BVGer BVGE 2009/44 vom 4. August 2009

Bundesverwaltungsgericht, 2009-08-04, DE

Quelle: https://mcp.opencaselaw.ch/entscheid/bvger_BVGE 2009_44

FR: TAF BVGE 2009/44 du 4 août 2009

IT: TAF BVGE 2009/44 del 4 agosto 2009

Regeste

Datenschutz

Erwägungen

E. 1

Der EDÖB klärt von sich aus oder auf Meldung Dritter hin den Sachverhalt näher ab, wenn Bearbeitungsmethoden geeignet sind, die Persönlichkeit einer grösseren Anzahl von Personen zu verletzen (Systemfehler, Art. 29 Abs. 1 Bst. a des Bundesgesetzes vom 19. Juni 1992 über den Datenschutz [DSG, SR 235.1]). Aufgrund seiner Abklärungen kann er empfehlen, das Bearbeiten zu ändern oder zu unterlassen (Art. 29 Abs. 3 DSG). Wird eine solche Empfehlung nicht befolgt oder abgelehnt, kann er die Angelegenheit dem BVGer auf dem Klageweg zum Entscheid vorlegen (Art. 29 Abs. 4 DSG i. V. m. Art. 35 Bst. b des Verwaltungsgerichtsgesetzes vom 17. Juni 2005 [VGG, SR 173.32]).

E. 1.1

Die vorliegende Klage richtet sich gegen die Nichtbefolgung beziehungsweise die Ablehnung einer Empfehlung des EDÖB durch die Beklagte. Insofern handelt es sich um eine Klage nach Art. 29 Abs. 4 DSG. Zunächst ist daher abzuklären, ob das DSG im vorliegenden Verfahren überhaupt Anwendung findet und der EDÖB zur vorliegenden Klageerhebung berechtigt war.

E. 1.2

Das DSG gilt für das Bearbeiten von Daten natürlicher und juristischer Personen durch private Personen und Bundesorgane (Art. 2 Abs. 1 DSG).

E. 1.2.1

Unter Personendaten (Daten) fallen nach Art. 3 Bst. a DSG alle Angaben, die sich auf eine bestimmte oder bestimmbare Person beziehen. Darunter ist jede Art von Information zu verstehen, die auf die Vermittlung oder die Aufbewahrung von Kenntnissen ausgerichtet ist, ungeachtet dessen, ob es sich dabei um eine Tatsachenfeststellung oder um ein Werturteil handelt. Unerheblich ist auch, ob eine Aussage als Zeichen, Wort, Bild, Ton oder Kombinationen aus diesen auftritt und auf welcher Art von Datenträger die Informationen gespeichert sind. Eine Person ist dann bestimmt, wenn sich aus der Information selbst ergibt, dass es sich um diese ganz bestimmte Person handelt (URS BELSER, in: Urs Maurer-Lambrou/Nedim Peter Vogt [Hrsg.], Datenschutzgesetz, Basler Kommentar, 2. Aufl., Basel 2006, Rz. 5 f. zu Art. 3). Der Bezug ist dort unproblematisch, wo sich der Personenbezug aus der Natur der Information selbst ergibt, wie bei biometrischen Informationen wie Fingerabdrücken (vgl. DAVID ROSENTHAL/YVONNE JÖHRI, Handkommentar zum Datenschutzgesetz, Zürich 2008, Art. 3 Bst. a N 13).

E. 1.2.2

Die Beklagte erhebt von jedem Dauerkarteninhaber die Personalien, das heisst Name, Vorname, Adresse, Sprache und Geburtsdatum. Dabei handelt es sich ohne Weiteres um Personendaten, die einerseits für sich alleine (Name, Vorname), andererseits in Zusammenhang mit den weiter erhobenen Daten - ohne grossen Aufwand - auf eine bestimmte Person schliessen lassen (Adresse, Sprache, Geburtsdatum). Daneben werden den Abonnenten die Fingerabdrücke genommen bzw. deren Minutien extrahiert, mittels Algorithmus in ein Template umgewandelt und dergestalt in einer zentralen Datenbank abgelegt. Der Fingerabdruck an sich, wie auch die extrahierten Minutien sind einzigartig und nur einer bestimmten Person zuzuordnen. Der Bezug zu einer Person geht daher aus diesen selbst hervor. Auf welche Art von Datenträger (Template) sie gespeichert werden, ist unerheblich. Im Übrigen ist auch noch eine Zuordnungsliste zentral abgelegt, sodass mit dieser Rückschluss auf einen bestimmten Abonnenten genommen werden kann. Insofern sind sämtliche hier in Frage stehenden Daten als Personendaten gemäss DSG zu qualifizieren.

E. 1.2.3

Bearbeiten im Sinne von Art. 2 Abs. 1 DSG bedeutet jeder Umgang mit Personendaten, unabhängig von den angewandten Mitteln und Verfahren, insbesondere das Beschaffen, Aufbewahren, Verwenden, Umarbeiten, Bekanntgeben, Archivieren oder Vernichten von Daten (Art. 3 Bst. e DSG). Für das BVGer besteht kein Zweifel, dass im vorliegenden Fall eine Bearbeitung nach DSG erfolgt. Dies wird im Übrigen auch nicht bestritten.

E. 1.2.4

Wie bereits erwähnt, klärt der Beauftragte gemäss Art. 29 Abs. 1 Bst. a DSG von sich aus oder auf Meldung Dritter hin den Sachverhalt näher ab, wenn Bearbeitungsmethoden geeignet sind, die Persönlichkeit einer grösseren Anzahl von Personen zu verletzen (Systemfehler). « Systemfehler » bedeutet in diesem Zusammenhang die Eignung, eine grössere Anzahl von Personen in ihrer Persönlichkeit zu verletzen (vgl. ROSENTHAL/JÖHRI, a. a. O., Art. 29 N. 11; RENÉ HUBER, in: Urs Maurer-Lambrou/Nedim Peter Vogt [Hrsg.], Datenschutzgesetz, Basler Kommentar, 2. Aufl., Basel 2006, Rz. 6 ff. zu Art. 29; Urteil der Eidgenössischen Datenschutzkommission vom 15. April 2005, veröffentlicht in Verwaltungspraxis des Bundes VPB 69.106 E. 3.2). Kann die fragliche Datenbearbeitung potentiell zur Schädigung einer grösseren Anzahl Betroffener führen, ist die Schwelle der « grösseren Anzahl » bereits beim Vorliegen einiger weniger Vorfälle erreicht (HUBER, a. a. O., Rz. 10 f. zu Art. 29). In der Klageantwort führt die Beklagte aus, dass jährlich 1'200 Dauerkarten verkauft würden. Insofern kann ohne Weiteres von einem « Systemfehler » im Sinne der Gesetzgebung ausgegangen werden.

E. 1.3

Das DSG kommt aus diesen Gründen zur Anwendung und der Kläger war zur Erteilung der Empfehlung ermächtigt. Auf die im Weiteren form- und fristgerecht eingereichte Klage ist daher einzutreten.

E. 1.4

Das Verfahren richtet sich gemäss Art. 44 Abs. 1 VGG grundsätzlich nach den Art. 373 sowie den Art. 7985 des Bundesgesetzes vom 4. Dezember 1947 über den

Bundeszivilprozess (BZP, SR 273). Obwohl im Bundeszivilprozess der Richter sein Urteil grundsätzlich nur auf Tatsachen gründen darf, die im Verfahren geltend gemacht worden sind (Art. 3 Abs. 2 BZP), gilt vor BVGer infolge der spezialgesetzlichen Bestimmung von Art. 44 Abs. 2 VGG der Grundsatz der Sachverhaltsabklärung von Amtes wegen. Art. 3 Abs. 2 BZP bestimmt, dass der Richter nicht über die Rechtsbegehren der Parteien hinausgehen darf. In einem Klageverfahren wie dem vorliegenden hat die Dispositionsmaxime somit grössere Bedeutung als im Beschwerdeverfahren vor BVGer. Im Verfahren vor dem BVGer wird der EDÖB in der Regel verlangen, dass die von ihm empfohlenen und nun klageweise geltend gemachten Massnahmen gegenüber den betreffenden Datenbearbeitern verfügt, das heisst den Datenbearbeitern durch das Gericht in verbindlicher und erzwingbarer Form angeordnet werden. Damit wird die Empfehlung zwar nicht verbindlich, doch wird ihr - soweit begehrt und gutgeheissen - ein entsprechendes Urteil zur Seite gestellt. Das BVGer kann aber auch weniger weit gehende Massnahmen anordnen (vgl. ROSENTHAL/JÖHRI, a. a. O., Art. 29 Abs. 4 N 47).

E. 2.1

Der Kläger rügt vorab, das Zugangssystem der Beklagten verstosse gegen das Gebot der Zweckbindung der Datenbearbeitung nach Art. 4 Abs. 3 DSG (Klageschrift, Ziff. 2.1). Eine Zweckänderung sei von den Betroffenen durch die zentrale Speicherung der biometrischen Daten aber nicht kontrollierbar. Damit bestehe die Gefahr einer Verletzung der informationellen Selbstbestimmung nach Art. 13 Abs. 2 der Bundesverfassung der Schweizerischen Eidgenossenschaft vom 18. April 1999 (BV, SR 101). Die biometrischen Daten dürften den Kontrollbereich der betroffenen Person deshalb nicht verlassen. Er empfehle daher ein milderes Mittel, die sogenannte « Smartcard match on card ». Die biometrischen Daten würden auf dem Sicherheitsmedium gespeichert und die Verifizierung finde ebenfalls darauf statt.

E. 2.2

Es ist nicht ersichtlich und wird vom Kläger auch nicht weiter begründet, inwiefern der Grundsatz der Zweckbindung nach Art. 4 Abs. 3 DSG hier verletzt worden sein soll. Der Kläger gesteht der Beklagten denn auch zu, dass sie bisher keine Zweckänderung vorgenommen habe (Klageschrift, Ziff. 43). Er rügt unter dem Grundsatz der Zweckbindung der Datenbearbeitung nichts anderes als den Grundsatz der Verhältnismässigkeit der Datenbearbeitung gemäss Ziffer 2.2 seiner Klage. Die Klage ist denn auch (hauptsächlich) unter diesem Gesichtspunkt zu behandeln.

E. 3

Gemäss Art. 13 Abs. 2 BV hat jede Person Anspruch auf Schutz vor Missbrauch ihrer persönlichen Daten. Diesem Anspruch hat der Bundesgesetzgeber im DSG Rechnung getragen und das Bearbeiten von Daten durch Private und Bundesbehörden eingehend geregelt (ULRICH HÄFELIN/WALTER HALLER/HELEN KELLER, Schweizerisches Bundesstaatsrecht, 7. Aufl., Zürich/Basel/Genf 2008, Rz. 390). Wer Personendaten bearbeitet, darf dabei die Persönlichkeit der betroffenen Personen nicht widerrechtlich verletzen. Er darf insbesondere nicht Personendaten entgegen den Grundsätzen des Artikels 4 bearbeiten (Art. 12 Abs. 2 Bst. a DSG).

E. 3.1

Nach Art. 4 Abs. 2 DSG muss die Bearbeitung der Daten verhältnismässig sein. Sowohl der Zweck, der mit der Datenbearbeitung verfolgt wird, als auch die Art und Weise der

Bearbeitung müssen verhältnismässig sein. Dies verlangt zunächst, dass Personendaten nur soweit bearbeitet werden dürfen, als dies für einen bestimmten Zweck objektiv geeignet und tatsächlich erforderlich ist. Der Verhältnismässigkeitsgrundsatz verlangt weiter, dass die Datenbearbeitung für die betroffene Person sowohl hinsichtlich ihres Zwecks als auch hinsichtlich ihrer Mittel zumutbar ist (das heisst verhältnismässig im engeren Sinne). Die Prüfung der Verhältnismässigkeit verlangt eine Gesamtwürdigung aller Umstände (BGE 122 II 199), das heisst auch der Interessen des Datenbearbeiters (ROSENTHAL/JÖHRI, a. a. O., Art. 4 N 19 ff.).

E. 3.2

Gemäss Klageschrift Ziff. 63 akzeptiert der Kläger die Einführung des biometrischen Erkennungssystems in Hinblick auf den Bearbeitungszweck unter Vorbehalt. Im Verhältnis zum Eingriff in die Grundrechte der betroffenen Person seien die von der Beklagten eingeführten Massnahmen und durchgeführten Datenbearbeitungen zwar geeignet, um das angestrebte Ziel - den Missbrauch der Dauerkarten - zu erreichen, sie stünden jedoch nicht in einem vernünftigen Verhältnis zum Eingriff in die Grundrechte der betroffenen Person. Insofern bemängelt der Kläger die Erforderlichkeit des Eingriffs.

E. 3.3

Eine Massnahme hat zu unterbleiben, wenn eine gleich geeignete, aber mildere Massnahme für den angestrebten Erfolg ausreichen würde. Das Gebot der Erforderlichkeit einer Massnahme wird auch als Prinzip der « Notwendigkeit », des « geringst möglichen Eingriffs », der « Zweckangemessenheit » oder als « Übermassverbot » bezeichnet (ULRICH HÄFELIN/GEORG MÜLLER/FELIX UHLMANN, Allgemeines Verwaltungsrecht, 5. Aufl., Zürich/Basel/Genf 2006, Rz. 591 f.). Der Eingriff darf in sachlicher, räumlicher, zeitlicher und personeller Beziehung nicht über das Notwendige hinausgehen (ULRICH HÄFELIN/WALTER HALLER/HELEN KELLER, a. a. O., Rz. 322). Bei der Verifizierung der Identität der Betroffenen sollen die biometrischen Daten statt in einer zentralen Datenbank vorzugsweise auf einem gesicherten individuellen Speichermedium gespeichert werden, dessen Einsatz durch den Betroffenen kontrolliert werden kann (URS MAURER-LAMBROU/ANDREA STEINER, in: Urs Maurer-Lambrou/Nedim Peter Vogt [Hrsg.], Datenschutzgesetz, Basler Kommentar, 2. Aufl., Basel 2006, Rz. 22 zu Art. 4).

E. 3.4

Mit dem aktuellen System werden die biometrischen Daten zusammen mit einer Zuordnungsliste auf dem Host der Beklagten gespeichert. Die Transponderkarte dient lediglich dazu, das entsprechende Template für den Überprüfungsprozess zu aktivieren, damit der Besucher über seinen Fingerabdruck als Abonnent identifiziert werden kann. Auf ihr sind keine Daten gespeichert. Der Verifizierungsprozess erfolgt auf dem Host. Jede korrekt durchgeführte Transaktion wird erfasst.

E. 3.5

Bei dem vom Kläger empfohlenen System « Smartcard match on card » erfolgt der Vergleich zwischen der biometrischen Charakteristik (Fingerabdruck) und den lokal gespeicherten biometrischen Daten (Referenz-Template) dezentral auf der Karte, so dass der Host lediglich ein Freigabesignal von der Smartcard erhält und keine biometrischen Daten zwischen Smartcard und dem elektronischen Zugangskontrollsystem ausgetauscht werden. Damit haben die betroffenen Personen sowohl die Kontrolle über ihre

biometrischen Referenzdaten als auch über die Transaktionsdaten im Rahmen des Vergleichs. In einem solchen Fall liegen lediglich Transaktionsdaten, welche zwischen der Smartcard und dem Leser ausgetauscht werden, ausserhalb des Kontrollbereichs der betroffenen Person.

E. 3.6

Bei der Gegenüberstellung der beiden verschiedenen Zugangssysteme wird ersichtlich, dass das vom Kläger geforderte System weit weniger in das informationelle Selbstbestimmungsrecht des Betroffenen eingreift als das bis anhin verwendete System und trotzdem das verfolgte Ziel erreichen kann. Der Betroffene gibt seine Daten dabei nicht mehr aus der Hand und behält damit stets die Kontrolle. Dass der Abonnent beim derzeitigen Zugangssystem jederzeit Einsicht in seine Daten nehmen könne, wie dies die Beklagte vorbringt, vermag die Kontrollmöglichkeiten des eingeklagten Zugangssystems bei Weitem nicht zu erreichen. Zentral gespeicherte Daten ausserhalb des Herrschaftsbereichs des Abonnenten bleiben für diesen mehrheitlich unerreichbar und damit verletzlich.

E. 3.7

Im Zusammenhang mit Art. 36 Abs. 4 Bst. c DSG, wonach der Bundesrat Bestimmungen erlassen kann, wie die Mittel zur Identifikation von Personen verwendet werden dürfen, verweist der Handkommentar DSG zudem auf den Schlussbericht des Klägers vom 11. April 2006 und begrüsst damit das vorliegende Begehren nach dezentraler Speicherung der biometrischen Daten (vgl. ROSENTHAL/JÖHRI, a. a. O., Art. 36 Abs. 4 Bst. c N 35 f.). Der Zürcher Datenschutzbeauftragte hat anlässlich seines 11. Tätigkeitsberichts 2005 ebenfalls empfohlen, dass Systeme vorzuziehen seien, bei denen die biometrischen Daten nicht bei der Schwimmbad-Betreiberin abgelegt würden (...). In diesem Sinne hat sich auch die Art. 29 - Datenschutzgruppe der EU als deren unabhängiges Beratungsgremium in Datenschutzfragen geäussert. Danach sind biometrische Daten bei der Verwendung als Zutrittskontrolle nicht auf einem Medium zu speichern, das sich nicht im Besitz der betroffenen Person befindet (vgl. Arbeitspapier über Biometrie der Art. 29 - Datenschutzgruppe vom 1. August 2003, Ziff. 3.2 S. 7). Europäische Länder sind diesen Empfehlungen gefolgt (u. a. Frankreich ... und Italien ...) und sprechen sich ebenfalls für die dezentrale Speicherung gemäss Klagebegehren aus. Der Kläger seinerseits hat sich im (gleichartigen) Fall des Check-In und Boarding beim Flughafen Zürich, wo auch Fingerabdrücke der Fluggäste genommen und in Form von Templates abgelegt wurden, geäussert. Auch hier hat er die dezentrale Speicherung empfohlen (...).

E. 3.8

Die Beklagte hat im Übrigen mit Schreiben vom 10. August 2006 (...) der Empfehlung Nr. 2 - mithin dem Klagebegehren - zugestimmt und ausgeführt, dass die Dauerkarten durch beschreibbare Medien ersetzt würden. Die Software werde so angepasst, dass die Daten auf der Karte gespeichert werden könnten. Dem Schreiben vom 29. Februar 2008 ist zudem zu entnehmen, dass die Beklagte nur die hohen Anschaffungskosten und den zusätzlichen logistischen Aufwand für das Festhalten an der bisherigen zentralen Speicherung der Daten vorbringt. Sie stellt sich hingegen nicht auf den Standpunkt, das vom Kläger begehrte Zugangssystem stelle kein milderes Mittel im Sinne der Verhältnismässigkeit dar. Dies scheint insofern auch nachvollziehbar, als kein Grund ersichtlich ist, weshalb eine zentrale Speicherung der Daten bei der Beklagten notwendig ist. Ein solcher wird von ihr auch nicht

geltend gemacht.

E. 3.9

Aus diesen Gründen steht fest, dass die zentrale Speicherung der biometrischen Daten, wie sie die Beklagte bisher handhabt, dem Gebot der Erforderlichkeit widerspricht und damit den Grundsatz der Verhältnismässigkeit der Datenbearbeitung gemäss Art. 4 Abs. 2 DSG verletzt. Es liegt daher eine Persönlichkeitsverletzung nach Art. 12 Abs. 2 Bst. a DSG vor.

E. 4

Nicht jede Verletzung der Persönlichkeit ist auch widerrechtlich; die Widerrechtlichkeit ist somit lediglich Grundsatz, von dem es Ausnahmen gibt. Eine Verletzung der Persönlichkeit ist dann nicht widerrechtlich, wenn sie unter anderem durch Einwilligung des Verletzten gerechtfertigt ist (Art. 13 Abs. 1 DSG).

E. 4.1

Die Einwilligung kann grundsätzlich jede Persönlichkeitsverletzung rechtfertigen, auch Verstösse gegen die allgemeinen Datenschutzbearbeitungsgrundsätze (vgl. dazu CORRADO RAMPINI, in: Urs Maurer-Lambrou/Nedim Peter Vogt [Hrsg.] Datenschutzgesetz, Basler Kommentar, 2. Aufl., Basel 2006, Rz. 3 f. zu Art. 13). Der Gesetzgeber hat sich bei der Definition des Begriffs der Einwilligung an demjenigen der Einwilligung des aufgeklärten Patienten (vgl. BGE 119 II 456, BGE 117 Ib 197, BGE 114 Ia 350) orientiert, und zwar in dem Sinne, dass die betroffene Person über alle Informationen im konkreten Fall verfügen muss, die erforderlich sind, damit sie eine freie Entscheidung treffen kann (Botschaft des Bundesrates zur Änderung des Bundesgesetzes über den Datenschutz [DSG] und zum Bundesbeschluss betreffend den Beitritt der Schweiz zum Zusatzprotokoll vom 8. November 2001 zum Übereinkommen zum Schutz des Menschen bei der automatischen Verarbeitung personenbezogener Daten bezüglich Aufsichtsbehörden und grenzüberschreitende Datenübermittlung vom 19. Februar 2003, BBl 2003 2127). Eine rechtlich gültige Einwilligung setzt nach Art. 4 Abs. 5 DSG voraus, dass eine angemessene Information bezüglich der Datenbearbeitung vorliegt, in die eingewilligt werden soll, eine Willenserklärung vorliegt, aus welcher eine Zustimmung zu dieser Datenbearbeitung entnommen werden kann und diese Willenserklärung freiwillig erfolgt (ROSENTHAL/JÖHRI, a. a. O., Art. 4 Abs. 5 N 67 f.).

E. 4.2

Das Erfordernis einer angemessenen Information will erreichen, dass die betroffene Person ihre Einwilligung in Kenntnis der Sachlage gibt, das heisst erst entscheiden muss, wenn sie sich ein Bild (auch) über die möglichen negativen Folgen ihrer Einwilligung machen konnte. Erforderlich, aber auch genügend ist letztlich, dass sich die betroffene Person im Klaren darüber sein kann, worin sie einwilligen soll, das heisst was die Tragweite ihrer Entscheidung ist. Je nach Situation wird eine Aufklärung erforderlich sein, die nicht nur auf die Umstände der Datenbearbeitung, sondern auch auf ihre wichtigsten möglichen Risiken bzw. Folgen für die betroffene Person hinweist, insbesondere wenn diese schwerwiegend sind. Ob und wie weit diesbezüglich informiert werden muss, hängt letztlich aber von den konkreten Umständen ab (ROSENTHAL/JÖHRI, a. a. O., Art. 4 Abs. 5 N 72 f.). Eine Einwilligung muss freiwillig erfolgen, das heisst Ausdruck des freien Willens der betroffenen Person sein. Ungültig ist die durch Täuschung, Drohung oder Zwang zustande gekommene Einwilligung. Der betroffenen Person muss « eine - mit nicht unzumutbaren Nachteilen behaftete - Handlungsalternative » zur Verfügung stehen (RAMPINI, a. a. O.,

Rz. 6 f. zu Art. 13; vgl. auch CHRISTIAN DRECHSLER, Die Revision des Datenschutzrechts, in: Aktuelle Juristische Praxis 2007 S. 1473). Etwas abweichend dazu äussert sich DAVID ROSENTHAL im Handkommentar DSG und meint, dass dies zu weit gehe: Wo davon auszugehen sei, dass eine Einwilligung subjektiv im Interesse der betroffenen Person liege, könne normalerweise ebenfalls von einer freiwilligen Willenserklärung ausgegangen werden, selbst wenn die betroffene Person keine Handlungsalternative habe. Seine Kritik berührt den vorliegenden Fall jedoch nicht, weil die Einwilligung hier dem Betroffenen keinen Vorteil bringt, insofern nicht in dessen subjektivem Interesse liegt.

E. 4.3

Die Beklagte bringt zum Rechtfertigungsgrund der Einwilligung vor, die Betroffenen würden beim Kauf einer Dauerkarte auf das System und die Datenbearbeitung aufmerksam gemacht. Die alternative Ausstellung von Dauerkarten ohne Finger-Print werde indes nicht öffentlich bekannt gemacht. Erst wenn sich ein Gast weigere, werde ihm die Alternativlösung angeboten. Die Betroffenen könnten zudem jederzeit Einblick in ihre Daten nehmen.

E. 4.4

In seinem Schlussbericht führt der Kläger in Bezug auf die Einwilligung der Betroffenen aus, dass keine Alternativlösungen bestünden. Die Kunden müssten auf teurere Zehner-Abonnemente ausweichen. Die Badegäste würden beim Umtausch oder Erwerb einer Dauerkarte vom Kassenpersonal über die Erhebung der biometrischen Daten und über die weitere Datenbearbeitung mündlich aufgeklärt. Bei der Sachverhaltsabklärung vor Ort seien an der Kassentheke aber keine Flyer erhältlich gewesen. Der Flyer habe ihm erst nach einer kleineren Suchaktion überreicht werden können. Er trage die Überschrift « Ist der Datenschutz bei der biometrischen Fingerabdruck Erkennung und Identifikation gewährleistet? ». Der Flyer erkläre, dass keine Rohdaten gespeichert, sondern extrahierte Merkmale eines Fingerabdruckes in Form eines « codierten » Templates in der Datenbank gespeichert würden. Der Flyer führe weiter aus, wie der Abgleich der Templates vor sich gehe und dass es nicht möglich sei, aus dem « Code » das Rohdatum wieder herzustellen. Ferner werde darauf hingewiesen, dass heute gängige Personendatenbanken aus Sicht des Datenschutzes eine weit grössere Gefahr darstellten als die Information des Fingerabdruckes. Der Flyer äussere sich nur grob über die Bearbeitungsmodalitäten der erhobenen Daten. Zudem erkläre der Flyer primär, warum der Einsatz von Biometrie aus Sicht des Systemlieferanten unproblematisch sei. In seinem Verbesserungsvorschlag Nr. 1 regt der Kläger daher an, dass der Informationsgehalt des Flyers hinsichtlich der Bearbeitungsmodalitäten der biometrischen Daten stark verbessert werden müsse. Aufgeführt werden müssten die Hauptpunkte der Datenbearbeitung, wie zum Beispiel wo und für wie lange die Daten gespeichert würden, insbesondere was mit den Templates und den Transaktionsdaten geschehe, wer Zugriff auf die Daten habe und an wen sie - wenn überhaupt - weitergegeben würden. Er sei jedem Kunden vor dem Enrolement (Registrierung) automatisch vom Kassenpersonal und ohne Nachfrage des Kunden auszuhändigen. Dem Badegast sei genügend Zeit zur Verfügung zu stellen, ihn vorher durchzulesen. Weitere Flyer seien griffbereit an der Kassentheke aufzulegen. Mit Schreiben vom 18. Oktober 2006 (...) stimmt die Beklagte auch diesem Verbesserungsvorschlag zu und führt aus, dass dieser umgesetzt werde. Der Flyer werde vollständig überarbeitet, wobei die vom Kläger genannten Punkte berücksichtigt würden. Weiter werde ein Ablauf- und

Organisationsdiagramm für das Kassenpersonal erstellt, aus welchem hervorgehe, wie bei der Herausgabe eines Abonnements (mit biometrischen Daten) vorzugehen sei. Aus den vorliegenden Unterlagen ist nicht ersichtlich, dass der Verbesserungsvorschlag von der Beklagten umgesetzt worden ist.

E. 4.5

Dem Kläger ist zuzustimmen, dass einem Badegast (faktisch) keine Alternativlösung geboten wird, wenn er die Möglichkeit für den Erwerb eines Jahres- oder Halbjahresabonnements ohne Fingerprint-Lösung erst dann erhält, wenn er sich geweigert hat, ein solches mit dem aktuellen Zugangssystem zu akzeptieren. In den meisten Fällen wird der Gast sich (vermeintlich) mangels Alternative dazu bewegen lassen, seine biometrischen Daten zentral zu hinterlegen. Insofern kann hier nicht von Freiwilligkeit die Rede sein.

E. 4.6

Im Weiteren wird der Gast auch nicht angemessen informiert, so dass er sich über die Tragweite seiner Entscheidung (vollends) im Klaren sein könnte. Der Flyer wird diesem offensichtlich gar nicht erst ausgehändigt. Wenn er schon bei der vorher vereinbarten Sachverhaltsfeststellung des Klägers erst nach einer kleineren Suchaktion überreicht werden kann, ist nicht davon auszugehen, dass er an einem « gewöhnlichen Tag » stets griffbereit ist, geschweige denn verteilt wird. Weiter scheint das Kassenpersonal weder spezifische Vorgaben noch eine besondere Schulung erhalten zu haben, wie beim Verkauf einer Dauerkarte vorzugehen ist. Dem Erfordernis der angemessenen Information kommt die Beklagte deshalb nicht genügend nach. Über den Inhalt des Flyers und ob dieser ausreichend ist, braucht das BVGer daher nicht weiter zu befinden. Zu bemerken sei hierzu lediglich, dass biometrische Daten (wohl unbestrittenermassen) sensibel sind und die Information hierüber umfassend sein müsste. Aufgrund der unbestrittenen Beschreibung des Klägers über den Informationsgehalt des Flyers und des Verbesserungsvorschlages lässt sich aber erahnen, dass dieser einer angemessenen Aufklärung nicht genügend Rechnung trägt.

E. 5

Eine Verletzung der Persönlichkeit ist ebenfalls nicht widerrechtlich, wenn sie durch ein überwiegendes privates Interesse gerechtfertigt ist (Art. 13 Abs. 1 DSG). Seitens des Datenbearbeiters sind nur die privaten Interessen an der zu rechtfertigenden Datenbearbeitung zu berücksichtigen. Zu ermitteln sind dabei sowohl das Interesse am Zweck als auch an den Mitteln der Datenbearbeitung, mit welchen der Zweck erreicht werden soll. Die Mittel der Datenbearbeitung umfassen insbesondere die Art und Weise der Datenbearbeitung und die Art und Auswahl der Personendaten (ROSENTHAL/JÖHRI, a. a. O., Art. 13 Abs. 1 N 8).

E. 5.1

Die Beklagte bringt in diesem Zusammenhang vor, durch die Anpassungen im Sinne des Klagebegehrens entstünden hohe Anschaffungskosten und zusätzlicher logistischer Aufwand.

E. 5.2

Der Kläger führt hingegen aus, es liege in der Verantwortung des Inhabers der Datensammlung dafür zu sorgen, dass eine Anlage zum vornherein datenschutzkonform sei.

Insofern seien die Änderungskosten und der zusätzliche logistische Aufwand keine stichhaltigen Argumente.

E. 5.3

Die Interessen der Beklagten sind nicht zu berücksichtigen, weil sich diese nicht auf die Datenverarbeitung selbst beziehen, sondern nur auf die Unannehmlichkeiten abstellen, die eine allfälligen Änderung im Sinne des Klägers mit sich brächten. Diese Interessen haben beim Rechtfertigungsgrund der überwiegenden privaten Interessen im Sinne von Art. 13 Abs. 1 DSG - wie den vorstehenden Erwägungen zu entnehmen ist - kein Gewicht. Insofern liegt auch keine Rechtfertigung vor.

E. 6

Zusammenfassend ergibt sich, dass die Beklagte mit dem bisherigen Zugangssystem und der entsprechenden Art und Weise der Bearbeitung der biometrischen Daten den Grundsatz der Verhältnismässigkeit verletzt. Diese Verletzung ist weder durch Einwilligung noch durch überwiegende private Interessen gerechtfertigt. Es kann damit offen gelassen werden, ob auch die Gefahr besteht, dass die Daten exportiert, kopiert und unbefugt weiterverarbeitet werden könnten, mithin die Datensicherheit nach Art. 7 DSG nicht gewährleistet ist, wie dies der Kläger weiter vorbringt. Aufgabe des BVGer ist es festzustellen, ob ein Zugangssystem datenschutzkonform ist. Es ist hingegen nicht dessen Aufgabe festzulegen, welche Art und Weise der Bearbeitung bei der Verwendung von biometrischen Daten angezeigt ist, mithin ein umfassendes (datenschutzkonformes) Zugangssystem zu liefern. Das vom Kläger vorgeschlagene System erscheint dem BVGer auf den ersten Blick geeignet und den gesetzlichen Anforderungen an die Bearbeitung von biometrischen Daten gewachsen zu sein. Zumindest stellt es ein milderes Mittel im Sinne der Erforderlichkeit im Rahmen der Verhältnismässigkeitsprüfung dar. Da sich die Zuordnungsliste aus technischen Gründen nicht aus der zentralen Datenbank und daher nicht von den entsprechenden Templates entfernen lässt (...), ist eine für die Beklagte weniger einschneidende Massnahme im Rahmen des vorliegenden Verfahrens nicht ersichtlich. Zur Überprüfung einer Zugangsberechtigung könnte es etwa ausreichen, die Templates ohne Zuordnungsliste zu speichern und bei der Einlasskontrolle lediglich zu prüfen, ob das präsentierte Merkmal in der Datenbank vorhanden ist. Zumindest zwischen den Matchingvorgängen bestünde dann für die speichernde Stelle bei ausreichender Grösse der Datenbank keine Möglichkeit der Herstellung eines Personenbezugs (GERRIT HORNUNG, Der Personenbezug biometrischer Daten, in: Zeitschrift « Datenschutz und Datensicherheit », 28 [2004] 7, S. 430). Der Beklagten steht es indes frei, von dem bisherigen System gänzlich abzusehen. Es besteht kein Grund, der Beklagten ein anderes Zugangssystem aufzuzwingen.

E. 7

Im Übrigen ist der Beklagten auch insofern nicht zu folgen als sie rügt, das Vorgehen des Klägers verletze den Grundsatz der Rechtsgleichheit und des Vertrauensschutzes, indem beispielsweise das Kontrollsystem der Bergbahnen nicht bemängelt werde und der Kläger im Rahmen ihres Beschaffungsprozesses keinen Einwand erhoben habe, obwohl gleichartige Systeme bereits im Einsatz gewesen seien. 7.1.1 Der Grundsatz des Vertrauensschutzes (Art. 9 BV) bedeutet, dass die Privaten Anspruch darauf haben, in ihrem berechtigten Vertrauen in behördliche Zusicherungen oder in anderes, bestimmte Erwartungen begründendes Verhalten der Behörden geschützt zu werden

(HÄFELIN/MÜLLER/UHLMANN, a. a. O., Rz. 627). Damit sich jemand auf den Vertrauensschutz berufen kann wird unter anderem eine Vertrauensgrundlage gefordert. Dabei kommt es auf den Bestimmtheitsgrad der Grundlage an, der so gross sein muss, dass der Private daraus die für seine Dispositionen massgebenden Informationen entnehmen kann (HÄFELIN/MÜLLER/UHLMANN, a. a. O., Rz. 631). Grundsätzlich hindert die vorübergehende Duldung eines rechtswidrigen Zustandes die Behörde nicht an der späteren Behebung dieses Zustandes. Eine Vertrauensgrundlage, die der Wiederherstellung der Rechtmässigkeit ganz oder teilweise entgegensteht, wird durch behördliche Untätigkeit nur in Ausnahmefällen geschaffen (HÄFELIN/MÜLLER/UHLMANN, a. a. O., Rz. 652). Weder kann sich die Beklagte vorliegend auf eine ausreichend bestimmte Vertrauensgrundlage stützen, wie etwa eine schriftliche oder mündliche Zusicherung des Klägers, noch kann sie sich im Sinne des Vertrauensschutzes darauf berufen, dass gleichartige - allenfalls auch datenschutzwidrige - Systeme im Einsatz gewesen seien und der Kläger nicht eingeschritten sei. Ein Ausnahmefall ist hier nicht ersichtlich und wird von der Beklagten auch nicht geltend gemacht. 7.1.2 Wie nachfolgend aufgezeigt, kann sich diese auch nicht auf den Grundsatz der Gleichbehandlung berufen. Der Anspruch auf Gleichbehandlung verlangt, dass Rechte und Pflichten der Betroffenen nach dem gleichen Massstab festzusetzen sind. Gleiches ist nach Massgabe seiner Gleichheit gleich, Ungleiches nach Massgabe seiner Ungleichheit ungleich zu behandeln. Das Gleichheitsprinzip verbietet einerseits unterschiedliche Regelungen, denen keine rechtlich erheblichen Unterscheidungen zu Grunde liegen. Andererseits untersagt es aber auch die rechtliche Gleichbehandlung von Fällen, die sich in tatsächlicher Hinsicht wesentlich unterscheiden. Die Gleichbehandlung durch den Gesetzgeber oder die rechtsanwendende Behörde ist allerdings nicht nur dann geboten, wenn zwei Tatbestände in allen ihren tatsächlichen Elementen absolut identisch sind, sondern auch, wenn die im Hinblick auf die zu erlassende oder anzuwendende Norm relevanten Tatsachen gleich sind (HÄFELIN/MÜLLER/UHLMANN, a. a. O., Rz. 495). Der Grundsatz der Gesetzmässigkeit der Verwaltung geht dem Rechtsgleichheitsprinzip im Konfliktfall in der Regel vor. Wenn eine Behörde in einem Fall eine vom Gesetz abweichende Entscheidung getroffen hat, gibt das den Privaten, die sich in der gleichen Lage befinden, grundsätzlich keinen Anspruch darauf, ebenfalls abweichend von der Norm behandelt zu werden (keine Gleichbehandlung im Unrecht). Dies gilt allerdings nur dann, wenn die abweichende Behandlung lediglich in einem einzigen oder in einigen wenigen Fällen erfolgt ist. Besteht hingegen eine eigentliche Praxis und lehnt es die Behörde ab, diese aufzugeben, so können Private verlangen, dass die widerrechtliche Begünstigung, die Dritten zuteil wurde, auch ihnen gewährt werde (Urteil des BVGer A-5541/2008 vom 2. Juli 2009 E. 5.1 mit Hinweisen; HÄFELIN/MÜLLER/UHLMANN, a. a. O., Rz. 518). Das von der Beklagten als Vergleich herangezogene Zugangssystem der Bergbahnen unterscheidet sich in wesentlichen Zügen von ihrem Zugangssystem. Wie der Kläger ausführt, waren die biometrischen Daten beim Zugangssystem der Bergbahnen in keiner Art und Weise Bestandteil der vorgenommenen Sachverhaltsabklärung, das heisst solche werden dabei offenbar auch nicht verwendet. Insofern unterscheiden sie sich in relevanten Tatsachen und taugen daher nicht für einen Vergleich. Im Übrigen ist der Kläger gewillt, die einmal entwickelte Rechtsprechung in Bezug auf die gleichartige Bearbeitung biometrischer Daten in sämtlichen Bereichen anzuwenden und so einer einheitlichen Handhabung zu Durchbruch zu verhelfen.