Datenschutzrecht und Sport

BRUNO BAERISWYL

Inhaltsverzeichnis

1. Einleitung

Bisher haben datenschutzrechtliche Fragestellungen im Bereich des Sportrechts noch wenig Anlass zu eingehenden Betrachtungen gegeben. Die vorliegenden Ausführungen[1] haben deshalb zum Ziel, eine erste Auslegeordnung datenschutzrechtlicher Problemstellungen zu erstellen. Dabei sind einerseits die aktuellen datenschutzrechtlichen Entwicklungen zu betrachten und andererseits die möglichen Auswirkungen auf die einschlägigen Sachverhalte und die verschiedenen Akteure im Bereich des Sports. Dazu gehören die Sportlerinnen und Sportler, die Zuschauerinnen und Zuschauer, Verbände und Vereine sowie Organisatoren von Sportveranstaltungen.

Datenbearbeitungen über Sportlerinnen und Sportler finden in den unterschiedlichsten Bereichen statt und gewinnen mit der Zunahme von medizinischen Untersuchungen an Sensibilität. Was mit all diesen medizinischen Daten geschieht oder geschehen darf, ist in vielen Fällen kaum geregelt und deshalb für die betroffenen Personen wenig transparent.

Zuschauerinnen und Zuschauer von Sportveranstaltungen haben sich zunehmenden Kontroll- und Überwachungsmassnahmen zu unterziehen. Soweit keine gesetzlichen Grundlagen bestehen, werden von ihnen Einwilligungserklärungen verlangt. Dabei stellen sich hier Fragen, wieweit aufgrund solcher Einwilligungserklärungen die persönliche Freiheit eingeschränkt werden kann und darf.

Verbände, Vereine und Organisatoren von Sportveranstaltungen bearbeiten immer mehr Daten über ihre Mitglieder oder teilnehmende Sportlerinnen und Sportler. Diese Daten werden vielfach publiziert und stehen beispielsweise im Internet einer unbeschränkten Personenzahl und auf unbestimmte Zeit zur Verfügung. Die damit verbundenen Risiken für die betroffenen Personen werden vielfach ausser Acht gelassen.

Die folgenden Betrachtungen beschränken sich auf eine Darstellung der datenschutzrechtlichen Ausgangslage und der mit dieser verbundenen technologischen Entwicklung. Anhand von beispielhaften Sachverhalten werden datenschutzrechtliche Fragestellungen insbesondere in Bezug auf die Zuschauerinnen und Zuschauer von Sportveranstaltungen aufgezeigt. Ein kurzer Blick wird auch auf die Vereine im Amateursport geworfen,

[1] Grundlage ist das am 24. Mai 2005 an der Tagung „Sport und Recht“ gehaltene Referat. Für die Unterstützung bei der Ausarbeitung dieses Beitrages danke ich lic.iur. SABIN BACHMANN.

die ebenfalls umfassende Datenbearbeitungen vornehmen. Weitere Themenbereiche werden in diesem Rahmen nicht bearbeitet.

2. Ausgangslage

Der Schutz der Persönlichkeitsrechte kennt in unserer Rechtsordnung eine lange Tradition[2]. Im Rahmen von sportrechtlichen Betrachtungen waren die Persönlichkeitsrechte deshalb schon immer zu beachten. Grundsätzlich liegt deshalb heute mit dem Datenschutzrecht keine neue Ausgangslage vor. Doch auch der Bereich des Sports ist von der allgemeinen Entwicklung unserer Gesellschaft zur Informations- und Kommunikationsgesellschaft betroffen. Informationen in unterschiedlichsten Ausprägungen spielen eine immer gewichtigere Rolle. Sie werden mehr und mehr zu einer eigenständigen Ressource, und die Technologie ermöglicht heute die Speicherung beliebiger Mengen von Daten, ihre Kombination und ihre Verbreitung über globale Netzwerke. Diese Fortschritte in der Informationstechnologie bringen neue Risiken für Eingriffe in die Persönlichkeitsrechte der betroffenen Personen: Einerseits lassen sich die Daten nahezu beliebig verknüpfen, und ein Personenbezug ist ohne weiteres herstellbar, andererseits geht für die betroffenen Personen die Transparenz über die über sie bearbeiteten Daten verloren. Damit erhält das Recht auf informationelle Selbstbestimmung, der Datenschutz, eine immer zentralere Bedeutung.

3. Entwicklung des Datenschutzrechts

Bereits Art. 8 EMRK sieht den Schutz der Privatsphäre vor, und in Art. 10 Abs. 2 und Art. 13 Abs. 2 der Bundesverfassung wird der Schutz der Privatheit im Rahmen der persönlichen Freiheit und als Schutz vor Missbrauch von persönlichen Daten gewährleistet. Das Datenschutzgesetz[3] beinhaltet die Konkretisierung dieser Bestimmungen in Bezug auf das Bearbeiten[4] von personenbezogenen Daten[5]. Obwohl technikneutral formu-

---

2 Vgl. Art. 28 ff. ZGB, Art. 8 EMRK.

3 Bundesgesetz über den Datenschutz (DSG) vom 19. Juni 1992. Das DSG regelt die Datenbearbeitungen durch private Personen und die Bundesverwaltung; soweit öffentlich-rechtliche Stellen von Kantonen und Gemeinden Daten bearbeiten, gelangen die entsprechenden kantonalen Datenschutzgesetze zur Anwendung.

4 Mit Bearbeiten ist jeglicher Umgang mit Personendaten gemeint: Art. 3 lit. e DSG.

liert, ist das DSG als Reaktion auf die Entwicklung der Informationstechnologie der 1960er und 1970er Jahre zu verstehen. Die informationelle Selbstbestimmung[6] soll auch bei der elektronischen Datenbearbeitung gewährleistet werden.

Es ist heute indessen nicht zu übersehen, dass die Konzeption der Datenschutzgesetzgebung angesichts der neuen gesellschaftlichen und technologischen Entwicklungen den Schutz der Privatheit nicht mehr risikoadäquat gewährleisten kann. Auf der einen Seite die Informationsflut und der eigentliche „Datenhunger", auf der anderen Seite die Möglichkeiten des „Ubiquitous Computing"[7] als augenfällige Zeichen der Informations- und Kommunikationsgesellschaft stellen den Schutz der Privatheit vor neue Herausforderungen. Die Frage der Wirksamkeit der Datenschutzgesetzgebung drängt sich deshalb immer mehr in den Vordergrund. Bemühungen um eine Revision des Datenschutzgesetzes[8] sind im Gange, doch, ob sie die festgestellten Defizite der ursprünglichen Datenschutzkonzeption beheben können, ist fraglich.

Neue Ansätze gehen heute in Richtung eines mehrdimensionalen Datenschutzes[9]. Das Recht kann den Schutz der Privatheit angesichts des Rhythmus des technologischen Fortschritts allein nicht mehr garantieren. Als Technikfolgenrecht soll es daher vorwiegend die Aufgabe eines Steuerungselements übernehmen. Daneben muss der datenschutzfreundlichen Technikgestaltung eine zentrale Bedeutung zukommen. Nur wenn die Technologie letztendlich auch so in Einsatz kommt, dass sie möglichst restriktiv mit personenbezogenen Daten umgeht, lassen sich in der Praxis unverhältnismässige Eingriffe in die Persönlichkeitsrechte vermeiden. Als weitere Elemente eines wirkungsorientierten Datenschutzes sind Selbstregulierungsmechanismen durch entsprechende Anreizsysteme zu fördern

5 Personenbezogene Daten oder Personendaten sind alle Angaben, die sich auf eine bestimmte oder bestimmbare Person beziehen: Art. 3 lit. a DSG.

6 Der Begriff der informationellen Selbstbestimmung, den das deutsche Bundesverfassungsgericht in Konkretisierung des Rechts auf Datenschutz erstmals verwendete (BverGe 65,43 in: EuGRZ 1983, 577 ff.), ist heute auch in der Schweiz gebräuchlich (BGE 120 II 118; 122 I 153; 127 III 481).

7 Siehe MATTERN; LANGHEINRICH/MATTERN.

8 Siehe BOTSCHAFT 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.

9 Siehe zu dieser Diskussion die Beiträge in: BAERISWYL/RUDIN.

und Nutzerinnen und Nutzer von neuen Informationstechnologien in Bezug auf Risiken respektive Risikovermeidung zu schulen.

In diesem Umfeld sind auch die Zunahme der Datenbearbeitungen im Bereich des Sports und der Einsatz moderner Informations- und Kommunikationstechnologien zu betrachten. Die Gewährleistung des Rechts auf informationelle Selbstbestimmung ist deshalb auch eine Herausforderung im Bereich des Sports.

4. Datenschutzrechtliche Prinzipien

Das Recht auf informationelle Selbstbestimmung hat sich in den datenschutzrechtlichen Prinzipien konkretisiert. Sie bilden die Grundlage der Datenschutzgesetze und können als Rahmenbedingungen für das Bearbeiten von personenbezogenen Daten bezeichnet werden. Zum Kern gehören die Prinzipien der Rechtmässigkeit, der Verhältnismässigkeit, der Zweckbindung, der Integrität und der Sicherheit.

4.1 Rechtmässigkeit

Die Bearbeitung von personenbezogenen Informationen muss rechtmässig sein[10]. Sie hat nach Treu und Glauben zu erfolgen und darf die Persönlichkeit der betroffenen Personen nicht widerrechtlich verletzen. Art. 12 und 13 DSG listen eine Reihe von Rechtfertigungsgründen auf, die eine Datenbearbeitung als rechtmässig legitimieren. Die Frage von Treu und Glauben stellt sich beim Einsatz von neuen Informationstechnologien, bei umfassenden Überwachungs- und Kontrollmassnahmen in Bezug auf die Zuschauerinnen und Zuschauer insbesondere betreffend die Einwilligungserklärungen und die Transparenz der dadurch autorisierten Datenbearbeitungen.

4.2 Verhältnismässigkeit

Personendaten dürfen bearbeitet werden, soweit sie für eine bestimmte Aufgabe geeignet und erforderlich sind[11]. Dieser Grundsatz, der dem öf-

[10] Art. 4 i.V.m. Art. 12 DSG.
[11] Art. 4 Abs. 2 DSG.

fentlichen Recht entnommen ist, will in diesem Zusammenhang insbesondere eine Datenbearbeitung auf Vorrat verhindern.

Das Verhältnismässigkeitsprinzip ist auch Technologie bezogen auszulegen. In diesem Sinne sind Grundsätze der Datenvermeidung und der Datensparsamkeit[12] bei technischen Einrichtungen umzusetzen. Soweit möglich, ist auf das Bearbeiten von personenbezogenen Informationen zu verzichten. Überwachungsmassnahmen sind demnach so zu gestalten, dass eine personenbezogene Auswertung der Daten nur bei konkreten Vorfällen ermöglicht wird.

4.3 Zweckbindung

Die Zweckbindung besagt, dass Daten nur zu einem vorher bestimmten Zweck bearbeitet werden dürfen[13]. Zweckänderungen sind danach bei Vorliegen eines Rechtfertigungsgrundes möglich. Insbesondere wird wiederum eine Einwilligung vorausgesetzt, damit Daten, die beim Abschluss eines Zuschauervertrages bearbeitet werden, für Marketingzwecke Verwendung finden oder zu Zwecken von Sicherheitsüberprüfungen registriert werden dürfen.

4.4 Integrität

Die Integrität[14] als weiterer datenschutzrechtlicher Grundsatz verlangt, dass die bearbeiteten Daten richtig und soweit es der Zweck verlangt, auch vollständig sind. Insbesondere das Bearbeiten von so genannten Verdachtsdaten durch private Organisationen hat unter Beachtung dieses Grundsatzes zu erfolgen. Es handelt sich um besonders schützenswerte Personendaten[15], die einen schweren Eingriff in die persönliche Freiheit beinhalten können. Beispiele in diesem Zusammenhang sind das Registrieren von Personen als „gewaltbereit“ oder „Angehöriger der Hooliganszene“.

12 BÄUMLER, 351 ff.
13 Art. 4 Abs. 3 DSG.
14 Art. 5 DSG.
15 Art. 3 lit. c DSG.

4.5 Sicherheit

Personendaten müssen durch angemessene technische und organisatorische Massnahmen gegen unbefugtes Bearbeiten geschützt werden[16]. Damit besteht ein Anspruch der betroffenen Personen gegenüber dem jeweiligen Datenbearbeiter, dass die über sie bearbeiteten Daten nicht missbräuchlich verwendet werden. Diese Anforderungen sind im Umfeld der Informatik eine dauernde Herausforderung und erfordern entsprechende Investitionen in Sicherheitsmassnahmen.

5. Neue Technologien

Auch im Bereich des Sports werden zunehmend neue Technologien eingesetzt, die zusätzliche Risiken für die Persönlichkeitsrechte der betroffenen Personen enthalten. Dem datenschutzkonformen Einsatz neuer Technologien kommt eine besondere Bedeutung zu. Das Datenschutzrecht zeigt sich dabei in seiner eigentlichen Rolle als Technikfolgenrecht. Der Einsatz von RFID-Technologien, der Biometrie, der Videoüberwachung und der automatisierten Gesichtserkennung, die heute im Bereich des Sports zur Anwendung gelangen, sind deshalb unter den Aspekten des Datenschutzes näher zu betrachten.

5.1 Radio Frequency Identifier (RFID)

Radio Frequency Identifier (RFID)[17] sind Chips in Miniaturgrösse, die Daten enthalten und diese mittels einer Antenne weitergeben können. Dabei lassen sich Daten berührungslos und ohne Sichtkontakt lesen und speichern. Sobald der Chip das Funksignal eines Lesegeräts – diese werden beispielsweise in so genannten Gates an Ein- und Ausgängen eingebaut oder können mobil verwendet werden – empfängt, übermittelt er automatisch und drahtlos die gespeicherten Daten. Die Übertragung erfolgt über Radiofrequenzen. Damit lassen sich gespeicherte Daten auslesen, mit anderen Daten verknüpfen und mit Datenbanken abgleichen. Da die RFID's

[16] Art. 7 DSG.

[17] Überblick über den Stand der RFID-Technologie: http://www.datenschutz.de/feature/detail/?featid=2 (besichtigt am 8.7.2005).

keine eigene Energiequelle brauchen, lassen sie sich in beliebige Gegenstände integrieren.

5.1.1 Eintrittskarten mit RFID

Für die Fussball-Weltmeisterschaft 2006 in Deutschland werden erstmals in grossem Umfang Eintrittskarten mit RFID-Technologie verwendet[18]. In jeder WM-Eintrittskarte steckt ein RFID-Chip, der über vier KByte Speicher verfügt und auf eine Distanz von bis zu zehn Zentimetern ausgelesen werden kann. Indem ein Lesegerät, welches beispielsweise an den Eingangsschleusen positioniert ist, ein Funksignal zum Ticket sendet, wird ein spezieller Zahlencode an das Lesegerät übermittelt. Dieser Code ermöglicht den Zugriff auf die Datenbank des Deutschen Fussballbundes (DFB-Datenbank), welche im Rahmen des Bestellverfahrens für das Ticket mit Personendaten der Ticketkäufer gespeist wurde. Die Datenbank enthält unter anderen Daten den Namen, die Adresse, das Geburtsdatum, die Fanzugehörigkeit und die Personalausweisnummer der betroffenen Person. Dadurch kann eine eindeutige Zuordnung des Tickets zur registrierten Person hergestellt werden. Solange die Person das Ticket auf sich trägt, ist sie eindeutig identifizierbar, und mit einer Ausdehnung der Stärke der Lesegeräte auch lokalisierbar.

Diese personifizierten Eintrittskarten bergen insbesondere Risiken in Bezug auf das dadurch ermöglichte Tracking – das Verfolgen von Personen und das Erstellen von Bewegungsprofilen. Gegenstände mit RFID-Chips sind aber auch geeignet, um Konsumentenprofile anzulegen und so das Konsumverhalten von Personen zu erfassen. Im Rahmen von Sportveranstaltungen stehen indessen die Kontrolle und die Überwachung der Zuschauerinnen und Zuschauer im Vordergrund. Dadurch, dass die RFID-Technik eine Verknüpfung mit einer Datenbank ermöglicht und somit innert Sekunden nachgeprüft werden kann, wer das Stadion beziehungsweise welchen Sektor betreten darf, erscheint diese Technik den Veranstaltern als geeignetes Mittel zur Eingangskontrolle.

Beim Einsatz von RFID-Technologie stellen sich Fragen in Bezug auf die Rechtmässigkeit und die Verhältnismässigkeit dieser Massnahmen. Insbesondere ist dabei nach dem Grundsatz von Treu und Glauben den Zuschauerinnen und Zuschauern volle Transparenz über die Verwendung dieser Technologie zu verschaffen. In Bezug auf die Verhältnismässigkeit

[18] WEICHERT, 7 ff.; NZZ, 28.1.2005, 65.

ist einerseits dafür zu schauen, dass nur erforderliche Daten auf dem Chip respektive in der Datenbank gespeichert werden und dass auch die RFID-Technologie so ausgestaltet wird, dass nach der Erfüllung des Zweckes – Eingangskontrolle – kein weiteres Auslesen von Daten mehr möglich ist. Ebenso ist das Prinzip der Zweckbestimmung zu beachten, und Daten, die in Zusammenhang mit einer Eingangskontrolle bearbeitet werden, sind nicht für andere Zwecke zu verwenden. Der datenschutzkonforme Einsatz dieser Technologien stellt deshalb einige Anforderungen an die Veranstalter. Gefahren, die zu einer allgemeinen Überwachung führen, ist deshalb durch den Einsatz einer datenschutzgerechten Technikgestaltung zu begegnen.

5.1.2 Sportgeräte mit RFID

RFID-Technologie wird auch in Sportgeräten Verwendung finden. RFID-Chips sollen in Skis und Snowboards eingebaut und die Sportgeräte in einer internationalen Datenbank registriert werden. Die in den Sportgeräten integrierten RFID's lösen alsdann an Kontrollstationen bei Bergbahnen Alarm aus, sofern es sich um ein Sportgerät handelt, welches als gestohlen gemeldet wurde.

Innerhalb der nächsten drei Jahre sollen in Österreich 80 Prozent der neuen Ski- und Snowboard-Modelle mit diesen RFID-Chips versehen werden[19]. Somit ist der Zweck dieser Datenbearbeitungen das Wiederauffinden von gestohlenen Geräten und letztendlich die Überführung der Täterschaft. Auch hier stellen sich die unter Ziffer 5.1.1 erwähnten datenschutzrechtlichen Fragestellungen.

Des weiteren sollen RFID's in Turnschuhen integriert werden. Damit ist es Veranstaltern von Grossanlässen möglich, den Sportlern und Sportlerinnen individuell eine genaue Zeitmessung zu garantieren. Auch mit dieser Zwecksetzung sind indessen Risiken für die betroffenen Personen nicht ausgeschlossen. Die unter Ziffer 5.1.1 aufgeführten datenschutzrechtlichen Massnahmen sind im gleichen Masse zu berücksichtigen.

[19] Vgl. www.futurezone.orf.at (Meldung vom 23.02.2005) (besichtigt am 8.7.2005).

5.2 Biometrische Verfahren

Bei biometrischen Verfahren werden individuelle – physiologische oder verhaltenstypische – Merkmale einer Person vermessen und digitalisiert gespeichert[20]. Aufgrund des Abgleichs dieser Templates wird es möglich, eine Person zu identifizieren oder den Besitzer eines Ausweises zu verifizieren. Biometrische Verfahren werden deshalb heute eingesetzt, um Personen zu kontrollieren beziehungsweise um ihnen Zugang zu bestimmten Einrichtungen zu geben.

Der Einsatz biometrischer Verfahren erfolgte bis vor einigen Jahren fast ausschliesslich im Hochsicherheitsbereich. In der Zwischenzeit hat sich das Anwendungsgebiet erweitert, und auch der Zutritt zu öffentlichen Sporteinrichtungen wird mittels biometrischer Verfahren geregelt. So sind bereits in der Schweiz Hallenbäder zu finden, die mit einem Zutrittssystem ausgerüstet sind, welches den Zutritt für die Saison- sowie die Jahreskarteninhaberinnen und -inhaber nur mittels Überprüfung des Fingerabdrucks ermöglicht[21].

Die Risiken, die sich aufgrund der Verwendung biometrischer Verfahren für die Persönlichkeitsrechte der betroffenen Personen ergeben, sind vielfältig. Grundlegend stellt sich die Frage der Rechtmässigkeit und der Verhältnismässigkeit solcher Massnahmen. Aus datenschutzrechtlicher Sicht ist auch entscheidend, ob solche Systeme der Identifikation oder der Verifikation dienen. Werden Datenbanken betrieben, die Rohdaten und Templates verwalten, ist eine korrekte Löschung der Rohdaten respektive eine Weiterverwendung der Templates in anderem Zusammenhang durch technische Massnahmen auszuschliessen. Damit kann dem Grundsatz der Zweckbindung Rechnung getragen werden.

5.3 Videotechnologie

Der Einsatz von Videotechnologie hat in den letzten Jahren sowohl im öffentlichen wie auch im privaten Bereich sehr stark zugenommen. Seit die Aufnahmen digitalisiert werden, ist die Handhabung dieser Technologie einfach geworden. Bilder und Daten lassen sich leicht kopieren, austauschen und mit anderen Daten verknüpfen. Sobald auf diesen Aufnahmen

[20] Überblick zum Thema Biometrie und Datenschutz: http://www.datenschutz.de/themen/?catchid=1308&score=1 (besichtigt am 8.7.2005).

[21] NZZ, 20.7.2005, 49.

bestimmte oder bestimmbare Personen erkennbar werden, handelt es sich um eine Bearbeitung von Personendaten, die den Anforderungen des Datenschutzgesetzes zu entsprechen hat.

Der Einsatz der Videotechnologie erfolgt im Rahmen von Sicherheitsmassnahmen insbesondere zur Überwachung von Stadien, Zuschaueransammlungen oder spezifischen Zu- und Ausgangsbereichen. Dabei werden mobile und feste Videogeräte eingesetzt. Soweit Geräte für eine rein observierende Überwachung[22] eingesetzt werden, um beispielsweise Zuschauerströme zu überwachen und keine Identifikation von Einzelpersonen möglich ist, liegt kein datenschutzrelevanter Sachverhalt vor. Allerdings zeigt sich, dass mit dieser Form der Überwachung mittels neuer technischer Einrichtungen – mittels Zoom- und Bildauflösungsmöglichkeiten – vermehrt auch Personen betroffen sein können.

Die dissuasive Videoüberwachung[23] wird präventiv eingesetzt, um Personen beobachten zu können und allenfalls bei einem deliktischen Verhalten auch überführen zu können. Diese Überwachung richtet sich in der Regel auf eine Vielzahl von unbestimmten Personen, die sich im überwachten Raum befinden. Da sie auf die Erkennbarkeit und Bestimmbarkeit von Personen ausgerichtet ist, handelt es sich um einen Eingriff in die persönliche Freiheit. Die datenschutzrechtlichen Rahmenbedingungen sind zu beachten. Im Vordergrund steht die Rechtmässigkeit dieser Überwachungsmassnahmen gegenüber einer unbestimmten Anzahl von Personen, bei denen weder ein konkreter Tatverdacht noch ein bestimmtes deliktisches Verhalten vorliegt. Soweit öffentliche Organe hier tätig werden, ist eine entsprechende formellgesetzliche Rechtsgrundlage notwendig[24]. Für privatrechtlich handelnde Organisationen ist ein Rechtfertigungsgrund Voraussetzung. Des Weiteren ist bei der präventiven Überwachung die Regelung der Verwendung und Aufbewahrung im Einzelnen zu regeln, damit die Voraussetzungen der Verhältnismässigkeit und der Zweckbindung der Datenbearbeitungen gewährleistet ist.

Die Videoüberwachung muss ein geeignetes Mittel zur Zweckerfüllung – Verhinderung von Gewaltausschreitungen – darstellen. Zudem kommt eine Überwachung nur in Frage, wenn nicht weniger einschneidende Massnahmen wie vermehrtes Sicherheitspersonal, Eingangskontrollen, Trennung von Fangruppen etc. zum gleichen Erfolg führen. Im Sinne

---

22 Zum Begriff: BAERISWYL, 26.

23 BAERISWYL, 26 f.

24 Vgl. zu den Anforderungen im öffentlich-rechtlichen Bereich: DATENSCHUTZBEAUFTRAGTER DES KANTONS ZÜRICH.

der Verhältnismässigkeit ist eine zeitlich und örtlich begrenzte Überwachung angebracht.

Durch technische Massnahmen ist zu verhindern, dass die Bilddaten manipuliert und verändert werden können (Integrität). Werden die Bilder aufgezeichnet, ist deren Aufbewahrungsdauer beziehungsweise Löschung zu regeln. Eine Weitergabe der Aufzeichnungen an die Strafuntersuchungsbehörden ist nur im Rahmen der Einleitung eines Strafverfahrens möglich und hat unverzüglich zu erfolgen. Die dissuasive Videoüberwachung ist aus Gründen der Transparenz für die betroffenen Personen durch entsprechende Hinweise erkennbar zu machen, bevor sie den Aufnahmebereich betreten.

Die Frage der Verhältnismässigkeit impliziert auch, dass der Einsatz der Überwachungsmassnahme im Rahmen eines Sicherheitskonzepts erfolgt, das auch den Schutz der betroffenen Person umfasst. In diesem Sinne ist eine Videoüberwachung in diesem Zusammenhang, die lediglich Aufzeichnungen vornimmt, ohne gleichzeitig ein aktives Handlungsdispositiv zum Schutz der betroffenen Personen beispielsweise vor Gewaltauswirkungen zu umfassen, zum vornherein nicht geeignet, um einen Eingriff in die persönliche Freiheit zu rechtfertigen. Deshalb stellt sich auch die Frage nach einer Garantenstellung desjenigen, der eine Videoüberwachung einsetzt. Unter Umständen könnte er zur Verantwortung gezogen werden, wenn er mittels Videoüberwachung einen Eingriff in die persönliche Freiheit der betroffenen Person vornimmt, aber nichts vorkehrt, um beispielsweise bei den dadurch beobachteten Delikten die körperliche Integrität der überwachten Personen zu schützen.

5.4 Gesichtserkennung

Bei der Gesichtserkennung („Face Recognition“) handelt es sich um eine Kombination von biometrischen Verfahren mit Videotechnologie[25]. Gesichter werden mittels biometrischer Verfahren vermessen und damit mit einem eindeutigen Merkmal versehen. Die vermessenen Bilder („Templates“) werden in einer Datenbank aufbewahrt, die weitere Identifikationsmerkmale einer Person enthalten kann. Erfolgt eine Aufnahme mittels eines Videogerätes, das eine Gesichtserkennung vornimmt, kann diese Auf-

[25] BUNDESAMT FÜR SICHERHEIT IN DER INFORMATIONSTECHNIK (BSI).

nahme ohne weiteres mit den in der Datenbank vorhandenen Daten abgeglichen werden[26].

Der Einsatz von Gesichtserkennungssystemen – bisher eine Technologie, die dem Hochsicherheitsbereich vorbehalten war – ist ebenfalls im Bereich des Sports bekannt. So wurde ein solches System bereits bei den Olympischen Spielen in Atlanta (1996) eingesetzt. Auch bei der Begegnung zwischen den Fussballvereinen West Ham United und Manchester United Ende 1999 machte man von diesem System Gebrauch. Eine breite Diskussion in den USA hat der Einsatz von Gesichtserkennungssystemen beim American-Football-Finale 2001 (Tempa) ausgelöst[27].

Gesichtserkennungssysteme basieren auf dem Abgleich mit einer Datenbank, weshalb sich aus datenschutzrechtlicher Sicht die Hauptfrage nach der rechtmässigen Führung dieser Datenbank richtet. Öffentliche Organe benötigen hierzu eine formellgesetzliche Rechtsgrundlage. Ein Rechtfertigungsgrund zur Führung einer solchen Datenbank durch private Organisationen dürfte kaum gegeben sein. Insbesondere wenn die Aufnahme in die Datenbank auf Verdachtsdaten beruht und zur Überführung von Delinquenten dienen soll, liegt für die betroffenen Personen ein schwerer Eingriff in die persönliche Freiheit vor, der in dieser Form staatlichen Organen vorbehalten sein dürfte. Grundsätzlich stellt sich aber beim Einsatz von Gesichtserkennungssystemen in diesem Zusammenhang die Frage der Verhältnismässigkeit, der Zweckbindung und der Integrität[28].

6. Zuschauerinnen und Zuschauer

6.1 Zuschauervertrag und Datenschutz

Der so genannte Zuschauervertrag regelt das Rechtsverhältnis zwischen Zuschauer und Veranstalter[29]. Über dessen Rechtsnatur bestehen verschiedene Theorien. Während die ältere Lehre und die Rechtsprechung auf den Zuschauervertrag die Vorschriften über den Werkvertrag angewendet ha-

---

26 PETERMANN/SAUTER, 63.

27 PETERMANN/SAUTER, 63 f.

28 Vgl. DATENSCHUTZBEAUFTRAGTER DES KANTONS ZÜRICH, Tätigkeitsbericht (Nr. 8) 2002, 29 f.

29 JENNY, 61 f.

ben, dürfte diese Ansicht heute weitgehend überholt sein[30]. Gemäss neuerer bundesgerichtlicher Rechtsprechung fallen unkörperliche Leistungen – worunter auch die Durchführung einer Sportveranstaltung zu subsumieren ist – nicht mehr unter den Werkbegriff. Vielmehr wird heute die Meinung vertreten, dass es sich um einen Innominatkontrakt handle, der je nach Ausgestaltung werkvertragliche, auftrags- und mietrechtliche Elemente enthalten kann[31]. Die herrschende Lehre geht davon aus, dass die Offerte vom Zuschauer abgegeben wird, indem er ein Ticket verlangt. Die Annahme der Offerte erfolgt durch den Veranstalter, sei es, dass ein Ticket ausgestellt wird oder dass eine Bestätigung erfolgt, beispielsweise bei einer Vertragsabwicklung im Internet.

Des Weiteren stellen sich Fragen, was zum Vertragsinhalt gehört[32].

Aus datenschutzrechtlicher Sicht ist von Bedeutung, dass mögliche Eingriffe in die persönliche Freiheit eines Rechtfertigungsgrunds bedürfen. Eine vertragliche Vereinbarung mit entsprechender Einwilligungsklausel kann dabei regelmässig als Rechtfertigungsgrund herangezogen werden.

Im vorliegenden Fall ist grundsätzlich davon auszugehen, dass der Zuschauer einer Sportveranstaltung nicht mit einem Eingriff in die persönliche Freiheit zu rechnen hat. Auch bei Sicherheitsmassnahmen ist davon auszugehen, dass sich diese in erster Linie gegen die Störer richten und nicht gegen Zuschauerinnen und Zuschauer, die sich keines deliktischen Verhaltens verdächtig machen. Liegt keine explizite Einwilligung des Zuschauers in bestimmte Sicherheits- und Überwachungsmassnahmen im Rahmen des Vertragsabschlusses vor, ist davon auszugehen, dass solche Massnahmen grundrechtskonform umgesetzt sind und nicht in die persönliche Freiheit der Zuschauerinnen und Zuschauer eingreifen dürfen. Es ist deshalb in der Regel problematisch, wenn auf Sicherheits- und Überwachungsmassnahmen nach Abschluss des Vertrages hingewiesen wird, da hier nicht mehr mit einer – auch konkludenten –Einwilligung der betroffenen Personen gerechnet werden kann[33]. Ebenso wenig kann von der notwendigen Freiwilligkeit der Einwilligung ausgegangen werden. Damit hat sich die Datenbearbeitung auf die für die Abwicklung des Vertrages geeigneten und erforderlichen Massnahmen zu begrenzen. Ein Eingriff in

30 JENNY, 67.
31 JENNY, 67.
32 JENNY, 62 ff.
33 Vgl. auch das Beispiel bei JENNY, 65 f.

die persönliche Freiheit ist dabei regelmässig nicht verhältnismässig und durch keinen Rechtfertigungsgrund legitimiert.

6.2 Eintrittskarten

Mit dem Vertragsschluss zum Besuch einer Sportveranstaltung wird oftmals eine Eintrittskarte abgegeben. Mit dem Ticket weist der Zuschauer gegenüber dem Veranstalter seine Forderung aus, weshalb das Ticket für die gesamte Rechtsbeziehung zwischen Veranstalter und Zuschauer von grosser Bedeutung ist[34]. Aus datenschutzrechtlicher Sicht stellt sich die Frage, welche Angaben der Veranstalter vom Zuschauer für die Abwicklung des Vertrages benötigt. Insbesondere steht heute die Absicht nach einer Identifizierung des Zuschauers im Vordergrund.

Grundsätzlich ist davon auszugehen, dass der Besuch einer Sportveranstaltung anonym erfolgen kann, da für den Abschluss des Vertrages – beim Bargeschäft – und für die Abwicklung des Vertrages eine Identifizierung nicht notwendig ist. Das Ticket ist somit nicht persönlich und die Leistung grundsätzlich übertragbar. Erfolgt die Bezahlung des Tickets über eine Kreditkarte, so wird der Käufer identifizierbar. Nach dem Prinzip der Zweckbindung sind solche Daten aber einzig für die Zahlungsabwicklung zu verwenden, und die Abwicklung des Vertrages – der Bezug der Leistung durch den Käufer – erfolgt wiederum anonym.

Aus diesen Sachverhalten wird auch deutlich, dass ein Zuschauervertrag grundsätzlich ohne die Bearbeitung von personenbezogenen Daten abgeschlossen und durchgeführt werden kann. Eine Bearbeitung von Personendaten in diesem Zusammenhang braucht deshalb einen Rechtfertigungsgrund[35].

Insbesondere bei grossen Sportveranstaltungen werden heute zunehmend Personendaten bearbeitet. Bereits beim Abschluss des Vertrages werden vom Käufer Daten verlangt, die eine eindeutige Identifizierung zulassen. Indem die Tickets personalisiert und mit entsprechender Technologie ausgestattet werden[36], bleibt der Zuschauer während der gesamten Vertragsabwicklung identifizierbar. Damit ist auch die identifizierende Eintrittskontrolle vorgegeben[37]. Diese Massnahmen, die einerseits mit Si-

[34] JENNY, 68.
[35] Art. 12 Abs. 2 lit. a DSG.
[36] Siehe Ziff. 5.1.1.
[37] Siehe Ziff. 6.3.

cherheitsüberlegungen begründet werden – gewaltbereite Sportfans sollen durch die Identifikationsmöglichkeit abgeschreckt werden – und andererseits mit wirtschaftlichen Gründen – der Schwarzhandel soll unterbunden werden – sind aus datenschutzrechtlicher Sicht nicht unproblematisch.

Grundsätzlich erfordert dieses Vorgehen die explizite Zustimmung der betroffenen Personen. Die Zielsetzung dieser Datenbearbeitung ist transparent darzulegen, und es sind nur Daten zu bearbeiten, die für diese Zielsetzung geeignet und erforderlich sind. Ausserdem sind diese Daten nur für diesen bestimmten Zweck zu verwenden, und nach der Zweckerfüllung wieder zu vernichten, sofern nicht eine anders lautende Zustimmung der betroffenen Person vorliegt. Insbesondere ist das Anlegen einer Datensammlung auf Vorrat in diesem Zusammenhang durch keinen Rechtfertigungsgrund abgedeckt.

Das Beispiel der Fussballweltmeisterschaften 2006 zeigt bereits, dass hier Datenbearbeitungen erfolgen können, die den datenschutzrechtlichen Prinzipien nicht gerecht werden. Im Zusammenhang mit den Tickets zu diesem Grossanlass ist nicht erkennbar, weshalb das genaue Geburtsdatum angegeben werden muss. Es ist anzunehmen, dass dieses Datum für die Werbebranche von grossem Wert ist, weil hierüber Datenbanken miteinander verknüpft werden können. Die Angabe „älter als 18 Jahre“ würde genügen. Damit stellen sich die Fragen der Verhältnismässigkeit, der Zweckbindung und bei der (widerrechtlichen) Verknüpfung mit anderen Daten auch diejenige der Integrität[38].

6.3 Eintrittskontrollen

Eintrittskontrollen variieren je nach Grösse und Art der Sportveranstaltung. In der Regel geht es um die Überprüfung der Zutrittsberechtigung durch das Vorweisen des Tickets. Immer mehr erfolgen aber neben der Berechtigungskontrolle auch Kontrollen, die Teil von Sicherheitsmassnahmen sind. Soweit es sich um weiter gehende Überprüfungen handelt, stellen sie einen Eingriff in die persönliche Freiheit dar. Insofern sie sich nicht an einen verdächtigen Störer richten, scheint als Rechtfertigungsgrund nur die Einwilligung gegeben. Sie ist im Rahmen des Vertragsabschlusses entsprechend transparent einzuholen[39].

[38] WEICHERT, 8.
[39] Siehe Ziff 6.1.

Weiter gehende Kontrollen, die eine Ausweiskontrolle respektive Identifikation der Zuschauerinnen und Zuschauer anstreben, sind im Rahmen von internationalen Grossveranstaltungen geplant. Dabei ist auch die Verweigerung der Leistung vorgesehen, sofern kein Ausweis zur Identifikation vorgelegt werden kann. Mit den Eintrittskontrollen an der Fussballweltmeisterschaft 2006 in Deutschland geht man noch einen Schritt weiter: Die Eintrittskontrolle soll mit Hilfe der RFID-Tickets[40] automatisiert werden. Die Ticketkontrolle wird per RFID-Leser an den Eingangsschleusen der Stadien erfolgen. Mit Hilfe der RFID-Tickets kann nicht nur eine eindeutige Identitätsfeststellung erfolgen, sondern die Informationen können gleichzeitig mit Datenbanken abgeglichen werden. Neben dem Abgleich mit der Datenbank des Veranstalters ist die Integration weiterer Datenbanken in diesen Prozessablauf denkbar. Insofern hier Datenbanken von öffentlichen Organen betroffen sind, ist eine entsprechende Rechtsgrundlage notwendig. Für die Zuschauerinnen und Zuschauer ist die notwendige Transparenz beim Abschluss des Zuschauervertrags zu schaffen. Insbesondere stellen sich aber generell Fragen der Verhältnismässigkeit solcher Massnahmen[41].

6.4 Verhaltenskontrollen

Zu den zahlreichen Sicherheitsmassnahmen in und um einen Veranstaltungsort gehören auch Verhaltenskontrollen der Zuschauerinnen und Zuschauer. Aus datenschutzrechtlicher Sicht kommt dabei den technischen Überwachungsmassnahmen eine besondere Bedeutung zu. Diese Eingriffe in die persönliche Freiheit brauchen klare Rahmenbedingungen, damit das Prinzip der Verhältnismässigkeit respektiert wird. Primär haben sich die Massnahmen an den potentiellen Störer zu richten und den „unbescholtenen" Zuschauer nicht zu tangieren. Sofern Aufzeichnungen erfolgen, sind sie – soweit keine Störungen registriert wurden, die zur Einleitung einer Strafuntersuchung Anlass geben – wieder zu vernichten. Zu beachten gilt auch das Prinzip der Zweckbindung: Die zur Eruierung von Störern und zur Aufrechterhaltung der Sicherheit gemachten Aufnahmen dürfen nicht zu anderen Zwecken verwendet werden.

Da der Zuschauer grundsätzlich nicht mit einer Beobachtung und/oder Aufzeichnung seines Verhaltens während einer Sportveranstaltung rech-

40 Siehe Ziff. 5.1.1.
41 WEICHERT, 7 ff.

nen muss, ist dies nur mit einer entsprechenden Einwilligung (im Rahmen des Vertragsabschlusses) möglich[42].

6.5 Datenaustausch

Da die Veranstalter von Sportveranstaltungen, um die Sicherheit zu gewährleisten, eigene Sicherheitsdienste einsetzen, andere private Sicherheitsdienste beauftragen und mit der Polizei zusammenarbeiten, stellt sich aus datenschutzrechtlicher Sicht die Frage des Informationsaustausches zwischen diesen Stellen.

Vorweg ist festzuhalten, dass die Polizei als öffentlich-rechtliches Organ aufgrund der jeweiligen kantonalen Datenschutzgesetze für ihre Tätigkeiten eine formellgesetzliche Rechtsgrundlage braucht. Polizeigesetze, Strafprozessordnungen oder Bundesgesetze geben der Polizei die Kompetenz zur Bearbeitung von Personendaten und zur Führung von entsprechenden Datenbanken auch im Zusammenhang mit polizeilichen Aufgaben im Rahmen von Sportveranstaltungen[43]. Nur die Polizei hat die Kompetenz, Personen anzuhalten, diese zu kontrollieren, zu befragen und gegebenenfalls zu verhaften. Private Sicherheitsdienste haben keine polizeilichen Befugnisse. Sie haben die gleichen Rechte wie eine Privatperson: Ein Angehöriger eines privaten Sicherheitsdienstes kann lediglich bei der Polizei Strafanzeige erstatten und in Notwehr- und Notstandssituationen eingreifen – genauso wie jeder andere Bürger es tun darf. Allenfalls liegt ein Rechtfertigungsgrund bei Sicherheitsmassnahmen im Rahmen der Eintrittskontrolle vor[44].

Soweit Beobachtungen oder Aufzeichnungen mittels Videoüberwachung oder anderen technischen Einrichtungen durch den Veranstalter oder Sicherheitsdienste erfolgen, darf dieses Material an die Polizei im Rahmen einer Strafanzeige weitergegeben werden. Die Polizei ihrerseits kann Private in einem verhältnismässigen Masse in die polizeiliche Ermittlung einbeziehen und so wiederum auf Informationen und Daten von Sicherheitsdiensten zugreifen. Allerdings handelt es sich hier um Datenbearbeitungen in einem konkreten Einzelfall. Für einen regelmässigen Datenaustausch zwischen privaten Sicherheitsdiensten und Polizei liegen we-

42 Siehe Ziff. 6.1.
43 GUNDELFINGER, 187 ff.
44 Siehe Ziff. 6.3.

der gesetzliche Grundlagen noch entsprechende Rechtfertigungsgründe vor.

6.6 Hooliganismus

Sicherheitsmassnahmen im Rahmen von Sportveranstaltungen sind heute sehr stark auf die Bekämpfung des so genannten Hooliganismus ausgerichtet. Hooliganismus gilt als markantes Sicherheitsproblem des modernen Sports. Ein Blick in die Vergangenheit zeigt jedoch, dass dieses Phänomen auch früheren Gesellschaften bekannt war: Formen ritualisierten Schlagabtausches sind bereits auf Fresken aus dem 1. Jahrhundert festgehalten. Eine der wohl bekanntesten Darstellungen ist der Tumult im Amphitheater von Pompeji[45].

Hooliganismus beschäftigt nicht nur die Veranstalter von Sportanlässen, sondern auch das sportliche Umfeld im Rahmen der Massnahmen zur inneren Sicherheit[46]. Auch auf Gesetzesebene werden deshalb Massnahmen zur Bekämpfung des Hooliganismus getroffen[47].

Insoweit der Veranstalter gegen Hooligans vorzugehen hat, kann er sich auf den Zuschauervertrag abstützen, denn es gehört zu den Pflichten des Zuschauers, die vom Organisator gebotene Veranstaltung nicht zu stören[48]. Entsprechende Massnahmen richten sich gegen den Störer und rechtfertigen sich durch die Vertragspflichten.

Mit dem Bundesgesetz über Massnahmen gegen Gewaltpropaganda und Gewalt anlässlich von Sportveranstaltungen[49] sollen Grundlagen geschaffen werden, um gegen den Hooliganismus vorgehen zu können. Die in diesem Zusammenhang geplanten Eingriffe in die persönliche Freiheit – insbesondere der Aufbau einer Hooligan-Datenbank – sind indessen kompetenzrechtlich fraglich geregelt. Der Aufbau der Massnahmen stützt sich auf Art. 1 BWIS, welcher die Bundeskompetenz zur Bearbeitung von Personendaten im präventiven Staatsschutz enthält. Dagegen handelt es

---

45 SOFSKY, 45.

46 BUNDESAMT FÜR POLIZEI, Bericht 2004 Innere Sicherheit der Schweiz, Bern 2005, 23 ff.

47 Eine umfassende Darstellung der Rechtslage betreffend Hooliganismus findet sich im Beitrag von DANIEL THALER in diesem Band.

48 JENNY, 65.

49 Botschaft zur Änderung des Bundesgesetzes über Massnahmen zur Wahrung der inneren Sicherheit (Massnahmen gegen Gewaltpropaganda und gegen Gewalt anlässlich von Sportveranstaltungen) vom 17. August 2005, BBl 2005, 5613.

sich bei Gewalt im Rahmen von Sportveranstaltungen um sicherheitspolizeiliche Massnahmen, die als Bestandteil der inneren Sicherheit in den Kompetenzbereich der Kantone fallen[50]. Massnahmen in diesem Rahmen haben sich deshalb zwingend auf eine kantonalrechtliche Gesetzesgrundlage abzustützen und wären bei einer gesamtschweizerischen Lösung im Rahmen eines Konkordates zu verwirklichen. Da es sich um einen schweren Eingriff in die Grundrechte handelt, erscheinen die aktuelle Abstützung der Massnahmen gegen den Hooliganismus und die mangelnde Abgrenzung zwischen Staatsschutz und Innere Sicherheit – auch unter Berücksichtigung des Prinzips der Zweckbindung – als problematisch.

Des Weiteren stellt sich aus datenschutzrechtlicher Sicht die Frage der Verhältnismässigkeit. Die Hooligan-Szene ist relativ klein[51], weshalb Massnahmen gezielt gegen die Störer zu richten sind. Auf jeden Fall kann nur ein Verhalten einer Person, das den dringenden Verdacht auf eine Straftat auslöst, Gegenstand von entsprechenden Massnahmen sein. Ebenso wären die weiteren geplanten Massnahmen im Umfeld der Hooligan-Szene deshalb auf ihre Verhältnismässigkeit zu überprüfen.

7. Sportvereine

7.1 Mitgliederdaten

Im Bereich des Amateursports existiert eine Vielzahl von Vereinen, die Daten über ihre Mitglieder oder über Teilnehmende an ihren Veranstaltungen bearbeiten. Da auch hier immer mehr moderne Kommunikationsmittel – insbesondere das auf dem Internet basierende World Wide Web (WWW) – in Anspruch genommen werden, stellen sich Fragen, wie mit diesen Daten umzugehen ist. Auch der privatrechtlich organisierte Verein hat sich beim Umgang mit Personendaten seiner Mitglieder an die Prinzipien des Datenschutzrechts zu halten. Im Vordergrund steht dabei die Rechtmässigkeit der Datenbearbeitung. Sie ergibt sich einerseits aus dem Zweck des Vereins und dessen Aufgabenumschreibung und andererseits aus der Einwilligung der Mitglieder zu bestimmten weiteren Datenbearbeitungen. Insbesondere bei der Weitergabe und der Publikation von Mitgliederdaten ist das Prinzip der Verhältnismässigkeit zu beachten.

[50] Art. 57 BV.
[51] Siehe Beitrag von DANIEL THALER, in diesem Band.

Ein Sportverein verfügt über zahlreiche Daten seiner Mitglieder. Beim Vereinsbeitritt und während der Vereinsmitgliedschaft sind indessen nur solche Daten von Mitgliedern zu bearbeiten, die zur Erreichung des Vereinszwecks tatsächlich benötigt werden, d.h. in direktem Zusammenhang mit dem Vereinszweck stehen.

Auch innerhalb des Vereins gilt das Verhältnismässigkeitsprinzip. Die Verwendung von Mitgliederdaten durch Funktionsträger ist auf die für die Ausübung ihrer Funktion notwendigen Mitgliederdaten zu beschränken.

Will der Verein im Einzelfall über die in den Statuten vorgesehenen Datenbearbeitungen hinaus weitere Mitgliederdaten erheben und bearbeiten, so sind die Mitglieder vorgängig darüber zu informieren, zu welchem Zweck solche Daten verwendet werden. Die Mitteilung solcher Daten, welche ausserhalb des Vereinszwecks liegen, erfolgt auf der (auch konkludenten) Einwilligung und muss daher freiwillig sein[52]. Auch wenn eine spätere andere Verwendung der Daten bei der Erhebung nicht absehbar war, ist das Mitglied darüber zu informieren, wenn die Daten für andere Zwecke benötigt werden. Den Mitgliedern ist beispielsweise mitzuteilen, wenn Personendaten an Dritte ausserhalb des Vereins oder an andere Mitglieder innerhalb des Vereins – etwa in Form von Mitgliederlisten – weitergegeben werden, an wen sie gegeben werden und zu welchem Zweck dies geschieht. Durch einen solchen Hinweis erhalten die Mitglieder Gelegenheit, rechtzeitig Einwände hiergegen geltend zu machen respektive ihre Einwilligung zurückzuziehen.

Die Bekanntgabe von Mitgliederdaten an Dritte (beispielsweise Medien, Sponsoren, Private) ist zulässig, sofern alternativ eine der folgenden Voraussetzungen erfüllt ist: Die Einwilligung der betroffenen Mitglieder wurde eingeholt, den Vereinsmitgliedern wurde unter vorgängiger Mitteilung des Empfängers und des Zwecks der Bekanntgabe ein Widerspruchsrecht eingeräumt oder den Vereinsstatuten ist klar zu entnehmen, welche Mitgliederdaten zu welchem Zweck (z.B. Werbung, Sponsoring) an Dritte – diese sollten im Einzelfall genau bezeichnet sein – bekannt gegeben werden dürfen. Vor allem Sponsoren verlangen nicht selten als Gegenleistung für ihre Unterstützung die Weitergabe von Mitgliederdaten, die dann zu Werbezwecken eingesetzt werden. Bei der Datenbekanntgabe an Dritte beruhend auf der Einwilligung steht jedem Mitglied frei, jederzeit seine Einwilligung zur Bekanntgabe der Daten teilweise oder ganz zu widerrufen[53].

---

[52] EDSB, 1.
[53] EDSB, 2.

7.2 Internet-Auftritt

Die Publikation von Personendaten auf Websites ist aus datenschutzrechtlicher Sicht mit zahlreichen Risiken für die Persönlichkeitsrechte der betroffenen Personen behaftet. Einmal ins World Wide Web (WWW) gestellte Informationen sind kaum mehr zu entfernen. Auch einzelne Daten oder Fotos lassen in Kombination mit anderen Informationen eine Identifikation einer Person zu. Zudem besteht das Risiko, dass Informationen im WWW zu anderen als den vorgesehenen Zwecken verwendet werden und sogar zur Erstellung von eigentlichen Persönlichkeitsprofilen herangezogen werden[54].

Trotzdem liegt es im Trend, dass Vereine Informationen über ihre Mitglieder im Internet veröffentlichen: Der Auftritt im Internet stellt für den Verein und dessen Sportler einerseits eine Informationsplattform für die eigenen Zwecke dar, andererseits sehen die Vereine darin die Möglichkeit der Selbstdarstellung.

Vereine haben aufgrund ihres Vereinszwecks zu überlegen, welche personenbezogenen Daten sie im Internet veröffentlichen können. Es ist zu prüfen, ob die zur Veröffentlichung ins Auge gefassten Informationen für den zu verfolgenden Zweck tatsächlich geeignet und erforderlich sind (Verhältnismässigkeitsprinzip). Soweit der Vereinszweck die Publikation von Daten im Internet nicht vorsieht respektive aus der Zwecksetzung keine konkreten Datenkategorien sich ableiten lassen, ist eine Publikation auf die Zustimmung des Vereinsmitglieds – nach einer vorgängigen Aufklärung über die Risiken – angewiesen[55]. Insbesondere die Veröffentlichung von Fotos im Internet ist nur mit der Einwilligung der betroffenen Person möglich. Eine Zustimmung kann auch stillschweigend erteilt werden, indem der Verein die Mitglieder beispielsweise über das Vorhaben der Publikation auf der Website informiert. Den Mitgliedern steht dabei ein Widerspruchsrecht zu.

8. Schlussfolgerungen

Durch die Nutzung moderner Informations- und Kommunikationstechnologien haben auch im Bereich des Sports Fragen des Datenschutzes und

[54] Zu den Risiken des Internet aus datenschutzrechtlicher Sicht: TINNEFELD/EHMANN/GERLING, 31 ff.

[55] EDSB, 2.

der Datensicherheit an Aktualität gewonnen. Dabei ist festzustellen, dass die datenschutzrechtlichen Prinzipien bisher noch keine einheitliche Umsetzung erfahren haben. Vielmehr sind die datenschutzrechtlichen Fragestellungen erst andiskutiert worden. Die Grenzziehung zwischen dem Recht der Zuschauerinnen und Zuschauer auf ihre persönliche Freiheit und den berechtigten Interessen der Organisatoren von Sportveranstaltungen auf eine sichere Durchführung dieser Anlässe hat noch nicht zu einer gesicherten Rechtspraxis geführt. Insbesondere mit dem Einsatz von neuen Technologien zur Kontrolle und Überwachung stellt sich die Frage nach der datenschutzkonformen Ausgestaltung der eingesetzten Systeme. Neben den im vorliegenden Beitrag betrachteten Bereichen sind zahlreiche weitere datenschutzrechtliche Themenfelder im Sport vorhanden, insbesondere die Frage der Persönlichkeitsrechte der aktiven Sportlerinnen und Sportler, des Umgangs mit besonders schützenswerten Daten, des (internationalen) Austauschs von Daten zwischen den verschiedenen Akteuren und generell der Verwendung und Aufbewahrung von personenbezogenen Informationen.

Literaturverzeichnis

BAERISWYL, BRUNO: Videoüberwachung – im rechtsfreien Raum? Datenschutzrechtliche Aspekte moderner Überwachung mittels optischen Geräten, digma 2002, 26.

BAERISWYL, BRUNO/RUDIN, BEAT: Perspektive Datenschutz, Praxis und Entwicklungen in Recht und Technik, Zürich 2002.

BÄUMLER, HELMUT: Datenvermeidung und Datensparsamkeit, in: BAERISWYL, BRUNO/RUDIN, BEAT (Hrsg.): Perspektive Datenschutz, Praxis und Entwicklungen in Recht und Technik, Zürich 2002, 351.

BUNDESAMT FÜR SICHERHEIT IN DER INFORMATIONSTECHNIK (BSI): BioFace, Vergleichende Untersuchung von Gesichtserkennungssystemen, Bonn 2003.

DATENSCHUTZBEAUFTRAGTER DES KANTONS ZÜRICH: Videoüberwachung durch öffentliche Organe, Grundlagen, Empfehlungen und Checkliste, Zürich 2002, abrufbar unter www.datenschutz.ch (besichtigt am 8.7.2005).

EIDGENÖSSISCHER DATENSCHUTZBEAUFTRAGTER (EDSB): Merkblatt über den Umgang mit Mitgliederdaten in einem Verein, Bern 2003, abrufbar unter www.edsb.ch (besichtigt am 8.7.2005).

GUNDELFINGER, DANIEL E.: Polizeieinsätze bei Sportgrossveranstaltungen – die Rechtsgrundlagen, in: SCHERRER, URS/ZÖLCH, FRANZ A. (Hrsg.): Sportveranstaltungen – im Fokus von Recht und Wirtschaft, Zürich 2004, 187.

JENNY, CHRISTIAN: Der Zuschauervertrag, in: SCHERRER, URS/ZÖLCH, FRANZ A. (Hrsg.): Sportveranstaltungen – im Fokus von Recht und Wirtschaft, Zürich 2004, 57.

LANGHEINRICH, MARC/MATTERN, FRIEDMANN: Wenn der Computer verschwindet, Was Datenschutz und Sicherheit in einer Welt intelligenter Alltagsdinge bedeuten, digma 2002, 138.

MATTERN, FRIEDMANN: Vom Verschwinden des Computers – Die Vision des Ubiquitous Computing, in: MATTERN, FRIEDMANN (Hrsg.): Total vernetzt, Berlin 2003.

PETERMANN, THOMAS/SAUTER, ARNOLD: Biometrische Identifikationssysteme, Sachstandsbericht, BÜRO FÜR TECHNIKFOLGENABSCHÄTZUNG BEIM DEUTSCHEN BUNDESTAG (Hrsg.), TAB Arbeitsbericht Nr. 76, Berlin 2002.

SOFSKY, WOLFGANG: Krawall machen, NZZ vom 13./14. November 2004, 45.

TINNEFELD, MARIE-THERES/EHMANN, EUGEN/GERLING, RAINER W.: Einführung in das Datenschutzrecht, München/Wien 2005.

WEICHERT, THILO: Die Fussball-WM als Überwachungs-Grossprojekt, Datenschutz Nachrichten 1/2005, 7.