Schweizerische Eidgenossenschaft
Confédération suisse
Confederazione Svizzera
Confederaziun svizra

Eidgenössischer Datenschutz- und Öffentlichkeitsbeauftragter
EDÖB

Verwendung biometrischer Daten für das Reservationssystem des Tennisclub XX

Schlussbericht

vom 13. Septembre 2010

der Kontrolle des Eidgenössischen Datenschutz- und Öffentlichkeitsbeauftragten (EDÖB) nach Art. 29 des Bundesgesetzes über den Datenschutz (DSG)

Feldeggweg 1, 3003 Bern
Tel. 031 323 74 84, Fax 031 325 99 96
www.edoeb.admin.ch

Inhaltsverzeichnis

1. Ausgangslage

Im Sommer 2009 hat der TC XX ein neues System für die Reservation der Tennisplätze eingeführt. Neu werden die Fingerabdrücke der Mitglieder erfasst und in Form von Templates gespeichert. Jede Reservation eines Tennisplatzes muss nun mit der Mitgliedernummer und mit Einsatz des Fingerabdruckes bestätigt werden, damit der Platz bespielt werden darf.

Das neue Reservationssystem soll sicherstellen, dass nur Berechtigte die Plätze des TC XX nutzen.

2. Umfang der Kontrolle

Die Datenschutzkontrolle bezog sich auf die Datenabläufe im Zusammenhang mit dem neuen Reservationssystem. Der Schwerpunkt lag dabei bei der Bearbeitung der erhobenen biometrischen Daten sowie der im Zusammenhang mit der Online-Reservation veröffentlichten Personendaten.

3. Chronologie der Kontrolle

Anfang Oktober 2009	Der EDÖB erfährt aufgrund von Anfragen von Clubmitgliedern des TC XX vom biometrischen Reservationssystem des Clubs. Nachdem sich innerhalb des Clubs Widerstand formiert hat und mehr als 1000 Personen von diesem Reservationssystem betroffen sind, beschliesst der EDÖB, eine Sachverhaltsabklärung durchzuführen.
15.10.2009	Der EDÖB informiert den TC XX schriftlich über die geplante Datenschutzkontrolle betreffend das Reservationssystem sowie über die geplante Sachverhaltsabklärung vor Ort. Zusätzlich bittet der EDÖB um Dokumentation über das neue System und um Beantwortung eines beigelegten Fragebogens.
30.10.2009	Der TC XX beantwortet den Fragekatalog des EDÖB und schickt Unterlagen.
03.12.2009	Der EDÖB stellt Rückfragen.
14.12.2009	Der TC XX beantwortet die Rückfragen und schickt weitere Unterlagen.
14.01.2010	Der EDÖB macht Terminvorschläge und bittet und Nennung der anwesenden Personen.
27.01.2010	Der Termin wird auf den 11.02.2010 festgelegt.
11.02.2010	Sachverhaltsabklärung mit den verantwortlichen Personen.
2. Hälfte Februar 2010	Mailverkehr zwischen dem EDÖB und dem TC XX betreffend Ergänzungsfragen
05.03.2010	Der EDÖB schickt dem TC XX ein Factsheet mit der Bitte um materielle Bereinigung des Textes und Beantwortung der Ergänzungsfragen.
22.03.2010	Der TC XX bestätigt schriftlich den Inhalt des Factsheets
April 2010	Analyse und Auswertung aller Unterlagen und Sachverhalte sowie Ausarbeitung des Schlussberichtes durch den EDÖB.
13. September 2010	Verabschiedung des Schlussberichtes durch den EDÖB.

4. Sachverhaltsabklärung vom 11. Februar 2010

4.1 Anwesende Personen :

- Präsident des TC XX
- Rechtsvertreter des TC XX
- Systemverantwortlicher des TC XX
- 2 Vertreter des Systemlieferanten
- 2 Mitarbeiter des EDÖB

4.2 Enrolement:

Das Enrolement wird durch das Mitglied selbständig durchgeführt. Die Personalien sowie die Mitgliedernummer bestehen bereits auf der Mitgliederdatenbank des Clubs. Das Mitglied gibt seine Mitgliedernummer in das System ein und liest seinen Fingerabdruck über einen Scanner ein. Aus dem Scan wird ein Template mit 12 Minutien extrahiert und unter der Mitgliedernummer auf dem Server „Biometrie“ im vom Lesegerät generierten Format (ASN.1 DER) gespeichert. Wir gehen davon aus, dass die Templates nur codiert und nicht verschlüsselt gespeichert werden. Der EDÖB verfügen jedenfalls trotz wiederholtem Nachfragen über keinerlei Informationen, welche eine allfällige Verschlüsselung belegen würden (Algorithmus, Schlüssel, Länge des Schlüssels).

Das Reservationssystem funktioniert ohne Karten, so dass sämtliche Daten zentral gespeichert werden. Die Templates befinden sich aber nicht auf demselben Rechner wie die übrigen Mitgliederdaten. Jene sind auf einem PC im Sekretariat (Mitgliederdatenbank) und auf einem Webserver (Reservationssystem) gespeichert. Der PC „Biometrie“ ist dabei durch ein drahtloses Netzwerk (WLAN/WPA) mit dem Sekretariats-PC verbunden, welcher seinerseits via ADSL mit dem Internet verbunden ist. Es werden keine Rohdaten des Fingerabdrucks gespeichert. Gemäss Aussage des Herstellers des Lesegeräts können aus den gespeicherten Templates keine Rohdaten rekonstruiert werden.

4.3 Reservation eines Tennisplatzes

Bevor auf einem Platz gespielt werden darf, muss dieser zwingend reserviert werden. Dies kann entweder vor Ort oder via Internet geschehen. Diese Reservation muss anschliessend bis spätestens 10 Minuten nach Spielbeginn mittels Fingerabdruck bestätigt werden. Es müssen sämtliche Spieler, mit Ausnahme eingeladener Gäste, ihre Anwesenheit mittels Fingerabdruck bestätigen.

Hierzu gibt das Mitglied seine Mitgliedernummer ein. Es folgt die Aufforderung, seinen Finger auf den Scanner zu legen. Durch die Mitgliedernummer wird automatisch das dazugehörende Template (Referenzdatum) aufgerufen und mit dem Fingerabdruck des anwesenden Mitglieds verglichen. Es findet also kein 1:n-Verlgeich (Identifikation) mit der ganzen Datenbank statt, sondern ein 1:1 Vergleich (Verifikation) über die Mitgliedernummer. Ist die Verifikation aller für die Reservation eingeschriebenen Mitglieder gelungen, wird die Reservation bestätigt. Gelingt die Verifikation nicht oder wird die Reservation nicht (vollständig) bestätigt, wird die Reservation 10 Minuten nach Beginn der Reservationszeit gelöscht. Der Platz erscheint im System als „frei“ und darf nicht benützt werden. Wird auf einem Platz ohne Reservation gespielt, können die Spieler vom Platz gewiesen werden.

Über die Reservationen werden im Reservationssystem (Webserver) Logfiles erstellt, und auch die Reservationsdaten selbst werden gespeichert. So ist es möglich, für ca. 1 Jahr Rückwirkend die Reservationen und damit die Platznutzung der Mitglieder einzusehen.

4.4 Löschung der Daten

Es werden an drei verschiedenen Orten Personendaten der Mitglieder gespeichert: In der Mitgliederdatenbank (Sekretariats-PC), im Reservationssystem (Webserver) und in der Template-Datenbank (Biometrie). Gemäss Aussage der Informatiker können alle Daten grundsätzlich jederzeit gelöscht werden. Es seien zurzeit jedoch keine Speicherfristen geregelt, dies läge im Verantwortungsbereich des TC XX. Wenn ein Mitglied austritt, kann das Template einfach gelöscht werden. Im Reservationssystem werden die Daten alle 2 bis 3 Jahre durch die Informatiker gelöscht, Logfiles nach ca. 1 Jahr, um Platz zu schaffen. Der TC XX selbst führt keine regelmässigen Datenlöschungen durch.

Der EDÖB macht vor Ort darauf aufmerksam, dass der Grundsatz der Verhältnismässigkeit der Datenbearbeitung eine frühest mögliche Löschung von Daten verlange und regt an, dass der TC XX Regeln für eine sinnvolle Löschung der Daten einführen soll.

4.5 Aufklärungs- und Auskunftsrecht

Die Mitglieder wurden im Rahmen der entsprechenden Abstimmung der GV vorgängig über das geplante System informiert. Anlässlich der GV fand eine Diskussion statt, in welcher ebenfalls Informationen ausgetauscht wurden. Nachdem der Beschluss zur Einführung des Systems gefasst worden ist, wurden sämtliche Mitglieder per Post oder Mail sowie im Clubmagazin über das System informiert. Eine standardisierte Information von Neumitgliedern besteht nicht. Auf Anregung des EDÖB wird der Präsident die Information der Mitglieder verbessern.

Die Mitglieder können sich jederzeit an den Clubpräsidenten wenden und Einsicht in die Templatedatenbank nehmen. Auf Anregung des EDÖB wird der Präsident dieses Auskunftsrecht auch auf die Mitgliederdatenbank und das Reservationssystem ausdehnen.

4.6 Alternativen zur biometrischen Erfassung

Das System erlaubt es, dass die Reservation mit einem PIN anstelle des Fingerabdrucks bestätigt werden kann. Diejenigen Personen, welche das biometrische System nicht nutzen können oder wollen, können auf dieses System ausweichen. Diese Alternative wird zurzeit von ca. 10 Personen genutzt.

Auf Anregung des EDÖB hat der Präsident eingewilligt, die Mitglieder zukünftig transparent über diese Alternative zu informieren.

4.7 Vorteile des biometrischen Erfassungssystems

Die Anlage des TC XX besteht hauptsächlich aus den Tennisplätzen und dem Clubhaus mit Garderoben und Restaurant. Eine Reception oder dergleichen existiert nicht. Aus diesem Grund muss die Kontrolle, dass nur Berechtigte die Anlage nutzen, automatisiert erfolgen.

Bisher wurde dies mit einem Reservationssystem mit PIN gemacht. Das Problem hierbei war, dass die PINs teilweise weitergegeben und von mehreren Personen (Nichtmitglieder) benutzt wurden. Das System musste daher so abgeändert werden, dass eine eindeutige Verifizierung mit möglichst geringem Aufwand (die finanziellen Mittel des Clubs seien gemäss Aussage des Präsidenten gering) möglich ist. Die Verifizierung mittels Fingerabdruck bietet diese Möglichkeiten und wurde daher ausgewählt. Der Club hat seither einen deutlichen Mitgliederzuwachs erlebt, und trotzdem sind die Plätze weniger ausgebucht als früher. Dies legt den Schluss nahe, dass der Missbrauch des früheren Systems bedeutend war.

Man hat sich bewusst gegen ein System mit Karten entschieden. Die Karten können leicht vergessen oder verloren gehen, was einerseits die Missbrauchsgefahr wieder erhöht und andererseits dem Mitglied einen Zusatzaufwand gibt. Die Mitglieder begrüssen mit grosser Mehrheit die Lösung ohne Karte, weil diese viel bequemer sei („die Finger hat man immer mit dabei…“). Das System sei bei einer grossen Mehrheit der Mitglieder akzeptiert und man sei sehr zufrieden mit dieser Lösung.

4.8 Weiterleitung von Daten an aussenstehende Dritte

Es werden keine biometrischen Daten an Dritte weitergeleitet. Es findet auch kein Transfer solcher Daten an den Hersteller statt, das System ist nicht mit dem Hersteller verbunden.

Dagegen ist das Reservationssystem (ohne biometrische Daten) ohne Passwortschutz oder dergleichen auf der Website des Clubs abrufbar. Jeder Internetnutzer kann damit sehen, wer zu welcher Zeit welchen Platz reserviert hat. Dies ist auch rückwirkend für 2-3 Jahre möglich. Jedes Clubmitglied kann beim Einrichten seines Benutzerkontos zwar den Benutzernamen abändern und so ein Pseudonym anzeigen lassen. Die Default-Einstellung entspricht jedoch dem ersten Buchstaben des Vornamens, gefolgt von max. den ersten 20 Buchstaben des Nachnamens.

4.9 Serverraum und Server, Datensicherheit

Die Templates sind auf einem PC „Biometrie“ gespeichert, welcher sich in einem Vorraum zum Clubhaus befindet. Der Raum ist mit einer normalen Türe mit einfachem Schloss gesichert. Zutritt zu diesem Raum haben der Clubpräsident, der Verwalter, der Informatiker sowie 2 bis 3 weitere Personen. Auf einem Tablar ausserhalb des Gebäudes befinden sich folgende zum PC „Biomentrie“ gehörenden Peripherie-Geräte: Eine numerische Tastatur zur Eingabe der Mitgliedernummer, ein Fingerabdrucklesegerät und eine Maus, mit der auf dem Bildschirm navigiert werden kann.

Die Mitgliederdaten befinden sich auf einem PC im Clubsekretariat, welches sich im 1. Stock des Clubhauses, von aussen zugänglich über eine Galerie, befindet. Das Sekretariat ist ebenfalls mit einer normalen Tür mit einfachem Schloss gesichert und kann während der Öffnungszeiten des Sekretariats von Jedermann betreten werden. Ausserhalb der Öffnungszeiten haben der Präsident, der Verwalter, der Informatiker, 4 Vorstandsmitglieder sowie 4 Angestellte Zutritt zum Sekretariat. Der Zugang zum Sekretariats-PC ist mit einem Passwort gesichert. Hier muss beachtet werden, dass auch vom Sekretariats-PC aus via eine versteckte Partition auf dem PC „Biometrie“ auf die Templates zugegriffen werden kann. Um die Sicherheit dieses Zugangs zu erhöhen, wurde dem EDÖB vorgeschlagen, hierfür ein separates Administratorenprofil zu erstellen.

Das Reservationssystem befindet sich auf einem Webserver. Der Zugang zu den Personendaten wird durch ein Passwort für den Administrator des Reservationssystems geschützt. Wir kennen die Vertragsbedingungen betreffend Datenschutz mit dem Serverbetreiber nicht.

Die beiden PCs sind mit dem Internet und untereinander via WIFI verbunden. Das WIFI wird zurzeit durch das Protokoll WPA geschützt (ab März 2010 durch das Protokoll WPA2) und kann gemäss Website auch von Mitgliedern für den Zugang zum Internet benutzt werden. Diese erhalten auf Anfrage das Zugangspasswort.

Die nicht biometrischen Personendaten der Mitglieder werden in Klartext gespeichert, während die Templates angeblich verschlüsselt gespeichert werden. Der EDÖB geht aber davon aus, dass es sich eher um eine Codierung (ASN.1 DER) als um eine Verschlüsselung handelt, insbesondere da er keinerlei Informationen betreffend die behauptete Verschlüsselung erhalten hat (Algorithmus, Schlüssel, Länge des Schlüssels).

4.10 Systemwartung

Die Systemwartung erfolgt durch die Informatiker des TC XX. Die Templates können aufgrund der Codierung/Verschlüsselung im Rahmen von Wartungsarbeiten nicht gelesen werden, die übrigen, unverschlüsselt gespeicherten Daten dagegen schon.

5. Datenschutzrechtliche Beurteilung

5.1 Biometrische Daten als Personendaten

5.1.1 Ausgangslage

Das Bundesgesetz über den Datenschutz vom 19. Juni 1992 (DSG; SR 235.1) findet dort Anwendung, wo mit Personendaten im Sinne des Art. 3 lit. a DSG operiert wird. Im vorliegenden Fall werden für die Reservation eines Tennisplatzes biometrische Daten bearbeitet (Templates von Fingerabdrücken).

5.1.2 Beurteilung aus Sicht des EDÖB

Biometrische Daten der Fingerabdrücke in Form von Templates (=Referenzdatum) machen eine Person durch Abgleich mit einem aktuell präsentierten Fingerabdruck bestimmbar. Somit können die biometrischen Daten der Verifizierung (resp. Identifizierung) einer Person dienen. Die Bestimmbarkeit ergibt sich nicht nur aus dieser Abgleichsmöglichkeit, sondern auch dadurch, dass eine Verbindung zwischen der Template-Datenbank und dem Sekretariats-PC mit den Mitgliederdaten besteht. Die biometrischen Daten in Form von Templates können in Verbindung mit diesen weiteren Daten klar einer Person zugeordnet werden und machen diese bestimmbar (Art. 3 lit. a DSG).

Im Falle des TC XX werden 12 Minutien, die aus einem Fingerabdruck entnommen werden, abgespeichert. Die Minutien-Daten werden mittels eines mathematischen Algorithmus codiert und komprimiert. Die Algorithmen für die Template-Extrahierung von biometrischen Rohdaten sind heutzutage weder standardisiert noch transparent, weswegen es derzeit schwierig ist, die Sensibilität (Elemente über Gesundheit/Rasse) eines Templates formell abschliessend einschätzen zu können. Zudem machen biometrische Daten in Form von Rohdaten oder Templates eine Person identifizierbar resp. bestimmbar, und ihre Erhebung hinterlässt in der Regel – insbesondere bei der Erhebung von Fingerab-

drücken – (Daten-) Spuren. Die Erhebung von Rohdaten oder Templates ist somit geeignet, ein Bewegungsprofil der betroffenen Person zu erstellen. Gestützt auf diese Tatsache besteht bei der Erhebung biometrischer Daten für die betroffene Person ein hohes Gefährdungspotenzial für ihre Persönlichkeitsrechte. Ferner ist festzuhalten, dass auch der Europarat und die Art. 29-Datenschutzgruppe der EU (Richtlinie 95/46/EG des Europäischen Parlaments und des Rates vom 24. Oktober 1995 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten und zum freien Datenverkehr) aus gleichen Gründen die hohe Sensibilität biometrischer Daten anerkennt.

5.2 Zweck der Datenbearbeitung

5.2.1 Ausgangslage

Jede Bearbeitung von Personendaten stelle einen Eingriff in das Recht auf informationelle Selbstbestimmung gemäss Art. 13 Abs. 2 der Bundesverfassung der Schweizerischen Eidgenossenschaft vom 18. April 1999 (BV; SR 101) dar. Daher bedarf die Bearbeitung einer besonderen Rechtfertigung. Praktikabilitätserwägungen oder allgemeine Kundenfreundlichkeit stellen grundsätzlich keine ausreichende Rechtfertigung für die Bearbeitung biometrischer Daten dar.

Gemäss Angaben des TC XX geht es beim Erfassen biometrischer Daten ausschliesslich darum, den Missbrauch der Tennisplätze durch Unberechtigte zu verhindern. Vor Einführung des biometrischen Reservationssystems wurden die Plätze mit einem PIN reserviert, was sich als missbrauchsanfällig erwiesen hat. Die Nummern wurden teilweise weitergeben und durch mehrere Personen (Nichtmitglieder) verwendet. Dies ist mit dem neuen, biometrischen System nicht mehr möglich. Der TC XX hat denn auch seit Einführung des neuen Systems einen deutlichen Mitgliederzuwachs erfahren, während die Plätze aber weniger frequentiert werden.

Auf den Einsatz von Kartensystemen wurde bewusst verzichtet, da hier die Gefahr besteht, dass die Karten verloren oder vergessen gehen und die Mitglieder ein kartenloses System aus Komfortgründen bevorzugen.

5.2.2 Beurteilung aus Sicht des EDÖB

Das neue Reservationssystem und die damit verbundene Erhebung biometrischer Daten verfolgt nachvollziehbare Zwecke. Für den EDÖB stellt sich jedoch ernsthaft die Frage, ob es nicht Alternativen zur Missbrauchsvermeidung gäbe, welche weniger stark in die Persönlichkeitsrechte der Betroffenen eingreifen würden (vgl. dazu auch die grundsätzlichen Bemerkungen zur Verhältnismässigkeit unter Ziff. 5.5).

5.3 Rechtmässigkeit der Datenbeschaffung / Einwilligung der Betroffenen

5.3.1 Ausgangslage

Biometrische Daten sind Personendaten im Sinne des Datenschutzgesetzes, für deren Bearbeitung ein Rechtfertigungsgrund (Art. 12 und 13 DSG) benötigt wird. Als Rechtfertigung der Datenbearbeitung kommt im vorliegenden Fall die Einwilligung der Betroffenen in Frage.

Gemäss Auskunft des TC XX wurde das geplante System an der Generalversammlung in grundsätzlicher Hinsicht besprochen. Bei der anschliessend durchgeführten Abstimmung har sich die Mehrheit

der Mitglieder für die Einführung eines solchen Systems ausgesprochen. Das System wurde in der Folge eingeführt und auf der Website resp. auf dem „Borne“ eine Gebrauchsanweisung aufgeschaltet, welche über das Reservationssystem Auskunft gibt. Gemäss Auskunft des TC XX werden Neumitglieder zudem vom Präsidenten mündlich über das Reservationssystem informiert.

Offenbar existieren keine schriftlichen Aufzeichnungen darüber, welche Informationen den Mitgliedern anlässlich der GV gegeben wurden. Es muss jedoch davon ausgegangen werden, dass die Informationen nur grundsätzlicher Natur waren und insbesondere nicht über die Bearbeitungsmodalitäten im Rahmen des biometrischen Reservationssystems (z.B. Speicherort, Speicherdauer, Zugriffsberechtigungen u.V.m.) Auskunft gaben.

Die Gebrauchsanweisung für das Reservationssystem äussert sich nur grob über die Bearbeitungsmodalitäten des Systems. Sie gibt hauptsächlich Auskunft über das Vorgehen beim Enrolement und bei der Reservation.

Die mündliche Auskunft durch den Präsidenten erfolgt jeweils individuell und ist nicht standardisiert. Es ist auch hier davon auszugehen, dass der Präsident nicht über die Bearbeitungsmodalitäten informiert.

Weiteres Informationsmaterial existiert zurzeit nicht, soll aber gemäss Auskunft des TC XX erstellt und an die Mitglieder abgegeben werden.

Diejenigen Personen, welche das biometrische Reservationssystem nicht benützten können oder wollen, können die Reservation, wie bis anhin, mit einem PIN vornehmen. Zurzeit machen ca. 10 Personen von dieser Möglichkeit Gebrauch. Die Mitglieder werden nicht vorgängig über diese Alternative informiert. Erst, wenn sich jemand weigert, seine biometrischen Daten zu erfassen, oder wenn sich herausstellt, dass das biometrische System nicht benutzt werden kann, wird auf die Alternative hingewiesen.

5.3.2 Beurteilung aus Sicht des EDÖB

Aus Sicht des EDÖB müssen für die Einwilligung der Betroffenen – gerade in so einem sensiblen Bereich wie bei der Bearbeitung von Fingerabdrücken – strenge Anforderungen an die Aufklärung der betroffenen Personen gestellt werden. Es ist daher zu fordern, dass die Mitglieder konkreter über die Bearbeitungsmodalitäten informiert werden, damit sie sich über die Tragweite ihrer Einwilligung im Klaren sind. Es sind den Betroffenen daher die Hauptpunkte der Datenbearbeitung mitzuteilen, wie z.B. wo und für wie lange die Daten gespeichert werden, was mit den Templates und den Transaktionsdaten geschieht, wer Zugriff auf die Daten hat und an wen sie, wenn überhaupt, weitergegeben werden. Dies sollte mittels standardisiertem Informationsblatt geschehen, welches sämtlichen bestehenden und neu eintretenden Mitgliedern abzugeben ist. Das Informationsblatt muss vom Vorstand des TC XX unterschrieben und mit einer Versionenkontrolle versehen werden. Zudem müssen die Mitglieder über die Alternative (vorliegend: Reservation mittels PIN) informiert werden, damit die Einwilligung freiwillig erfolgt und nicht unter der vermeintlichen Annahme, man habe keine Wahl.

Die Mitglieder verfügten im Zeitpunkt der GV-Abstimmung nicht über die notwendigen Kenntnisse der Sachlage, um eine rechtsgenügliche Einwilligung abzugeben. Zudem muss an dieser Stelle darauf hingewiesen werden, dass nur die Einwilligung jedes einzelnen Betroffenen die Verletzung der Persönlichkeitsrechte zu rechtfertigen vermag. Ein Mehrheitsbeschluss an einer GV erfüllt diese Voraussetzung nicht.

Auch im jetzigen Zeitpunkt muss davon ausgegangen werden, dass die Mitglieder nicht genügend über die Bearbeitungsmodalitäten informiert sind, um rechtsgültig in die Datenbearbeitung einzuwilligen. Erst, wenn die oben aufgeführten Voraussetzungen erfüllt sind und sich die Mitglieder in Kenntnis dieser Informationen für das biometrische Reservationssystem entscheiden, kann eine rechtsgültige Einwilligung geprüft werden.

5.4 Bearbeitung nach Treu und Glauben / Transparenz

5.4.1 Ausgangslage

Die Bearbeitung von Personendaten muss nach Treu und Glauben erfolgen (Art. 4 Abs. 1 DSG). Die bedeutet zum einen, dass die Datenbearbeitung für die betroffenen Personen transparent erfolgen muss. Zum anderen muss eine Datenbeschaffung und jede weitere Datenbearbeitung grundsätzlich für die Betroffenen erkennbar sein.

Wie bereits unter Ziffer 5.3 ausgeführt, wurden die Mitglieder anlässlich der GV, durch die Gebrauchsanweisung für das Reservationssystem sowie mündlich durch den Vereinspräsidenten über die Erhebung biometrischer Daten informiert. Ein standardisiertes Infoblatt besteht indessen nicht. Das Enrolement erfolgt durch das Mitglied selbst. Dieses muss also aktiv tätig werden, damit seine biometrischen Daten erfasst werden können (Abrollen des Fingers auf dem Sensor beim „Borne“ beim Clubeingang). Ohne sein Zutun können keine biometrischen Daten erhoben werden.

5.4.2 Beurteilung aus Sicht des EDÖB

Da die biometrischen Daten nicht ohne Zutun der Betroffenen erhoben werden können, erfolgt die Datenbearbeitung für diese auf klar erkennbare Weise. Für eine möglichst transparente Datenbearbeitung sollte neben den zurzeit den Mitgliedern gegebenen Informationen noch ein standardisiertes Informationsblatt abgegeben werden, auf dem beschrieben wird, was mit den Personendaten geschieht. Es kann auf das unter Ziffer 5.3 Geschriebene verwiesen werden.

5.5 Verhältnismässigkeit der Datenbearbeitung

Die Bearbeitung von Personendaten hat sich am Grundsatz der Verhältnismässigkeit auszurichten (Art. 4 Abs. 2 DSG). Dies bedeutet, dass ein Datenbearbeiter nur diejenigen Daten bearbeiten darf, die er für einen bestimmten Zweck objektiv tatsächlich benötigt und die im Hinblick auf den Bearbeitungszweck und die Persönlichkeitsbeeinträchtigung in einem vernünftigen Verhältnis stehen.

5.5.1 Verhältnismässigkeit in inhaltlicher Hinsicht - Ausgangslage

Eine Datenbearbeitung ist dann verhältnismässig, wenn sie sich inhaltlich auf das absolut Notwendige beschränkt, um ein bestimmtes Ziel zu erreichen. Die inhaltliche Verhältnismässigkeit fordert einen möglichst schonenden Umgang mit Personendaten. Dies bedingt auch, dass keine für den verfolgten Zweck nicht benötigten Überschussinformationen anfallen. Ebenso ist es unzulässig, Personendaten auf Vorrat zu erheben, sofern der damit verfolgte Zweck dies nicht unabdingbar erfordert.

Mit der Einführung des neuen Reservationssystems werden aus den Fingerabdrücken der Mitglieder Templates generiert und diese zentral in einer Datenbank abgelegt. Rohdaten (d.h. das Originalbild des Fingerabdrucks) werden keine erhoben. Das System funktioniert ohne Karten. Eine zuvor über das Reservationssystem online oder auf dem „Borne“ getätigte Platzreservation wird bestätigt, indem die Mitgliedernummer eingegeben und anschliessend der Finger auf das Lesegerät gehalten wird. Das aktuell erstellte Template wird nun mit dem durch die Mitgliedernummer ermittelten Referenzdatum verglichen. Stimmen die beiden Templates überein, wird die Reservation bestätigt und die Reservation bleibt für die nächsten zwei bis drei Jahre im Reservationssystem gespeichert und abrufbar. Stimmen die Templates nicht überein, wird die Reservation nicht bestätigt und 10 Minuten nach Beginn der Reservationszeit gelöscht.

Nebst den Templates werden im Sekretariats-PC weitere Daten der Mitglieder (Personalien, Spielerdaten etc.) und im Reservationssystem die Reservationsdaten gespeichert. Die Reservationsdaten sind ohne Passwortschutz durch sämtliche Internetnutzer über das Internet abrufbar. Hierbei werden der Benutzername (im Defaultzustand erster Buchstabe des Vornamens sowie max. die ersten 12 Buchstaben des Nachnamens) sowie die Reservationszeiten für die vergangenen zwei bis drei Jahre angezeigt. Um eine Reservation zu tätigen, muss sich das Mitglied mit seinem Benutzernamen und einem Passwort einloggen. Der angezeigte Name kann durch das Mitglied selbständig geändert werden.

5.5.2 Beurteilung der inhaltlichen Verhältnismässigkeit aus Sicht des EDÖB

5.5.2.1 Zentrale Speicherung biometrischer Daten

Der Einsatz biometrischer Verfahren im Privatbereich stellt je nach Ausgestaltung im konkreten Einzelfall einen mehr oder weniger intensiven Eingriff in die Persönlichkeitsrechte der Betroffenen dar. Grundsätzlich sind daher vor dem Einsatz biometrischer Verfahren immer auch andere geeignete Massnahmen zu prüfen, welche weniger in die Grundrechte der Betroffenen eingreifen und mit denen der angestrebte Zweck ebenfalls erreicht werden kann. Des Weiteren muss schon bei der Auswahl und Ausgestaltung des biometrischen Verfahrens darauf geachtet werden, ein möglichst datensparsames System auszuwählen, das in einem vernünftigen Verhältnis zum angestrebten Zweck steht. Wie die Art. 29-Datenschutzgruppe der EU in ihrer Stellungnahme zum Einsatz von Biometrie festhält, sind bei der Beurteilung der Verhältnismässigkeit „auch die Risiken für den Schutz der Grundrechte und –freiheiten des Einzelnen zu berücksichtigen, vor allem die Frage, ob der beabsichtigte Zweck nicht auch auf eine weniger in die Rechte der Betroffenen eingreifende Weise zu erreichen ist“. Wie die Art. 29-Datenschutzgruppe weiter festhält, „sind biometrische Systeme, die zur Zugangskontrolle (Verifikation) eingesetzt werden, mit geringeren Gefahren für den Schutz der Grundrechte und –freiheiten des Einzelnen verbunden, wenn sie entweder auf Körpermerkmalen basieren, die keine Spuren hinterlassen (z.B. in Form der Hand, aber keine Fingerabdrücke), oder wenn sie zwar Körpermerkmale verwendet, die Spuren hinterlassen, die Daten jedoch auf einem Medium gespeichert werden, das sich im Besitz der betroffenen Person befindet (mit anderen Worten, wenn die Daten nicht im Gerät, das den Zugang kontrolliert oder in einer zentrales Datenbank gespeichert werden (Art. 29-Datenschutzgruppe, Arbeitspapier über Biometrie, angenommen am 1. August 2003, 12168/08/DE WP 80)).

Im vorliegenden Fall geht es um ein Reservationssystem für eine Freizeitanlage. Die Biometrie wird zur Verifizierung der Clubmitglieder eingesetzt. Datensparsamkeit erreicht man, indem nur die unbedingt zur Verifizierung notwendigen biometrischen Daten erhoben werden. Zur Verifizierung werden keine Rohdaten benötigt. Der Vergleich mit Templates reicht aus, um die berechtigte Person bei der Bestätigung der Reservation zu verifizieren. Die Beschränkung der Speicherung biometrischer Daten auf Templates, wie dies vom TC XX vollzogen wird, ist unter dem Gesichtspunkt der Datensparsamkeit verhältnismässig.

Biometrische Daten sind dauerhaft personengebunden. Aus diesem Grund sollten die biometrischen Daten – gerade wenn es um so heikle Bereiche wie Fingerabdrücke geht – im Einflussbereich der betroffenen Person, d.h. des Mitglieds, gespeichert werden und dort verbleiben.

Aus dem bisher Gesagten folgt, dass für eine datenschutzkonforme Umsetzung biometrischer Verifizierungssystemen im Freizeitbereich die nachfolgend beschriebenen drei Varianten in Frage kommen. Für den Einsatz biometrischer Charakteristika, die (physische oder digitale) Spuren hinterlassen (z.B.

Fingerabdrücke oder Gesichtsfotografien), können nur die Varianten a) und b) durch den Einsatz von individuellen Karten ein genügendes Sicherheitsniveau garantieren. Die Variante c) ohne Karten kann dagegen nur dann eingesetzt werden, wenn biometrische Charakteristika verwendet werden, die keine Spuren hinterlassen (z.B. Fingervenen oder Handumriss).

a) Dezentralisierung (auf Karten)

Wie der EDÖB in seinem Leitfaden zu biometrischen Erkennungssystemen vom September 2009 festhält, wird beim Einsatz von Biometrie im Privatbereich der Persönlichkeitsschutz der Betroffenen am ehesten gewahrt, indem

1. die biometrischen Daten auf einem Sicherheitsmedium, da sich in der alleinigen Kontrolle der betroffenen Person befindet, auslesesicher gespeichert werden;

2. die betroffene Person jeden Zugriff auf die Daten explizit und bewusst freigeben muss; und

3. die Verifizierung der Identität ausschliesslich auf diesem Sicherheitsmedium stattfindet, so dass die biometrischen Daten zu keinem Zeitpunkt die gesicherte Umgebung des Mediums und die Kontrolle der betroffenen Person verlassen (biometrischer Vergleich auf Karte, vgl. Leitfaden S. 13).

b) Pseudodezentralisierung (mit Karten)

Ein annährend gleich hohes Niveau betreffend den Persönlichkeitsschutz kann mit der Pseudodezentralisierung erreicht werden. Diese Lösung wurde denn auch vom Bundesverwaltungsgericht in seinem Urteil vom 4 August 2009 in Sachen KSS (A-3908/2008) skizziert. Im Unterscheid zur richtigen Dezentralisierung werden die biometrischen Daten zentral gespeichert, der logische Zugang zu diesen Daten ist aber einzig durch den Einsatz eines Zuordnungscodes möglich, der auf einer Karte gespeichert wird, die sich ausschliesslich im Besitz der betroffenen Person befindet. Im Einzelnen bedeutet dies Folgendes:

1. Die biometrischen Daten werden als verschlüsselte Templates zentral gespeichert (und nicht als Rohdaten, z.B. als Fingerabdruckbild oder als Fotografie);
2. die Templates sind so gespeichert, dass der Inhaber der Datensammlung keinen Bezug zu einer bestimmten oder bestimmbaren Person herstellen kann. Statistische Daten oder weitere Angaben (z.B. Zeitstempel) können in Verbindung mit den biometrischen Daten so lange gespeichert werden, wie durch sie keine Identifizierung der fraglichen Person möglich wird;
3. die Verbindung zwischen dem Template und der betroffenen Person kann einzig durch eine explizite und bewusste Freigabe durch die Verwendung der persönlichen Karte hergestellt werden.

c) Zentralisierung (ohne Karten)

Wird ein Verifizierungssystem ohne die Verwendung persönlicher Karten im Freizeitbereich gewünscht, so ist dies nur mit einer Zentralisierung der biometrischen Daten möglich. Da die zentrale Speicherung biometrischer Daten für den Verifzierungsprozess normalerweise nicht notwendig wäre, muss das System angepasst werden, damit es nicht gegen den Grundsatz der Verhältnismässigkeit verstösst:

1. Es dürfen nur biometrische Charakteristika verwendet werden, die keine (physischen oder digitalen) Spuren hinterlassen;

2. die biometrischen Daten werden als verschlüsselte Templates zentral gespeichert (und nicht als Rohdaten, z.B. als Fotografie);
3. die Templates sind so gespeichert, dass der Inhaber der Datensammlung keinen Bezug zu einer bestimmten oder bestimmbaren Person herstellen kann. Statistische Daten oder weitere Angaben (z.B. Zeitstempel) können in Verbindung mit den biometrischen Daten so lange gespeichert werden, wie durch sie keine Identifizierung der fraglichen Person möglich wird;
4. die Verbindung zwischen dem Template und der betroffenen Person wird einzig in flüchtiger Weise durch das Erkennungssystem hergestellt, mit dem Ziel, die Zugehörigkeit einer Person zum Kreis der Berechtigten festzustellen. Alle weiteren Operationen (Identifizierung der Person, Bestätigung der Reservation…) werden davon getrennt und ohne Verwendung biometrischer Charakteristika durchgeführt.

Daraus folgt, dass der TC XX in Zukunft eine der vorgeschlagenen Varianten wählt, wenn an der Verwendung biometrischer Erkennungssysteme festgehalten wird. Die gilt auch für die bereits zentral gespeicherten biometrischen Daten. Eine zentrale Speicherung, wie sie zurzeit praktiziert wird, ist unter dem Blickwinkel des Grundsatzes der Datensparsamkeit und des Grundsatzes der möglichst schonenden Bearbeitung von Personendaten, im vorliegenden Fall der Reservation von Tennisplätzen des TC XX, unverhältnismässig.

5.5.2.2 Veröffentlichung der Reservationsdaten im Internet

Das Reservationssystem ermöglicht es den Mitgliedern, die Platzreservation via Internet vorzunehmen und die so getätigte Reservation anschliessend vor Ort mit dem Fingerabdruck zu bestätigen. Zu diesem Zweck ist das System auf der Website des TC XX aufgeschaltet. Der EDÖB anerkennt, dass die Online-Reservation den Mitgliedern einen grossen Nutzen bringt und daneben auch die Möglichkeit eröffnet, Spielpartner zu suchen und zu finden. Zur Erfüllung dieses Zwecks erscheint es auch verhältnismässig, den Mitgliedern einen Online-Zugang zum Reservationssystem zu gewähren.

Nach Ansicht des EDÖB besteht dagegen kein Grund dafür, den Zugang zu den Reservationsdaten ohne Beschränkung zuzulassen und damit auch Nichtmitgliedern Einsicht zu gewähren. Dies geht weit über das für die Zweckerreichung Notwendigen hinaus. Nach Ansicht des EDÖB ist der Online-Zugang zum Reservationssystem daher auf die Clubmitglieder zu beschränken. Dies kann beispielsweise durch einen Passwortschutz geschehen. Nachdem die Online-Reservation ohnehin ein Login erfordert, bedarf es für diese Beschränkung nur einer geringfügigen Änderung des Systems. So könnte man beispielsweise bereits für die Einsicht in die Reservationsdaten ein Login verlangen.

Der EDÖB regt zudem an, dass bei Erstellung eines Benutzerkontos automatisch darauf hingewiesen wird, dass bei unveränderten Grundeinstellungen im Online-Reservationssystem der richtige Nachname angezeigt wird, dass explizit danach gefragt wird, ob die betroffene Person damit einverstanden ist und auf die Möglichkeit der Pseudonymisierung des angezeigten Namens verwiesen wird.

Zusammenfassend kann festgehalten werden, dass die jetzige Veröffentlichung der Reservationsdaten im Internet weit über das zur Zweckverfolgung Notwendige hinausgeht. Sie ist damit unter dem Grundsatz der möglichst schonenden Bearbeitung von Personendaten unverhältnismässig.

5.5.3 Verhältnismässigkeit in zeitlicher Hinsicht – Ausgangslage

Das Erfordernis der Verhältnismässigkeit begrenzt die Datenbearbeitung auch in zeitlicher Hinsicht. Sofern personenbezogene Daten für den verfolgten Zweck nicht mehr gebraucht werden, sind sie zu vernichten oder zu anonymisieren. Dabei ist eine frühest mögliche Löschung/Anonymisierung vorzusehen.

Vorliegend werden an drei Orten Personendaten gespeichert: Auf dem PC „Biometrie“, auf dem Sekretariats-PC und auf dem Webserver für das Reservationssystem. Für keinen dieser Speicherorte besteht eine Regelung für die Speicherdauer oder die Zuständigkeit für die Löschung. Bis jetzt werden auf dem PC „Biometrie“ und auf dem Sekretariats-PC keine regelmässigen Datenlöschungen durchgeführt, im Reservationssystem werden die Reservationsdaten aus Platzgründen alle 2 bis 3 Jahre, die Logdaten nach ca. 1 Jahr, gelöscht.

5.5.4 Beurteilung der zeitlichen Verhältnismässigkeit aus Sicht des EDÖB

Der EDÖB hat bereits bei der Besichtigung der Anlage vor Ort darauf aufmerksam gemacht, dass bei der Bearbeitung von sensiblen Personendaten die Speicherdauer der Daten sowie die Zuständigkeit für die Löschung nicht mehr benötigter Daten geregelt und in einem Reglement festgehalten werden sollte, da für die Betroffenen sonst nicht einschätzbar ist, wie lange die Daten gespeichert werden. Zudem besteht tatsächlich die Gefahr, dass der Löschung der Daten zu wenig Beachtung geschenkt wird und diese daher dauerhaft aufbewahrt würden.

Die Templates auf dem PC „Biometrie“ sowie die auf dem Sekretariats-PC gespeicherten Mitgliederdaten sind zu löschen, sobald sie nicht mehr benötigt werden. Dies ist spätestens dann der Fall, wenn ein Mitglied den Austritt gibt. Die Löschung der Daten beim Austritt muss daher einerseits im Reglement festgehalten und in den Standardprozess für solche Fälle aufgenommen werden. Für den EDÖB sind keinerlei Gründe ersichtlich, welche die Speicherdauer von 2 bis 3 Jahren für die Reservationsdaten und die von einem Jahr für die Logdaten im Reservationssystem rechtfertigen würden.

Es wird daher davon ausgegangen, dass die Speicherdauern unverhältnismässig lange sind und auf ein angemessenes Mass reduziert werden müssen. Der TC XX hat dem EDÖB daher einen Vorschlag zu unterbreiten, wie die Löschfristen festgelegt werden sollen und diese Fristen anschliessend (technisch) umzusetzen. Dabei muss nebst der Löschung der oberwähnten Daten auch diejenige von diesen Daten gemachten Backups und dergleichen geregelt werden.

5.6 Zweckbindung der Datenbearbeitung

5.6.1 Ausgangslage

Personendaten dürfen nur für den Zweck bearbeitet werden, welcher bei der Beschaffung angegeben worden ist oder der aus den Umständen ersichtlich oder gesetzlich vorgesehen ist (Art. 4 Abs. 3 DSG). Da eine Änderung des Bearbeitungszwecks von den Betroffenen durch die zentrale Speicherung der biometrischen Daten nicht kontrollierbar ist, sind technische Lösungen vorzuziehen, welche die Zweckbindung ausreichend gewährleisten.

5.6.2 Beurteilung aus Sicht des EDÖB

Durch die zentrale Speicherung der Templates in der Datenbank ist eine Zweckentfremdung in der Bearbeitung dieser Daten nicht gänzlich ausgeschlossen. Dies unter anderem auch deshalb, weil die Daten sich nicht in der Nutzersphäre der Betroffenen befinden. Eine Zweckentfremdung im Sinne einer Verknüpfung mit anderen Datensammlungen oder eine Weitergabe an aussen stehende Dritte wäre möglich. Auch wenn die Tatsache berücksichtigt wird, dass keine Rohdaten, sondern Templates in der Datenbank abgelegt werden, ist auch aus Gründen der Zweckbindung der Datenbearbeitung

auf eine zentrale Speicherung der biometrischen Daten, wie sie zurzeit praktiziert wird, zu verzichten und auf einer der unter Ziffer 5.5.2.1 aufgeführten Varianten umzustellen.

5.7 Datenrichtigkeit (Zuverlässigkeit, Anwendbarkeit)

5.7.1 Ausgangslage

Das Vergleichsverfahren zwischen Referenz- und aktuell präsentieren Daten (hier Templates der Fingerabdrücke) basiert auf Wahrscheinlichkeitsberechnungen und ergibt einen Übereinstimmungswert, der grösser als eine vordefinierte Schwelle sein muss, um die Person zu erkennen. Von dieser einzigen Schwelle sind die beiden Werte „Fals Rejection Rate (FFR)“ und „False Acceptance Rate (FAR)“ umgekehrt abhängig. Aus Gründen des Persönlichkeitsschutzes sollte von allem die FAR vermindert werden, ohne aber die FRR zu stark zu beeinträchtigen. Die Wahl eines optimalen Schwellenwertes für eine ausreichende Zuverlässigkeit des gesamten biometrischen Systems ist aus diesem Grunde nicht einfach zu treffen.

Nicht ausser Acht gelassen werden darf auch die Tatsache, dass gewisse Anwender (aufgrund fehlender Gliedmassen, Verletzungen, Narben oder aufgrund des Alters, wie z.B. Kinder oder ältere Personen) keine oder zu wenig gute biometrische Merkmale vorweisen und ihre Verifizierung misslingen kann. Für diese Personen ist ein Alternativszenario vorzusehen, welches nicht zu einer Diskriminierung der Betroffenen führen darf.

5.7.2 Beurteilung aus Sicht des EDÖB

Aus Datenschutzgründen sollte die FAR vermindert werden, ohne aber die FRR zu stark zu beeinträchtigen. Zudem sollte ein optimaler Schwellenwert gewählt werden. Jedes biometrische System weist einen gewissen Prozentsatz an FAR auf. Die Verifizierung kann infolgedessen nicht zu 100 % zuverlässig erfolgen. Das System des TC XX extrahiert 12 Minutien pro Template. Dies ist aus heutiger Sicht knapp ausreichend. Tests vor Ort haben denn auch ergeben, dass das System funktioniert.

Probleme ergeben sich weiter auch bei Personen, denen gewisse biometrische Merkmale fehlen oder nur schlecht lesbar vorhanden sind (Enrolement). Für solche Ausnahmen muss eine äquivalente Anwendbarkeit des Erkennungssystems geplant und eingesetzt werden. Eine solche Alternative besteht vorliegend. Anstelle einer Verifizierung mittels Fingerabdrücken wird eine PIN eingesetzt. Diese Alternative ist für die Betroffenen sowohl kostenneutral als auch von der Handhabung her äquivalent. Es gibt offenbar bereits Mitglieder, welche das Fingerabdrucksystem aus gesundheitlichen Gründen nicht nutzen können und ihre Reservationen daher mittels PIN bestätigen. Dies funktioniert problemlos.

Die Datenrichtigkeit ist damit beim Reservationssystem des TC XX gewährleistet. Der EDÖB hat hier keine weiteren Bemerkungen.

5.8 Datensicherheit

5.8.1 Ausgangslage

Gemäss Art. 7 DSG müssen Personendaten durch angemessene technische und organisatorische Massnahmen gegen unbefugtes Bearbeiten gesichert werden. Zu gewährleisten sind insbesondere die Vertraulichkeit, die Verfügbarkeit sowie die Integrität der Personendaten. Diese Anforderungen

sind dann nicht mehr gewährleistet, wenn Unbefugte leichten Zugriff auf die Daten haben oder ein fremdes „Drittgerät“ die Daten abhören oder manipulieren könnte. Die Datensicherheit liegt in der Verantwortung derjenigen Stelle, welche die Datenherrschaft über die Personendaten inne hat (Art. 8 Abs. 1 der Verordnung zum Bundesgesetz über den Datenschutz vom 14. Juni 1993 (VDSG; SR 235.11).

Wie bereits ausgeführt wurde, befinden sich sowohl der PC „Biometrie“ als auch der Sekretariats-PC in von aussen zugänglichen und nur durch ein einfaches Schloss gesicherten Räumen des Clubhauses. Zum PC „Biometrie“ haben 5 bis 6 Personen Zutritt, wobei 2 bis 3 davon vom TC XX nicht näher benannt werden konnten. Zum Sekretariats-PC haben ausserhalb der Öffnungszeiten 11 Personen Zutritt, während der Öffnungszeiten kann der Raum von jedermann betreten werden, wobei der PC dann i.d.R. nicht unbeaufsichtigt ist und der Zugang auf die dort gespeicherten Daten passwortgeschützt ist.

Der PC „Biometrie“ und der Sekretariats-PC sind via WIFI miteinander und mit dem Internet verbunden. Das WIFI ist durch das Protokoll WPA (seit März 2010 WPA2) gesichert. Den Mitgliedern wird auf Wunsch das WIFI-Passwort bekannt gegeben, damit diese während ihres Aufenthalts auf dem Clubgelände via WIFI aufs Internet zugreifen können.

Vom Sekretariats-PC aus kann via eine versteckte Partition auf dem PC „Biometrie“ auf die dort gespeicherten Templates zugegriffen werden.

5.8.2 Beurteilung aus Sicht des EDÖB

Der EDÖB beurteilt die physische Sicherung des PC „Biometrie“ und des Sekretariats-PC als ungenügend. Die Türen samt Schlössern können ohne grösseren Aufwand aufgebrochen werden. Damit sind die beiden PCs nicht in dem Masse physisch gesichert, wie dies vorliegend angezeigt wäre, und ein „Datendiebstahl“ oder gar die Entwendung der ganzen PCs wäre leicht möglich. Dies muss aus Sicht des EDÖB dringend verbessert werden, insbesondere in Anbetracht der Sensibilität der auf den PCs gespeicherten Daten.

Der Zugang zu den PCs „Biometrie“ und dem Sekretariats-PC ist zuwenig klar geregelt. Es muss daher für beide Rechner sowie eine Liste erstellt werden, in der die Zutrittsberechtigten klar definiert werden, wobei die Anzahl der Berechtigten auf ein Minimum reduziert werden muss. Dasselbe gilt für die Zugangsberechtigten für die genannten Rechner (Benutzerkonten) und den Zutritt und den Zugang zu Backups und dergleichen.

Der EDÖB erachtet es zudem als problematisch, dass die Übertragung (biometrischer) Persondaten via WIFI erfolgt, welches nicht denselben Sicherheitsstandard bieten kann wie eine Übermittlung via Kabel, und dieses WIFI auch von den Mitgliedern für den Zugang zum Internet genutzt werden kann. Er schlägt daher vor, dass die Verbindung zwischen dem PC „Biometrie“ und dem Sekretariats-PC sowie die Verbindungen zum Router/Modem mittels Kabel erfolgen und das WIFI nur noch für den Internetzugang der Mitglieder genutzt wird. Damit erfolgt die Übertragung der (biometrischen) Personendaten sicherer und getrennt vom Internetverkehr der Mitglieder.

5.9 Auskunftsrecht

5.9.1 Ausgangslage

Gemäss Art. 8 DSG kann jede Person vom Inhaber der Datensammlung Auskunft darüber verlangen, ob Daten über sie bearbeitet werden.

Beim TC XX können die Mitglieder sich jederzeit an den Präsidenten wenden, um Einsicht in die Template-Datenbank zu erhalten. Der Präsident will dieses Auskunftsrecht auf sämtliche Mitgliederdaten ausweiten.

5.9.2 Beurteilung aus Sicht des EDÖB

Mit der Ausweitung des Auskunftsrechts auf sämtliche Mitgliederdaten sind die diesbezüglichen Rechte der Mitglieder gewahrt. Der EDÖB hat dazu keine weiteren Bemerkungen.

6. Ergebnisse

Aufgrund der Auswertung der eingereichten Unterlagen und Dokumente sowie gestützt auf die durchgeführte Kontrolle vom 11. Februar 2010 gemäss Art. 29 DSG gelangt der EDÖB zu einer kritischen Gesamtbeurteilung des biometrischen Reservationssystems. Die Datenschutzkontrolle hat gezeigt, dass die seit der Einführung des biometrischen Reservationssystems erfolgte Bearbeitung von Personendaten durch den TC XX nicht in allen Aspekten datenschutzkonform verläuft. Der EDÖB ist in seiner Kontrolle auf Sachverhalte gestossen, welche aus datenschutzrechtlicher Sicht einer Verbesserung resp. Änderung bedürfen.

Ausgehend von diesem Gesamtbild erlässt der EDÖB zuhanden des TC XX seine Gesamtbeurteilung in folgender Form:

- Feststellungen und/oder
- Empfehlungen im Sinne des Art. 29 Abs. 3 DSG.

6.1 Biometrische Daten als Personendaten

Bei biometrischen Daten der Fingerabdrücke handelt es sich um Personendaten gemäss Art- 3 lit. a DSG. Biometrische Daten in Form von Rohdaten oder Templates machen eine Person identifizierbar resp. bestimmbar. Ihre Erhebung hinterlässt in der Regel – insbesondere bei der Erhebung von Fingerabdrücken – (Daten-)Spuren. Die Erhebung von Rohdaten oder Templates ist somit geeignet, ein Bewegungsprofil der betroffenen Person zu erstellen. Gestützt auf diese Tatsache besteht bei der Erhebung biometrischer Daten für die betroffene Person ein hohes Potenzial für Persönlichkeitsverletzungen.

6.2 Zweck der Datenbearbeitung

Jede Bearbeitung von Personendaten stellt einen Eingriff in das Recht auf informationelle Selbstbestimmung gemäss Art. 13 Abs. 2 des Bundesverfassung der Schweizerischen Eidgenossenschaft vom 18. April 1999 (BV; SR 101) dar. Daher bedarf die Bearbeitung einer besonderen Rechtfertigung. Praktikabilitätserwägungen oder allgemeine Bedienerfreundlichkeit stellen grundsätzlich keine ausreichende Rechtfertigung für die Bearbeitung biometrischer Daten dar.

Gemäss Auskunft des TC XX geht es bei der Erfassung der biometrischen Daten ausschliesslich um die automatisierte Missbrauchsbekämpfung bei der Reservation und der Nutzung von Tennisplätzen. Der Vorteil für den TC XX läge darin, dass keine persönliche Prüfung der Identität der Spieler bei der Reservation und der Platznutzung (z.B. durch den Betrieb einer Reception) vorgenommen werden müsse. Das neue biometrische Reservationssystem ersetzt das veraltete Reservationssystem mittels PIN, bei dem es zu zahlreichen Missbräuchen gekommen sei. Gemäss Angaben des TC XX hat sich die Zahl der Mitglieder seit Einführung des neuen Systems stark erhöht, während die Plätze in derselben Zeit weniger genutzt wurden, was mit der fehlenden Missbrauchsmöglichkeit in Zusammenhang stehe. Der Vorteil für die Mitglieder besteht darin, dass sie keine Mitgliederkarte oder dergleichen mit sich führen müssen. Zudem sind, wie unter dem bisherigen System, Reservationen via Internet möglich.

Das neue biometrische Reservationssystem des TC XX verfolgt nachvollziehbare Zwecke. Dennoch möchte der EDÖB seine ernsthaften Bedenken bezüglich der Frage äussern, ob es nicht andere Alternativen zur Missbrauchsvermeidung geben würde, welche weniger stark in die Persönlichkeitsrechte der Betroffenen eingreifen würden (vgl. dazu auch das Ergebnis des Verhältnismässigkeitsprüfung unter Ziffer 6.5.1.1, Empfehlung Nr. 2).

6.3 Rechtmässigkeit der Datenbeschaffung / Einwilligung der Betroffenen

Die Bearbeitung biometrischer Daten bedarf eines Rechtfertigungsgrundes (Art. 12 und 13 DSG). Als Rechtfertigungsgrund kommt im vorliegenden Fall die Einwilligung der Betroffenen in Frage. Das biometrische Reservationssystem wurde nach einem entsprechenden GV-Beschluss eingeführt. Denjenigen Mitgliedern, die mit dem System nicht einverstanden waren, wurde eine valable Alternative geboten, so dass davon ausgegangen werden kann, dass diejenigen Mitglieder, welche das biometrische System nutzen, ihre Einwilligung geben. Aus Sicht des EDÖB fehlen jedoch wichtige Informationen, wie insbesondere die Bearbeitungsmodalitäten und der explizite Hinweis auf die Alternative ohne Einsatz biometrischer Daten.

Aus Sicht des EDÖB fehlen vorliegend wichtige Informationen, insbesondere über die Bearbeitungsmodalitäten, die explizite Erwähnung des Bestehens einer Alternative ohne Verwendung biometrischer Daten und die Tatsache, dass der Familienname im Reservationssystem angezeigt wird (vgl. Ziffer 6.5.1.2 nachstehend).

Emfpehlung Nr. 1:

a) Der TC XX erarbeitet bis zum 31.12.2010 ein Informationenblatt, welches die Modalitäten der Bearbeitung der biometrischen Daten, die Möglichkeit einer Alternative ohne Verwendung biometrischer Daten, wie auch die Tatsache, dass der Familiennamen der Mitglieder im Reservationssystem angezeigt wird, wenn nicht von der Möglichkeit der Pseudonymisierung Gebrauch gemacht wird, Auskunft gibt. Aufgeführt werden müssen die Hauptpunkte der Datenbearbeitung, wie z.B. die Einzelheiten Datenbearbeitung, wo und wie lange die Daten gespeichert werden, insbesondere, was mit den Templates und den Transaktionsdaten

geschieht, wer Zugriff auf die Daten hat und an wen sie, wenn überhaupt, weitergegeben werden etc.

b) Dieses Informationsblatt muss von einem Mitglied des Vorstands unterzeichnet und mit einer Versionenkontrolle versehen werden.

c) Dieses Informationsblatt ist umgehend allen bestehenden Mitgliedern auszuhändigen und jedem Neumitglied vor dem Enrolement abzugeben. Dem Neumitglied ist genügend Zeit zu Verfügung zu stellen, das Informationsblatt vor dem Enrolement durchzulesen.

6.4 Bearbeitung nach Treu und Glauben / Transparenz

Das Enrolement erfolgt ausschliesslich unter Mitwirkung des Mitglieds. Ohne sein Zutun können beim TC XX keine biometrischen Daten erhoben werden. Die Datenbearbeitung erfolgt in diesem Punkt transparent und ist für die Betroffenen erkennbar.

Jedoch muss bemängelt werden, dass die Information der Mitglieder hinsichtlich der Bearbeitungsmodalitäten ungenügend ist. Die Mitglieder wurden zwar anlässlich der GV, durch die Gebrauchsanweisung sowie mündlich durch den Vereinspräsidenten informiert. Für eine möglichst transparente Datenbearbeitung sollte neben den mündlichen Informationen durch den Vereinspräsidenten und der rein über die richtige Handhabung des Systems informierende Gebrauchsanweisung auch ein Infoblatt abgegeben werden, auf dem umschrieben ist, was mit den Personendaten geschieht und dass eine Alternative ohne Erhebung biometrischer Daten besteht (vgl. EmpfehlungNr. 1).

6.5 Verhältnismässigkeit der Datenbearbeitung

6.5.1 Verhältnismässigkeit in inhaltlicher Hinsicht

6.5.1.1 Zentrale Speicherung biometrischer Daten

Der Einsatz biometrischer Verfahren im Privatbereich stellt, je nach Ausgestaltung im konkreten Einzelfall, einen mehr oder weniger intensiven Eingriff in die Persönlichkeitsrechte der Betroffenen dar. Grundsätzlich sind daher vor dem Einsatz biometrischer Verfahren immer auch andere geeignete Massnahmen zu überprüfen, welche weniger in die Grundrechte der Betroffenen eingreifen und mit denen der angestrebte Zweck ebenfalls erreicht werden kann. Des Weitere muss bei der Auswahl und Ausgestaltung des biometrischen Verfahrens darauf geachtet werden, ein möglichst datensparsames System auszuwählen, das in einem vernünftigen Verhältnis zum angestrebten Zweck steht.

Im vorliegenden Fall geht es um ein Reservationssystem für Tennisplätze. Die Biometrie wird hier zur Verifizierung der Mitglieder eingesetzt. Datensparsamkeit erreicht man, indem nur die unbedingt zur Verifizierung notwendigen biometrischen Daten erhoben werden.

Für den Einsatz des neuen Reservationssystems werden aus den Fingerabdrücken der Mitglieder Templates generiert und diese zentral in einer Datenbank abgelegt. Rohdaten (d.h. das Originalbild

des Fingerabdrucks) werden keine erhoben. Die Beschränkung der Speicherung biometrischer Daten auf Templates, wie dies vom TC XX vollzogen wird, ist unter dem Gesichtspunkt der Datensparsamkeit verhältnismässig und zu begrüssen.

Biometrische Daten sind dauerhaft personengebunden und geeignet, von der betroffenen Person ein Bewegungsprofil zu erstellen. Aus diesem Grund sollten die biometrischen Daten – gerade wenn es um so heikle Bereiche wie Fingerabdrücke geht – im Einflussbereich der betroffenen Person resp. des Nutzers gespeichert werden. Der Grundsatz der inhaltlichen Verhältnismässigkeit erfordert, dass bei biometrischen Systemen, die auch ohne zentrale Speicherung funktionsfähig sind, die biometrischen Merkmale möglichst nicht in einer zentralen Datenbank gespeichert werden sollten, sondern nur auf einem Medium, das ausschliesslich dem Benutzer zugänglich ist. Insbesondere beim Einsatz der Biometrie für ein Reservationssystem in einer Freizeitanlage muss aus Gründen des Persönlichkeits- und Datenschutzes auf eine zentrale Speicherung verzichtet werden.

Aus dem bisher Gesagten folgt, dass für eine datenschutzkonforme Umsetzung biometrischer Verifizierungssystemen im Freizeitbereich die nachfolgend beschriebenen drei Varianten in Frage kommen. Für den Einsatz biometrischer Charakteristika, die (physische oder digitale) Spuren hinterlassen (z.B. Fingerabdrücke oder Gesichtsfotografien), können nur die Varianten a) und b) durch den Einsatz von individuellen Karten ein genügendes Sicherheitsniveau garantieren. Die Variante c) ohne Karten kann dagegen nur dann eingesetzt werden, wenn biometrische Charakteristika verwendet werden, die keine Spuren hinterlassen (z.B. Fingervenen oder Handumriss).

a) Dezentralisierung (auf Karten)

Wie der EDÖB in seinem Leitfaden zu biometrischen Erkennungssystemen vom September 2009 festhält, wird beim Einsatz von Biometrie im Privatbereich der Persönlichkeitsschutz der Betroffenen am ehesten gewahrt, indem

1. die biometrischen Daten auf einem Sicherheitsmedium, da sich in der alleinigen Kontrolle der betroffenen Person befindet, auslesesicher gespeichert werden;

2. die betroffene Person jeden Zugriff auf die Daten explizit und bewusst freigeben muss; und

4. die Verifizierung der Identität ausschliesslich auf diesem Sicherheitsmedium stattfindet, so dass die biometrischen Daten zu keinem Zeitpunkt die gesicherte Umgebung des Mediums und die Kontrolle der betroffenen Person verlassen (biometrischer Vergleich auf Karte, vgl. Leitfaden S. 13).

b) Pseudodezentralisierung (mit Karten)

Ein annährend gleich hohes Niveau betreffend den Persönlichkeitsschutz kann mit der Pseudodezentralisierung erreicht werden. Diese Lösung wurde denn auch vom Bundesverwaltungsgericht in seinem Urteil vom 4 August 2009 in Sachen KSS (A-3908/2008) skizziert. Im Unterscheid zur richtigen Dezentralisierung werden die biometrischen Daten zentral gespeichert, der logische Zugang zu diesen Daten ist aber einzig durch den Einsatz eines Zuordnungscodes möglich, der auf einer Karte gespeichert wird, die sich ausschliesslich im Besitz der betroffenen Person befindet. Im Einzelnen bedeutet dies Folgendes:

4. Die biometrischen Daten werden als verschlüsselte Templates zentral gespeichert (und nicht als Rohdaten, z.B. als Fingerabdruckbild oder als Fotografie);

5. die Templates sind so gespeichert, dass der Inhaber der Datensammlung keinen Bezug zu einer bestimmten oder bestimmbaren Person herstellen kann. Statistische Daten oder weitere Angaben (z.B. Zeitstempel) können in Verbindung mit den biometrischen Daten so lange gespeichert werden, wie durch sie keine Identifizierung der fraglichen Person möglich wird;
6. die Verbindung zwischen dem Template und der betroffenen Person kann einzig durch eine explizite und bewusste Freigabe durch die Verwendung der persönlichen Karte hergestellt werden.

c) Zentralisierung (ohne Karten)

Wird ein Verifizierungssystem ohne die Verwendung persönlicher Karten im Freizeitbereich gewünscht, so ist dies nur mit einer Zentralisierung der biometrischen Daten möglich. Da die zentrale Speicherung biometrischer Daten für den Verifizierungsprozess normalerweise nicht notwendig wäre, muss das System angepasst werden, damit es nicht gegen den Grundsatz der Verhältnismässigkeit verstösst:

5. Es dürfen nur biometrische Charakteristika verwendet werden, die keine (physischen oder digitalen) Spuren hinterlassen;
6. die biometrischen Daten werden als verschlüsselte Templates zentral gespeichert (und nicht als Rohdaten, z.B. als Fotografie);
7. die Templates sind so gespeichert, dass der Inhaber der Datensammlung keinen Bezug zu einer bestimmten oder bestimmbaren Person herstellen kann. Statistische Daten oder weitere Angaben (z.B. Zeitstempel) können in Verbindung mit den biometrischen Daten so lange gespeichert werden, wie durch sie keine Identifizierung der fraglichen Person möglich wird;
8. die Verbindung zwischen dem Template und der betroffenen Person wird einzig in flüchtiger Weise durch das Erkennungssystem hergestellt, mit dem Ziel, die Zugehörigkeit einer Person zum Kreis der Berechtigten festzustellen. Alle weiteren Operationen (Identifizierung der Person, Bestätigung der Reservation…) werden davon getrennt und ohne Verwendung biometrischer Charakteristika durchgeführt.

Empfehlung Nr. 2:

a) In Zukunft, jedoch spätestens ab 30.06.2011verzichtet der TC XX auf die zentrale Speicherung der biometrischen Daten in der heute praktizierten Form von Templates der Fingerabdrücke.
b) Wenn der TC XX an der Verwendung biometrischer Daten für die Verifizierung seiner Mitglieder im Reservationssystem festhalten will, so
- sind diese biometrischen Daten – auch diejenigen, welche bereits zentral erfasst wurden – auf einem Datenträger, welcher in der Benutzersphäre und unter Kontrolle der betroffenen Personen verbleibt (Minimum biometrischer Vergleich auf Karte, vgl. S. 13 des Leitfadens), zu speichern; oder
- sind diese biometrischen Daten zentralisiert als verschlüsselte Templates zu speichern, ohne jegliche Verbindung zu anderen Personendaten, so dass der Bezug zu einer bestimmten oder bestimmbaren Person einzig durch eine bewusste und explizite Freigabe durch die betroffene Person durch die Verwendung einer persönlichen Karte hergestellt werden kann; oder

- sind nur biometrische Charakteristika zu verwenden, die keinerlei (physische oder digitale) Spuren hinterlasse. Die biometrischen Daten sind dabei als verschlüsselte Templates ohne dauerhaften Bezug zu anderen Personendaten zu speichern.

6.5.1.2 Veröffentlichung der Reservationsdaten im Internet

Eine Veröffentlichung von Personendaten im Internet ist stets mit besonderen Risiken Verbunden. Aus diesem Grund ist der Zweck der Veröffentlichung vorgängig sorgfältig zu prüfen und die Veröffentlichung auf die für den Zweck unbedingt erforderlichen Daten zu beschränken. Wenn immer möglich, ist der Zugang beispielsweise durch einen Passwortschutz auf diejenigen Personen zu beschränken, die den Zugang zur Zweckerreichung benötigen.

Vorliegend dient die Veröffentlichung im Internet dem Zweck, den Clubmitgliedern eine Online-Reservation zu ermöglichen. Dieser Zweck kann ohne Einschränkungen auch erreicht werden, wenn der Zugang auf die Clubmitglieder beschränkt wird. Auch die technische Umsetzung der Zugangsbeschränkung dürfte wenig Probleme bereiten, wird doch für die Tätigung einer Reservation bereits jetzt ein Login benötigt. Die Beschränkung kann mit Benutzeridentifikation und Passwort erreicht werden. Für die vertrauliche Übertragung stehen heute erprobte Verschlüsselungssysteme, wie beispielsweise das SSL-Protokoll (Secure Socket Layer), zur Verfügung. Die Schlüssellänge sollte dabei mindestens 128 Bit betragen.

Empfehlung Nr. 3:

Der Zugang zum online- Reservationssystem ist bis zum 31.12.2010 auf die Mitglieder zu beschränken und daher mit einem Passwortschutz zu versehen Die Übertragung der Daten hat verschlüsselt (nach aktuellem Stand der Technik) zu erfolgen.

Für die Online-Reservation ist die Namensnennung zudem nicht notwendig. Es genügt, wenn erkennbar ist, ob ein Platz frei oder besetzt ist. Der Mehrwert, durch die Namensnennung Spielpartner finden zu können, muss auf freiwilliger Basis geschehen. Wird in den Grundeinstellungen jedoch der richtige Name angezeigt, besteht die Gefahr, dass viele Mitglieder aus Unwissenheit oder Bequemlichkeit den richtigen Namen stehen lassen, ohne dass sie mit einer Veröffentlichung ihres Namens im Reservationssystem tatsächlich einverstanden sind. Aus diesem Grund müssen die Mitglieder auf diesen Umstand sowie die Möglichkeit der Pseudonymisierung aufmerksam gemacht werden (vgl. Empfehlung Nr. 1a).

6.5.2 Verhältnismässigkeit in zeitlicher Hinsicht

Beim TC XX werden zurzeit keine regelmässigen Datenlöschungen durchgeführt. Die Daten im Reservationssystem werden aus Platzgründen alle 2 bis 3 Jahre gelöscht, die übrigen Daten werden bis

jetzt gar nicht gelöscht. Es sind nirgends Löschfristen für die Daten festgehalten. Dies ist in zeitlicher Hinsicht unverhältnismässig.

Empfehlung Nr. 4:

Der TC XX hat für sämtliche Personendaten Löschfristen einzuführen, inkl. für die Backupdaten. Daher hat der TC XX dem EDÖB einen Vorschlag für die Regelung der Löschfristen einzureichen und diese bis zum 31.12.2010 umzusetzen und die technischen Anpassungen vorzunehmen.

6.6 Zweckbindung der Datenbearbeitung

Durch die derzeit praktizierte zentrale Speicherung der Templates kann eine Zweckentfremdung (d.h. eine über die Missbrauchsverhinderung hinausgehende Datenbearbeitung) dieser heiklen Daten nicht gänzlich ausgeschlossen werden. Eine Zweckentfremdung im Sinne einer Verknüpfung mit anderen Datensammlungen oder einer Weitergabe an aussenstehende Dritte wäre möglich. Da eine Änderung des Bearbeitungszwecks der biometrischen Daten von den Betroffenen durch die zentrale Speicherung der Daten nicht kontrollierbar ist, sind technische Lösungen vorzuziehen, welche die Zweckbindung ausreichend gewährleisten. Unter dem Aspekt der Zweckbindung ist die dezentrale Speicherung der biometrischen Daten auf einem sich in der Nutzersphäre der Betroffenen befindenden Datenträger und nicht, wie vorliegend, eine zentrale Speicherung der Daten vorzusehen. Es kann an dieser Stelle auf die Empfehlung Nr. 2 verwiesen werden.

6.7 Datenrichtigkeit (Zuverlässigkeit, Anwendbarkeit)

Aus Datenschutzgründen sollte die False Acceptance Rate (FAR) vermindert werden, ohne aber die False Rejection Rate (FRR) zu stark zu beeinträchtigen. Gleichzeitig sollte ein optimaler Schwellenwert gewählt werden. Jedes biometrische System weist einen gewissen Prozentsatz an FAR auf. Die Verifizierung kann infolgedessen nicht zu 100 % zuverlässig erfolgen.

Für Personen, denen biometrische Merkmale fehlen oder deren biometrische Merkmale z.B. aufgrund des Alters, Narben oder sonstiger Gründe nicht oder nur schlecht eingelesen werden können, muss eine äquivalente Anwendbarkeit des Erkennungssystems geplant und eingesetzt werden.

Die Anzahl der vom TC XX verwendeten Minutien pro Template liegt innerhalb der Bandbreite des Zulässigen. Diejenigen Personen, die das biometrische System aufgrund fehlender oder für das System nicht genügender biometrischer Merkmale nicht nutzen können, können ihre Reservationen mittels PIN vornehmen und haben damit eine äquivalente Alternative. Abgesehen davon, dass der EDÖB der Ansicht ist, die zentrale Speicherung sei unverhältnismässig und daher eine dezentrale Speicherung auf einem Speichermedium in der Nutzersphäre der betroffenen Person einzuführen (vgl. Empfehlung Nr. 2), hat der EDÖB zur Datenrichtigkeit keine Bemerkungen.

6.8 Datensicherheit

Die Datensicherheit ist beim TC XX, gerade in Anbetracht der Sensibilität der verwendeten Personendaten, zu wenig gewährleistet. Die Rechner müssen physisch besser gesichert werden, um die Wahrscheinlichkeit eines Diebstahls zu verringern. Zudem müssen die Zugangs- und Zutrittsberechtigung genauer geregelt und reduziert werden, um auch hier die Risiken zu senken. Eine Umgestaltung des Netzwerks sollte ausserdem die Sicherheit der Datenübertragung erhöhen.

Empfehlung Nr. 5:

Um die zurzeit ungenügende Datensicherheit zu erhöhen, insbesondere auch in Anbetracht der Sensibilität der fraglichen Daten, hat der TC XX bis zum 31.12.2010
a die physische Sicherung des PC „Biometrie" und des Sekretariats-PC durch geeignete Massnahmen verbessert.
b. die Zutrittsberechtigungen zum PC „Biometrie" und zum Sekretariats-PC regelt, wobei die Anzahl der Zutrittsberechtigten auf ein Minimum zu reduzieren ist.
c. die Zugangsberechtigungen zu sämtlichen vom TC XX gespeicherten Personendaten, inkl. Backups, regelt, wobei die Anzahl der Zutrittsberechtigten auf ein Minimum zu reduzieren ist.
d. die kabellose Datenübertragung zwischen dem PC „Biometrie" und dem Sekretariats-PC und zwischen dem Sekretariats-PC und dem Modem/Router durch eine Übermittlung via Kabel ersetzt.

6.9 Auskunftsrecht

Die Mitglieder haben jederzeit die Möglichkeit, ihre persönlichen Daten einzusehen und aktualisieren zu lassen. Das Auskunftsrecht der Mitglieder wird gewährleistet. Der EDÖB hat dazu keine Bemerkungen.

7. Schlussfolgerungen

7.1 Bezüglich der Kontrolle der Erhebung biometrischer Daten

Zum Zweck der Eindämmung von Missbräuchen bei der Reservation und Nutzung der Tennisplätze hat der TC XX im Sommer 2009 ein neues Reservationssystem eingeführt, bei dem neben der Personalien der Mitglieder auch biometrische Daten in Form von Templates der Fingerabdrücke erhoben und gespeichert werden.

Die durchgeführte Datenschutzkontrolle konnte dem EDÖB einen vertieften Einblick in das neue Reservationssystem liefern. Die vom TC XX zu Verfügung gestellten Unterlagen und Dokumente haben es dem EDÖB erlaubt, die damit verbundene Datenbearbeitung auf die Einhaltung der Datenschutzbestimmungen zu überprüfen.

Der EDÖB gelangt zu einer kritischen Gesamtbeurteilung des biometrischen Reservationssystems. Die Datenschutzkontrolle hat gezeigt, dass die seit der Einführung des neuen biometrischen Reservationssystems erfolgte Bearbeitung von Personendaten durch den TC XX nicht in allen Aspekten datenschutzkonform verläuft. Wo Änderungen vorgenommen werden müssen oder wo Verbesserungsbedarf besteht, hat dies der EDÖB mit Begründung erläutert.

7.2 Verfahren und weiteres Vorgehen

Der vorliegende Kontrollbericht enthält eine Reihe von Feststellungen sowie Empfehlungen, welche vom EDÖB auf Basis der durchgeführten Kontrolle verfasst wurden. Der vorliegende Kontrollbericht wird dem TC XX zur Kenntnisnahme zugestellt. Innert Frist von 30 Tagen nach Zustellung hat der TC XX dem EDÖB mitzuteilen, ob seitens des TC XX irgendwelche Bemerkungen dazu vorliegen und ob der TC XX die Empfehlungen akzeptiert. Falls die Empfehlungen akzeptiert werden, lässt der TC XX innert derselben Frist dem EDÖB einen Vorschlag für die Regelung der Löschristen zukommen (vgl. Empfehlung Nr. 4). Für den Fall, dass der TC XX die Empfehlungen nicht akzeptiert oder umsetzt, kann der EDÖB die Angelegenheit dem Bundesverwaltungsgericht zum Entscheid vorlegen (Art- 29 Abs. 4 DSG).

In Anbetracht der Sensibilität der bearbeiteten Daten und der Reaktionen einiger Clubmitglieder ist die Notwendigkeit der Kontrolle des neuen Reservationssystems des TC XX in Bezug auf den Datenschutz offensichtlich. Die Feststellungen und Empfehlungen des EDÖB zeigen nun die Richtung auf, die andere private Betreiber von Freizeitanlagen bei der Umsetzung biometrischer Systeme einzuschlagen haben.

Aus besagten Gründen besteht ein grundsätzliches Interesse daran, die Öffentlichkeit für diese Art der Datenerhebung zu sensibilisieren und sie insbesondere über die erfolgte Datenschutzkontrolle beim TC XX und die diesbezüglichen Ergebnisse zu informieren. Gestützt auf Art. 30 Abs. 2 DSG wird der EDÖB daher den vorliegenden Kontrollbericht in einer angepassten und anonymisierten Version publizieren. Selbstverständlich erfolgt die Publikation unter dem Vorbehalt, dass keine aus Sicht des TC XX (und dem Systemlieferanten) vertraulichen Daten, welche Geschäftsgeheimnisse offenbaren oder die Konkurrenzfähigkeit beeinflussen könnten, bekannt gegeben werden. Der TC XX wird daher aufgefordert, den Schlussbericht auf solche vertraulichen Inhalte hin zu überprüfen und dem EDÖB mit Frist von 30 Tagen entsprechend schriftliche Rückmeldung zu erstatten.