicz, stan na dzień 1 lipca 2015 r. – LEX). Powyższe ograniczenie jest zawarte w art. 6 ust. 3 ustawy w myśl którego, informacji nie uważa się za umożliwiającą określenia tożsamości osoby, jeżeli wymagałoby to nadmiernych kosztów, czasu lub działań. Zawarte w tym przepisie określenie „nadmierności” nie jest zdefiniowane, a przez to jest nieostre. Jednakże – w ocenie Sądu – nie musi to oznaczać np. braku umiarkowania, przesadności, zawyżonych kosztów, nieumiarkowania, zwiększonego nakładu pracy ...etc., lecz adekwatność w realizacji postawionego zadania i przy takim podejściu ową „nadmierność” należy zawsze oceniać w sposób indywidualny w zależności do zamierzonego celu i wagi tej

informacji. Skoro zaś tak, to można – wbrew stanowisku Spółki – na podstawie kodu alfanumerycznego ustalić tożsamość jej klienta.

W tym stanie rzeczy, na podstawie art. 151 w zw. z art. 132 ustawy z dnia 30 sierpnia 2002 r. – Prawo o postępowaniu przed sądami administracyjnymi (tekst jedn. Dz. U. z 2012 r., poz. 270), należało orzec jak w sentencji wyroku.



Właściwe podpisy  
Za zgodność z oryginałem