Sportverbandskommentar 15.05.2024

Datenschutz im Sport

Rehana C. Harasgama
Sebastiano Tela
Jan Kleiner

Zitiervorschlag: Rehana C. Harasgama/Sebastiano Tela/Jan Kleiner, Datenschutz im Sport, in: Anne Mirjam Schneuwly/Yael Nadja Strub/Mirjam Koller Trunz (Hrsg.), Sportverbandskommentar, https://sportverbandskommentar.ch/datenschutz, 1. Aufl. (publiziert am 15. Mai 2024)

Kurzzitat: Harasgama/Tela/Kleiner, Rz. xx.

Literatur

Anz Philipp, **Xplain-Hack legt offen: Einträge aus Hooligan-Datenbank wurden nicht gelöscht**, Inside IT, 12. Juli 2023, besucht am 26. Januar 2024; Baeriswyl Bruno; in: Baeriswyl Bruno/Pärli Kurt/Blonski Monika (Hrsg.), Stämpflis Handkommentar Datenschutzgesetz, 2. Aufl., Bern 2023; Bieri Adrian/Powell Julian, in: Bieri Adrian/Powell Julian (Hrsg.), Orell Füssli Kommentar zum Schweizerischen Datenschutzgesetz mit weiteren Erlassen, Zürich 2023; Blonski Dominika, in: Baeriswyl, Bruno/Pärli, Kurt/Blonski, Monika (Hrsg.), Stämpflis Handkommentar Datenschutzgesetz, 2. Aufl., Bern 2023; Contat Laurent et al., Dopingbekämpfung durch Staat und Private in der Schweiz, Causa Sport 2016, S. 159-179; Dal Molin Luca/Wesiak-Schmidt Kirsten, in: Bieri Adrian/Powell Julian (Hrsg.), Orell Füssli Kommentar zum Schweizerischen Datenschutzgesetz mit weiteren Erlassen, Zürich 2023; Fanger Reto, in: Bieri Adrian/Powell Julian (Hrsg.), Orell Füssli Kommentar zum Schweizerischen Datenschutzgesetz mit weiteren Erlassen, Zürich 2023; Fey Marco, in: Baeriswyl Bruno/Pärli Kurt/Blonski Monika (Hrsg.), Stämpflis Handkommentar Datenschutzgesetz, 2. Aufl., Bern 2023; Gamp Roland, **Viel Gewalt durch Fussballchaoten – trotz verschärfter Massnahmen**, 17. Oktober 2023; Glass Philip, in: Bieri Adrian/Powell Julian (Hrsg.), Orell Füssli Kommentar zum Schweizerischen Datenschutzgesetz mit weiteren Erlassen, Zürich 2023; Glatthaar Matthias/Schröder Annika, Art. **19** und **20**, in: Hürlimann Daniel/Morand Anne-Sophie/Steiner Thomas, Onlinekommentar Datenschutzgesetz, Stand vom 20. August 2023; Gola Peter, in: Gola, Peter/Heckmann, Dirk (Hrsg.), Datenschutz-Grundverordnung, Bundesdatenschutzgesetz Kommentar, 3. Aufl., München 2022; Gordon Clara-Ann/Egli Luisa, in: Bieri Adrian/Powell Julian (Hrsg.), Orell Füssli Kommentar zum Schweizerischen Datenschutzgesetz mit weiteren Erlassen, Zürich 2023; Harasgama Rehana C./Haux Dario, Art. **22** und **23**, in: Hürlimann Daniel/Morand Anne-Sophie/Steiner Thomas (Hrsg.), Onlinekommentar Datenschutzgesetz, Stand vom 20. August 2023; Husi-Stämpfli Sandra/Morand Anne-Sophie/Sury Ursula, Datenschutzrecht, Zürich 2023; Hüsi-Stämpfli Sandra, in: Baeriswyl Bruno/Pärli Kurt/Blonski Monika (Hrsg.), Stämpflis Handkommentar Datenschutzgesetz, 2. Aufl., Bern 2023; Hügi Thomas, Sportrecht, Bern 2015; Kunz Christian, in: Bieri Adrian/Powell Julian (Hrsg.), Orell Füssli Kommentar zum Schweizerischen Datenschutzgesetz mit weiteren Erlassen, Zürich 2023; Lezzi Lukas, in: Bieri Adrian/Powell Julian (Hrsg.), Orell Füssli Kommentar zum Schweizerischen Datenschutzgesetz mit weiteren Erlassen, Zürich 2023; Nolte Martin, Datenschutzrechtliche Grenzen von Anti-Doping-Meldepflichten, Causa Sport 2010, S. 309-316; Pärli Kurt/Flück Nathalie, in: Baeriswyl Bruno/Pärli Kurt/Blonski Monika (Hrsg.), Stämpflis Handkommentar Datenschutzgesetz, 2. Aufl., Bern 2023; Pfaffiger, Monika, in: Baeriswyl Bruno/Pärli Kurt/Blonski Monika (Hrsg.), Stämpflis Handkommentar Datenschutzgesetz, 2.

Aufl., Bern 2023; Plitz Carlo, in: Gola Peter/Heckmann Dirk (Hrsg.), Datenschutz-Grundverordnung, Bundesdatenschutzgesetz Kommentar, 3. Aufl., München 2022; Powell Julian/Schönbächler Matthias R., in: Bieri Adrian/Powell Julian (Hrsg.), Orell Füssli Kommentar zum Schweizerischen Datenschutzgesetz mit weiteren Erlassen, Zürich 2023; Rosenthal David, Das neue Datenschutzgesetz, **Jusletter vom 16. November 2020**; Rudin Beat, in: Baeriswyl Bruno/Pärli Kurt/Blonski Monika (Hrsg.), Stämpflis Handkommentar Datenschutzgesetz, 2. Aufl., Bern 2023; Schmidt Stefan/Hermonies Felix, Dopingkontrollen und Datenschutz am Beispiel der Mannschafts-Whereabouts im Fussball, Causa Sport 2009, S. 339-342; Schulz Sebastian, in: Gola, Peter/Heckmann, Dirk (Hrsg.), Datenschutz-Grundverordnung, Bundesdatenschutzgesetz Kommentar, 3. Aufl., München 2022; Spacek Dirk, in: Bieri, Adrian/Powell, Julian (Hrsg.), Orell Füssli Kommentar zum Schweizerischen Datenschutzgesetz mit weiteren Erlassen, Zürich 2023; Striegel Heiko, Aktuelle Praxis der Whereabouts aus juristischer Sicht, Causa Sport 2009, S. 6-7; Studer Marcel, Mit Datenbanken gegen Hooliganismus Hooligan-Datenbanken als informationelle Massnahmen gegen Gewaltausschreitungen an Sportanlässen, digma 2006, S. 66-69; Sury Ursula, in: Bieri, Adrian/Powell, Julian (Hrsg.), Orell Füssli Kommentar zum Schweizerischen Datenschutzgesetz mit weiteren Erlassen, Zürich 2023; Widmer Micheal, in: Bieri Adrian/Powell Julian (Hrsg.), Orell Füssli Kommentar zum Schweizerischen Datenschutzgesetz mit weiteren Erlassen, Zürich 2023.

Materialien

Allgemeine Vertragsbedingungen (AVB) zum Arbeitsvertrag für Nichtamateur-Spieler der Klubs des Schweizerischen Fussballverbandes, Ausgabe Juni 2017, Anhang 6; **Anleitung für die Prüfung der Zulässigkeit von Datenübermittlungen mit Auslandsbezug, EDÖB**, veröffentlicht im Juni 2021 und angepasst an das revidierte DSG im Mai 2023 (zit. Anleitung Datenübermittlungen mit Auslandsbezug); **Bekämpfung des Hooliganismus, Bericht des Bundesrates in Erfüllung des Postulats 19.3533 der Sicherheitspolitischen Kommission des Ständerates vom 23. Mai 2019**, veröffentlicht am 22. Juni 2022 (zit. Bericht Bekämpfung Hooliganismus); **Botschaft zum Bundesgesetz über die Totalrevision des Bundesgesetzes über den Datenschutz und die Änderung weiterer Erlasse zum Datenschutz vom 15. September 2017**, **BBl 2017 S. 6941** ff.; **Leitfaden zu den technischen und organisatorischen Massnahmen des Datenschutzes (TOM) der EDÖB vom 15. Januar 2024** (zit. Leitfaden zu den TOM); **Medienmitteilung des Bundesrats zum Schutz vor Gewalt im Sport: Bundesrat schafft verbindliche Vorgaben für ethisches Verhalten vom 25. Januar 2023**; **Medienmitteilung der EDÖB zur Untersuchung gegen fedpol und BAZG vom 16. Mai 2023**; **Totalrevision des Datenschutzgesetzes: Häufig gestellte Fragen, Bundesamt für Justiz, veröffentlicht im September 2023** (zit. Häufig gestellte Fragen, BJ).

I. Einleitung

[1] Sportverbände bearbeiten Personendaten in einem grossen Umfang, und zwar nicht nur über Sportler*innen, sondern auch über Fans, Trainer*innen, Manager*innen, Funktionäre*innen, Agent*innen oder Mitarbeitende. Sportverbände verfügen über zahlreiche Kanäle, über die sie Daten erheben können: auf ihren Websites, im Rahmen von Sportanlässen, Spielen und

Wettbewerben, beim Verkauf von *merchandise*, bei der Vermarktung oder Übertragung von Sportanlässen, bei der Durchsetzung von internen Regularien und Vorgaben, durch das *live-tracking* der Leistung von Athlet*innen an einer Sportveranstaltung, beim Betrieb eines Meldeportals für Disziplinarfälle oder durch den Austausch von Daten zwischen den Verbandsmitgliedern und dem Dachverband. Sportverbände erheben nicht nur selbst Daten, sondern erhalten diese z.B. auch von ihren Verbandsmitgliedern, Länderorganisationen, Trainer*innen oder Manager*innen.

[2] Die Personendaten, die erhoben und bearbeitet werden, reichen von allgemeinen Personalien und Kontaktdaten über Gesundheitsdaten bis hin zu detaillierten Profilen. Sportler*innen haben oft wenig Entscheidungsfreiheit darüber, ob sie all diese Daten über sich preisgeben wollen, insbesondere wenn sie eine Profikarriere verfolgen möchten.

[3] Sportverbände bewegen sich bei der Bearbeitung all dieser Personendaten selbstredend nicht in einem rechtsfreien Raum, sondern sind genauso, wie andere Organisationen, die Personendaten bearbeiten, an das geltende Datenschutzrecht gebunden.

[4] Die vorliegende Kommentierung bietet zunächst einen Überblick über die allgemeinen Rechtsgrundlagen und die geltenden Datenschutzgrundsätze, die einzuhaltenden Pflichten sowie über die Rechte, welche Sportverbände gewähren müssen. Danach werden ausgewählte Fragestellungen näher beleuchtet, welche sich spezifisch für Sportverbände stellen.

II. Rechtsgrundlagen

[5] Sportverbände mit Sitz in der Schweiz unterliegen den Bestimmungen des Schweizer Datenschutzgesetzes (DSG). Da sich die Tätigkeit von Sportverbänden häufig auch über die Landesgrenze hinaus erstreckt, können zahlreiche weitere Rechtsordnungen zur Anwendung gelangen, wie z.B. die EU-Datenschutzgrundverordnung (DSGVO), die *UK General Data Protection Regulation* oder etwa das brasilianische LGPD. So navigieren Sportverbände durch ein komplexes, oft internationales Regelgeflecht, wenn sie Personendaten bearbeiten.

[6] Die vorliegende Kommentierung befasst sich primär mit den Bestimmungen des DSG. Vereinzelt wird auf Unterschiede zur DSGVO verwiesen, da gerade Sportverbände in der Schweiz häufig in den Anwendungsbereich der DSGVO fallen.

A. Persönlicher und sachlicher Anwendungsbereich des DSG

[7] Nach Art. 2 Abs. 1 **DSG** gilt das Gesetz für die Bearbeitung von Personendaten natürlicher Personen durch private Personen oder Bundesorgane. Im Gegensatz zum aDSG schützt das aktuelle DSG somit nur natürliche Personen. Juristische Personen sind nicht mehr durch das DSG geschützt, können sich aber weiterhin auf Art. 28 **ZGB**, das Gesetz gegen den unlauteren Wettbewerb und beispielsweise auch auf das Urheberrecht berufen (**BBl 2017 6972**; OFK DSG-Powell/Schönbächler, Art. 2 N 4; SHK DSG-Rudin, Art. 3 N 13).

[8] Als Personendaten gelten gemäss Art. 5 lit. a **DSG** alle Angaben, die sich auf eine bestimmte oder bestimmbare natürliche Person beziehen. Eine Person ist bestimmbar, wenn sie unmittelbar oder mittelbar identifiziert werden kann, z.B. anhand anderer Informationen oder gestützt auf den Kontext (**BBl 2017 7019**). Die rein theoretische Möglichkeit, identifiziert zu werden, reicht jedoch

noch nicht aus. Entscheidend ist der Aufwand, der ein Dritter einsetzen müsste, um die Person zu identifizieren. Ist dieser Aufwand derart gross, dass niemand diesen Aufwand auf sich nehmen würde, dann gilt die betroffene Person nicht als bestimmbar (**BBl 2017 7019**). Ausserdem liegen keine Personendaten mehr vor, solange eine vollständige und endgültige Anonymisierung erfolgt und jegliche Re-Identifizierung verunmöglicht wird (**BBl 2017 7019**). Bei den Personendaten, die von Sportverbänden bearbeitet werden, handelt es sich z.B. um Namen, Geburtsdatum und Kontaktdaten von Sportler*innen, Funktionäre*innen oder Fans, aber auch um Daten über die Nutzung von Websites, Informationen im Zusammenhang mit der Meldung von Regelverstössen, Gesundheitsdaten oder Resultate von Dopingtests.

[9] Das Gesetz findet nur auf die Bearbeitung von Personendaten Anwendung. Unter Bearbeitung ist nach Art. 5 lit. d **DSG** jeder Umgang mit Personendaten gemeint, unabhängig von den angewandten Mitteln und Verfahren. Der Begriff der Bearbeitung ist sehr weit gefasst und umfasst jede Tätigkeit in Zusammenhang mit Personendaten, wie die Erhebung, Veränderung, Löschung, Aufbewahrung oder Speicherung (OFK DSG-Glass, Art. 5 lit. d N 3 ff.; SHK DSG-Rudin, Art. 5 N 34 f.). Sobald Sportverbände also etwas mit den beispielhaft genannten Personendaten machen, wie z.B. die Speicherung von Daten zu Ticketverkäufen, das *Live-Streaming* einer Sportveranstaltung, die Entnahme von Blut oder Urin für einen Dopingtest oder die Untersuchung von Regelverstössen, bearbeiten sie Personendaten i.S.v. Art. 5 lit. d **DSG**.

[10] Die in der Schweiz domizilierten Sportverbände sind regelmässig als Verein i.S.v. Art. 60 ff. **ZGB** organisiert (Hügi, § 8 N 33.). Aus diesem Grund gelten sie als private Personen i.S.v. Art. 2 Abs. 1 **DSG**.

[11] Es bleibt zu beachten, dass das DSG nur zur Anwendung gelangt, wenn Personendaten von natürlichen Personen, wie z.B. Athleten*innen, Funktionäre*innen oder Fans, bearbeitet werden. Dementsprechend bietet das DSG keinen Schutz für juristische Personen wie Landesverbände, Kontinentalverbände oder internationale Verbände.

[12] Der sachliche Anwendungsbereich für die Bearbeitung von Personendaten durch private Personen gemäss Art. 2 DSGVO ist nahezu identisch mit dem DSG. Sofern also ein Schweizer Sportverband in den räumlichen Anwendungsbereich der DSGVO fällt und Personendaten bearbeitet, sind auch die Regeln der DSGVO anwendbar.

B. Räumlicher Anwendungsbereich des DSG

[13] Der räumliche Anwendungsbereich des DSG stützt sich auf das Territorialitäts- und Auswirkungsprinzip. Demnach ist das DSG auf Sachverhalte anwendbar, die sich in der Schweiz ereignen sowie auf diejenigen, die sich zwar im Ausland ereignen, aber Auswirkungen in der Schweiz haben (Art. 3 Abs. 1 **DSG**; OFK DSG-Dal Molin/Wesiak-Schmidt, Art. 3 N 10; SHK DSG-Rudin, Art. 3 N 4).

[14] Für die räumliche Anwendbarkeit des **DSG** auf Sachverhalte im Ausland wird ein Bezug von einer gewissen Intensität zur Schweiz verlangt, d.h. die Auswirkungen müssen in der Schweiz spürbar sein (OFK DSG-Dal Molin/Wesiak-Schmidt, Art. 3 N 9). In der Lehre wird anerkannt, dass der Anknüpfungspunkt zur Schweiz z.B. dann vorliegt, wenn eine potenzielle oder tatsächliche

Persönlichkeitsverletzung von betroffenen Personen in der Schweiz erfolgen kann (OFK DSG-Dal Molin/Wesiak-Schmidt, Art. 3 N 14). So liegt z.B. eine räumliche Anwendbarkeit vor, wenn die Daten in der Schweiz gespeichert werden, die betroffenen Personen sich in der Schweiz befinden oder sich eine Verletzung der Datensicherheit auf Personen in der Schweiz auswirkt (BGE **138 II 346**, E. 3.2.; OFK DSG-Dal Molin/Wesiak-Schmidt, Art. 3 N 15 f.).

[15] Viele internationale Sportverbände haben ihren statutarischen Sitz in der Schweiz (z.B. FIFA, FIBA, IIHF, FIS, ISU usw.) und fallen demnach für ihre Datenbearbeitungstätigkeiten unter das DSG. Dasselbe gilt für viele Kontinentalverbände (z.B. UEFA, WBSC Europe usw.) und sämtliche schweizerischen Nationalverbände (z.B. SFV, Swiss Cycling, SIHF, SAFV usw.). So erfolgt die Datenbearbeitung meistens in der Schweiz, sodass diese Sportverbände in Anwendung des Territorialitätsprinzips dem DSG unterstehen. Das DSG kommt auch auf diejenigen Sportverbände zur Anwendung, die zwar im Ausland domiziliert sind, aber z.B. die Personendaten von Sportler*innen oder von Fans mit Wohnsitz in der Schweiz bearbeiten.

C. Räumlicher Anwendungsbereich der DSGVO

[16] Gemäss Art. 3 Abs. 2 DSGVO müssen die in der Schweiz domizilierten Sportverbände die DSGVO beachten, wenn sie Personendaten von Personen bearbeiten, die sich in der EU befinden und die Datenbearbeitung dazu dient, den betroffenen Personen Waren oder Dienstleistungen anzubieten, oder das Verhalten der betroffenen Personen zu beobachten.

[17] Das Anbieten von Dienstleistungen setzt nicht zwingend den Abschluss eines Vertrages oder die Leistung einer Zahlung voraus (Beck DSGVO Kommentar-Plitz, Art. 3 N 37). Demgegenüber ist die Absicht zur Unterbreitung des Angebots an Personen in der EU erforderlich (Beck DSGVO Kommentar-Plitz, Art. 3 N 38). Hinweise dafür sind z.B. Angebote, die direkt Personen in der EU ansprechen, Preisangaben in Euro oder die Verfügbarkeit einer Website oder eines Angebots in EU-Sprachen, die nicht im Sitzstaat des Verantwortlichen gesprochen werden (z.B., wenn die Website einer Schweizer Organisation auch auf Polnisch verfügbar ist; Beck DSGVO Kommentar-Plitz, Art. 3 N 38 f.). Mit dem Begriff Verhaltensbeobachtung sind hauptsächlich sämtliche Datenbearbeitungen zum Nachvollzug der Internetaktivitäten einer Person gemeint (z.B. *Cookies*, Geolokalisierung, Aufzeichnung des Kaufverhaltens in einem Online-Shop usw.). Dennoch schliesst diese Bestimmung Verhaltensweisen, die ausserhalb des Online-Umfeldes erfolgen, nicht aus (z.B. Videoüberwachung; Beck DSGVO Kommentar-Plitz, Art. 3 N 42 f.). Dabei ist zu beachten, dass eine Beobachtung allein ausreichend ist und es nicht unbedingt erforderlich ist, dass aus der Bearbeitung Schlüsse über die entsprechenden Personen gezogen werden können. Das Ziehen solcher Schlüsse stellt jedoch ein starkes Indiz für das Vorliegen einer Verhaltensbeobachtung dar (Beck DSGVO Kommentar-Plitz, Art. 3 N 44).

[18] Die in der Schweiz domizilierten Sportverbände weisen oft einen Bezug zur EU auf. Dies trifft etwa zu, wenn ein Sportverband über seine Webseite Eintrittskarten an Fans in der EU verkauft, beispielsweise für die Spiele von Nationalmannschaften im Rahmen von Welt- oder Kontinentalmeisterschaften (z.B. verkauft die UEFA auf ihrer Webseite die Tickets für die Fussball-Europameisterschaften). Gleiches gilt, wenn z.B. ein schweizerischer Fussballclub die Tickets für die Heimspiele so verkauft, dass auch spanische Fans des Clubs sie kaufen können. Schliesslich ist

denkbar, dass ein in der Schweiz domizilierter Verband Athleten*innen, Trainer*innen oder Funktionäre*innen Onlinekurse anbietet und dabei die Personalien dieser Personen sammelt und speichert. Auch dies kann zur Anwendbarkeit der DSGVO führen. Schliesslich kann auch der Betrieb einer Website den Anwendungsbereich der DSGVO eröffnen, etwa durch den Einsatz von *Cookies*, mit denen die Internetaktivitäten von Nutzern*innen aus dem EU-Raum beobachtet werden (z.B. Erfassung und Nachverfolgung der Einkäufe, die eine Person auf dem Shop eines Verbandes tätigt).

[19] Im Ergebnis müssen die in der Schweiz domizilierten Sportverbände i.d.R. sowohl die Bestimmungen des DSG als auch diejenigen der DSGVO einhalten.

III. Welche Grundsätze gelten bei der Bearbeitung von Personendaten?

[20] Bei der Bearbeitung von Personendaten müssen stets die Grundsätze gemäss Art. 6 **DSG** eingehalten werden. Dies sind: Rechtmässigkeit (Abs. 1), Treu und Glauben (Abs. 2), Verhältnismässigkeit (Abs. 2), Zweckbindung (Abs. 3), Transparenz und Datenrichtigkeit (Abs. 5). Eine Verletzung der Datenschutzgrundsätze führt zu einer Persönlichkeitsverletzung, welche ohne Rechtfertigungsgrund (Einwilligung, überwiegende Interessen oder gesetzliche Pflicht) widerrechtlich ist (Art. 30 und 31 **DSG**) und zivilrechtliche Ansprüche seitens der betroffenen Person auslösen kann (Art. 32 **DSG**). Sofern sich die Bearbeitung von Personendaten auf eine Einwilligung der betroffenen Person stützt, ist diese nur gültig, wenn die betroffene Person vollständig aufgeklärt ist und die Einwilligung freiwillig erteilt wird. Eine Einwilligung, die unter Zwang oder aufgrund mangelnder Wahlmöglichkeiten erteilt wird (etwa bei Vorliegen eines Subordinationsverhältnisses), kann ungültig sein (Baeriswyl, SHK, Art. 6 DSG N 78 ff.). Ausserdem enthält Art. 31 Abs. 2 **DSG** eine Liste von privaten Interessen, welche greifen und im Einzelfall überwiegen können, um eine persönlichkeitsverletzende Datenbearbeitung zu rechtfertigen. Im Prinzip kommt jedes Interesse – auch wirtschaftliche Interessen – in Frage, doch müssen die betroffenen Interessen stets im Einzelfall abgewogen werden (SHK DSG-Pfaffinger, Art. 31 N 47).

A. Rechtmässigkeit

[21] Der Grundsatz der Rechtmässigkeit besagt, dass Personendaten nur rechtmässig bearbeitet werden dürfen. Dieser Grundsatz hat unterschiedliche Ausprägungen, je nachdem, ob Personendaten durch eine private Person oder durch ein Bundesorgan bearbeitet werden (SHK DSG-Baeriswyl, Art. 6 N 5; OFK DSG-Fanger, Art. 6 N 4). Bei Sportverbänden verlangt der Grundsatz der Rechtsmässigkeit, dass sie durch die Datenbearbeitung keine schweizerische Rechtnorm verletzen, welche unmittelbar oder mittelbar den Persönlichkeitsschutz bezweckt (Entscheid des Bundesverwaltungsgerichts A-3548 vom 19. März 2019, E. 5.4.4.; SHK DSG-Baeriswyl, Art. 6 N 7; OFK DSG-Fanger, Art. 6 N 4; Für Bundesbehörden bedeutet dieser Grundsatz, dass Personendaten nicht ohne gesetzliche Grundlage bearbeitet werden dürfen, statt vieler: SHK DSG-Baeriswyl, Art. 6 N 9 f.).

[22] Sportverbände müssen somit bei der Erhebung und Bearbeitung von Personendaten stets sicherstellen, dass solche Rechtsnormen nicht verletzt sind, was in der Regel unproblematisch sein wird.

B. Verhältnismässigkeit

[23] Der Grundsatz der Verhältnismässigkeit setzt voraus, dass eine Datenbearbeitung geeignet, erforderlich und zumutbar ist. Dementsprechend muss die Bearbeitung geeignet sein, den Bearbeitungszweck zu erreichen. Die Datenbearbeitung darf nur so weit gehen, als es zur Erreichung dieses Zweckes erforderlich ist, und es muss ein zumutbares Verhältnis zwischen dem Zweck der Datenbearbeitung und dem Grundrechts- bzw. Persönlichkeitseingriff bestehen; es ist immer die mildeste Form der Datenbearbeitung zu wählen (SHK DSG-Baeriswyl, Art. 6 N 22; OFK DSG-Fanger, Art. 6 N 6). Die Einhaltung des Verhältnismässigkeitsprinzips ist im Einzelfall unter Berücksichtigung sämtlicher Elemente objektiv zu bestimmen (SHK DSG-Baeriswyl, Art. 6 N 32; OFK DSG-Fanger, Art. 6 N 6). Aus dem Verhältnismässigkeitsgrundsatz werden weiter die Grundsätze der Datensparsamkeit und der Datenvermeidung abgeleitet. Diese besagen, dass nur die Personendaten erhoben und bearbeitet werden dürfen, die für den Bearbeitungszweck notwendig sind; kann der Zweck auch ohne die Bearbeitung von Personendaten erreicht werden, ist die Erhebung von Personendaten zu vermeiden (**BBl 2017 7024**; OFK DSG-Fanger, Art. 6 N 6). Ausserdem sollte der Zugriff auf die bearbeiteten Daten gemäss dem *Need-to-Know*-Prinzip eingeschränkt werden, und Personendaten müssen gelöscht werden, sofern der Zweck erreicht wurde oder deren Bearbeitung für den Zweck nicht mehr notwendig ist (OFK DSG-Fanger, Art. 6 N 6).

[24] Wenn Sportverbände Personendaten bearbeiten, sollten sie entsprechend sicherstellen, dass die erhobenen Daten auf das Minimum beschränkt werden. Ausserdem sollte der Zugriff auf die Daten streng geregelt sein, was i.d.R. mittels Zugriffskriterien und einer *Access Management Policy* sichergestellt wird. Sportverbände sollten schliesslich Archivierungs- und Löschungsrichtlinien (sog. *Retention Schedules*) implementieren, damit Daten nicht länger aufbewahrt werden als notwendig.

C. Zweckbindung und Transparenz

[25] Der Grundsatz der Zweckbindung besagt, dass Personendaten nur zu einem oder mehreren bestimmten und für die betroffene Person erkennbaren Zweck(en) beschafft werden dürfen und dass sie nur bearbeitet werden dürfen, solange die Bearbeitung noch von diesem Zweck gedeckt ist. Zunächst wird also die Erkennbarkeit des Zweckes für die betroffene Person verlangt, d.h. sie muss diesbezüglich informiert werden, die Bearbeitung muss gesetzlich vorgesehen sein oder sie muss klar aus den Umständen hervorgehen (**BBl 2017 7024** f.; SHK DSG-Baeriswyl, Art. 6 N 41; OFK DSG-Fanger, Art. 6 N 8). Zweitens ist eine Datenbearbeitung nur im Rahmen des ursprünglich bestehenden Zwecks oder eines Zwecks, der mit dem ursprünglichen Zweck vereinbar ist, zulässig (**BBl 2017 7025**; SHK DSG-Baeriswyl, Art. 6 N 38; OFK DSG-Fanger, Art. 6 N 9). Wenn ein Sportverband beispielsweise Eintrittskarten für ein Spiel verkauft und dafür Kreditkartendaten der Fans erhebt, um die Zahlung zu überprüfen, dürfen diese Daten nicht im Anschluss an eine Versicherung verkauft werden, damit diese die Fans anwerben kann. Zulässig wäre hingegen, die Kreditwürdigkeit des betreffenden Fans anhand dieser Daten zu überprüfen, weil dieser Zweck mit dem ursprünglichen Zweck (Verkauf der Eintrittskarte) vereinbar ist.

[26] Der Grundsatz der Transparenz entspringt aus dem Verhältnismässigkeitsprinzip und konkretisiert sich in den Informationspflichten gemäss Art. 19 ff. **DSG** (siehe nachstehend Rz. 35

ff.). Eine Datenbearbeitung durch Sportverbände muss für die betroffenen Personen stets erkennbar sein, d.h. die heimliche Sammlung von Daten ist unzulässig.

D. Datenrichtigkeit

[27] Der Grundsatz der Datenrichtigkeit besagt, dass es Aufgabe des Verantwortlichen ist, sich über die Richtigkeit der bearbeiteten Daten zu vergewissern und die dafür erforderlichen Massnahmen zu treffen. Daraus folgt, dass unrichtige oder unvollständige Daten berichtigt, gelöscht oder vernichtet werden müssen. Die Richtigkeit ist anhand des Bearbeitungszweckes und -umfeldes zu bestimmen (SHK DSG-Baeriswyl, Art. 6 N 63; OFK DSG-Fanger, Art. 6 N 11). Sportverbände sollten Prozesse implementieren, um die Richtigkeit von Daten zu überprüfen und die Daten zu berichtigen, sofern sie unrichtig sind (und zwar nicht nur auf Aufforderung der betroffenen Person).

E. Treu und Glauben

[28] Der Grundsatz von Treu und Glauben ist ein **Auffanggrundsatz** und besagt, dass wer Personendaten bearbeitet, sich loyal und vertrauenswürdig zu verhalten hat. Jegliches treuwidrige Handeln ist somit zu unterlassen (SHK DSG-Baeriswyl, Art. 6 N 17; OFK DSG-Fanger, Art. 6 N 5). So dürfen Personendaten namentlich nicht entgegen den objektiven Erwartungen der betroffenen Personen bearbeitet werden.

F. "Privacy-by-Design" und "Privacy-by-Default"

[29] Art. 7 **DSG** verankert darüber hinaus die Prinzipien von *Privacy-by-Design* und *Privacy-by-Default*. Diese bedeuten, dass Organisationen technische und organisatorische Massnahmen implementieren sollten, um stets sämtliche Datenschutzgrundsätze einhalten zu können sowie, dass Datenbearbeitungen grundsätzlich datenschutzfreundlich ausgestaltet werden sollten (SHK DSG-Baeriswyl, Art. 7 N 1 ff.; OFK DSG-Spacek, Art. 7 N 7 ff.).

G. Bearbeitungsgrundsätze nach der DSGVO

[30] Die Bearbeitungsgrundsätze gemäss Art. 5 DSGVO sind nahezu identisch mit den Grundsätzen gemäss Art. 6 **DSG**. Art. 5 Abs. 2 DSGVO sieht einzig noch eine Rechenschaftspflicht vor, wonach Verantwortliche stets verpflichtet sind, die Einhaltung der Grundsätze nachzuweisen. Ein zentraler Unterschied zwischen dem DSG und der DSGVO liegt indes darin, dass eine Datenbearbeitung gemäss DSG grundsätzlich zulässig ist, sofern die Datenschutzgrundsätze eingehalten werden. Eine Rechtfertigung bedarf es nur, in den Fällen gemäss Art. 30 **DSG**. Die DSGVO hingegen verlangt, dass für jede Datenbearbeitung eine Rechtsgrundlage gemäss Art. 6 DSGVO vorliegt.

IV. Welche Pflichten treffen die Verbände?

A. Einführung

[31] Welche Pflichten einen Sportverband treffen, hängt davon ab, ob der Verband sich als sog. Verantwortlicher (*Controller*) oder sog. Auftragsbearbeiter (*Processor*) qualifiziert.

[32] Ein Verantwortlicher ist eine private Person, die über den Zweck und die Mittel der Datenbearbeitung entscheidet (Art. 5 lit. j DSG). Das bedeutet, sie legt fest, welche Daten wozu bearbeitet werden, wie sie erhoben werden, wo sie gespeichert werden, mit wem sie geteilt werden, wer Zugriff auf die Daten hat etc. (OFK DSG-Lezzi, Art. 5 lit. j N 14; SHK DSG-Rudin, Art. 5 N 62). Ein Auftragsbearbeiter hingegen bearbeitet Personendaten im Auftrag eines Verantwortlichen und nicht zu eigenen Zwecken (Art. 5 lit. k DSG), was etwa bei Cloud-Anbietern, externen Lohnbuchhaltern, IT-Support, Anbieter von Newsletter-Versandtools oder CRM-Datenbanken zutrifft. Mitarbeitende gelten in der Regel nicht als (separate) Auftragsbearbeiter, sondern sind Teil des Verantwortlichen oder des Auftragsbearbeiters.

[33] In den meisten Fällen wird ein Sportverband bei der Bearbeitung von Personendaten als Verantwortlicher auftreten. Einzig, wenn ein Verband beispielsweise ein Ticketingsystem oder eine Schulungsplattform zu Integrität oder Anti-Doping für Verbandsmitglieder betreibt (siehe z.B. die **I Run Clean-Plattform**, die von World Athletics betrieben wird) oder für Verbandsmitglieder einen Cloud-Speicher zur Verfügung stellt, ist denkbar, dass der Sportverband als Auftragsbearbeiter gilt.

[34] Nachfolgend werden sämtliche Rechte und Pflichten gemäss DSG, welche ein Sportverband erfüllen muss, kurz erläutert.

B. Informationspflicht

[35] Die Informationspflicht der Verantwortlichen wird in den Art. 19 ff. DSG geregelt (den Auftragsbearbeiter trifft grundsätzlich keine Informationspflicht). Nach Art. 19 Abs. 1 DSG muss der Verantwortliche die betroffene Person angemessen über die Beschaffung von Personendaten informieren (OFK DSG-Bieri/Powell, Art. 19 N 1 f.; OK DSG-Glatthaar/Schröder, Art. 19 N 7). Das Gesetz enthält in Art. 19 Abs. 2 und 4 DSG eine Auflistung der Mindestangaben, die Gegenstand der Informationspflicht sind. Konkret müssen betroffene Personen über den Bearbeitungszweck, die Identität und die Kontaktdaten des Verantwortlichen, die Empfänger von Personendaten und allfällige Übermittlungen von Personendaten ins Ausland informiert werden (OFK DSG-Bieri/Powell, Art. 19 N 6 f.; SHK DSG-Pärli/Flück, Art. 19 N 10).

[36] Werden Personendaten bei Dritten erhoben, muss ausserdem aufgelistet werden, welche Kategorien von Personendaten bearbeitet werden (Art. 19 Abs. 3 DSG). Schliesslich müssen betroffene Personen über automatisierte Einzelentscheidungen informiert werden (Art. 21 DSG; für Beispiele von automatisierten Entscheiden siehe: Häufig gestellte Fragen, BJ, S. 31 f.; OFK DSG-Bieri/Powell, Art. 21 N 10 und Rosenthal, Rz. 107 ff.).

[37] Im Gegensatz zum DSG ist die Liste von Mindestangaben in der DSGVO länger und umfasst ausserdem die Aufklärung über die Rechte gemäss DSGVO, die Aufbewahrung der Daten, die Rechtsgrundlagen und die Datensicherheitsmassnahmen (Art. 13 und 14 DSGVO) (OFK DSG-Bieri/Powell, Art. 19 N 7; SHK DSG-Pärli/Flück, Art. 21 N 5). Aus diesem Grund richten sich Organisationen in der Schweiz oft nach dem Katalog in der DSGVO.

[38] Die Informationspflicht wird in der Regel mittels einer Datenschutzerklärung umgesetzt, die auf der entsprechenden Webseite abrufbar ist. Denn die Information muss leicht zugänglich, verständlich und transparent (aber gleichzeitig auch präzis) sein (Art. 13 DSV; OFK DSG-Bieri/Powell,

Art. 19 N 14 ff.; SHK DSG-Pärli/Fluck, Art. 19 N 17). Die Informationspflicht gilt nicht nur gegenüber Websitenutzern*innen, sondern gegenüber allen natürlichen Personen, deren Personendaten bearbeitet werden, wie z.B. Mitarbeitende, Fans, Athleten*innen etc.

[39] Es gibt Ausnahmen zur Informationspflicht, welche in Art. 20 **DSG** verankert sind. So besteht keine Informationspflicht, wenn die betroffenen Personen bereits über die Information verfügen, Geheimhaltungspflichten verletzt würden oder eine gesetzliche Bearbeitungspflicht besteht (Art. 20 Abs. 1 **DSG**; OFK DSG-Bieri/Powell, Art. 20 N 6 ff.; OK DSG-Glatthaar/Schröder, Art. 20 N 6 ff.; SHK DSG-Pärli/Flück, Art. 20 N 5 ff.). Ausserdem kann die Information eingeschränkt, verweigert oder aufgeschoben werden, wenn dadurch z.B. der Zweck der Datenbearbeitung vereitelt würde (beispielsweise bei einer laufenden Untersuchung eines Disziplinarfalls) oder wenn Interessen Dritter verletzt würden (Art. 20 Abs. 3 lit. a und b **DSG**; OFK DSG-Bieri/Powell, Art. 20 N 22 ff.; OK DSG-Glatthaar/Schröder, Art. 20 N 31 ff.; SHK DSG-Pärli/Flück, Art. 20 N 16 ff.). Des Weiteren muss keine Information erfolgen, wenn sie unmöglich oder mit unverhältnismässigem Aufwand verbunden wäre (Art. 20 Abs. 2 **DSG**). Ob ein Ausnahmetatbestand erfüllt ist, ist einzelfallabhängig zu prüfen. Die DSGVO enthält weniger weitgehende Ausnahmen zur Informationspflicht, wobei nationale Gesetze weitere Ausnahmen vorsehen können, solange sie Art. 23 DSGVO nicht verletzen (Beck DSGVO Kommentar-Gola, Art. 23 N 1 f.).

[40] Aus praktischer Sicht sollten Sportverbände also stets prüfen, über welche Personen sie Daten bearbeiten und diese Personen entsprechend informieren. Üblicherweise erfolgt dies mittels einer Datenschutzerklärung auf der Website des Verbands (siehe z.B. die Datenschutzerklärung von **FIFA**, **FIVB**, **EA**, **UEFA**, **IOC**, **UCI** oder **Swiss Football League**), oder anhand von spezifischen Datenschutzerklärungen, die im Einzelfall direkt zur Verfügung gestellt oder übermittelt werden (zu denken ist etwa an gesonderte Datenschutzbestimmungen für die Durchführung eines konkreten Grossanlasses). Um den Aufwand gering zu halten, bietet es sich für kleinere Verbände an, entweder die Datenschutzerklärungen von grösseren Verbänden als Vorlage zu nehmen oder mit Beratern zu arbeiten, die Vorlagen oder Tools anbieten, um solche Datenschutzerklärungen zu erstellen.

C. Verzeichnis der Bearbeitungstätigkeiten

[41] Nach Art. 12 Abs. 1 **DSG** müssen Verantwortliche und Auftragsbearbeiter je ein Verzeichnis ihrer Bearbeitungstätigkeiten führen. Die Mindestangaben eines solchen Verzeichnisses sind in Art. 12 Abs. 2 **DSG** aufgelistet, wobei Auftragsbearbeiter weniger Informationen aufführen müssen. Das Verzeichnis sollte die wesentlichen Informationen zu allen Datenbearbeitungen enthalten, wie z.B. Name des Verantwortlichen, Bearbeitungszwecke, Kategorien der Daten und betroffenen Personen, Empfänger der Daten, Speicherfristen, Datensicherheitsmassnahmen etc. (SHK DSG-Beariswyl, Art. 12 N 1; OFK DSG-Lezzi, Art. 12 N 4 ff.). Das EU-Datenschutzrecht sieht in Art. 30 DSGVO nahezu identische Pflichten vor.

[42] Für Sportverbände kann dieses Verzeichnis eine Vielzahl von Bearbeitungen enthalten, etwa über die Datenbearbeitung betreffend die Mitarbeitenden, Daten im Zusammenhang mit Ticketing, die Bearbeitung von Daten über verhängte Disziplinarmassnahmen oder Stadionverbote, usw. Die

konkrete Ausgestaltung hängt selbstredend von den konkreten Tätigkeiten eines jeden Verbandes ab.

[43] Gemäss Art. 12 Abs. 5 DSG i.V.m. Art. 24 DSV entfällt die Pflicht zur Führung eines Verzeichnisses für privatrechtliche Organisationen, die weniger als 250 Mitarbeitende beschäftigen, es sei denn, es werden besonders schützenswerte Personendaten in grossem Umfang bearbeitet oder es wird ein Profiling mit hohem Risiko durchgeführt (SHK DSG-Beariswyl, Art. 12 N 25 ff.; OFK DSG-Lezzi, Art. 12 N 11).

[44] Grosse Sportverbände können durchaus mehr als 250 Mitarbeitende beschäftigen, womit sie die Pflicht zur Führung eines Verzeichnisses trifft. Selbst bei weniger als 250 Mitarbeitenden kann die Pflicht greifen, insbesondere wenn der betroffene Verband Gesundheitsdaten (z.B. Ergebnis medizinischer Untersuchungen eines bestimmten Spielers bzw. einer bestimmten Spielerin oder die von Sportler*innen eingenommenen Medikamenten), Informationen zur Rasse oder Ethnie oder religiösen Einstellung von Sportler*innen, Strafregisterauszüge, Informationen zu Gerichtsverfahren, an denen Athlet*innen beteiligt sind, oder Leistungsprofile von Sportler*innen bearbeitet.

[45] In der Praxis bedarf die Erstellung eines Bearbeitungsverzeichnisses eines ziemlich grossen Aufwands. Aber auch hierfür gibt es Tools oder Vorlagen, die von kleineren Verbänden genutzt werden können. Es gibt auch keine formelle Vorgabe, wie ein solches Verzeichnis geführt werden muss, es kann elektronisch oder physisch, in einem Word-File oder einer Excel-Tabelle oder in einem Tool geführt werden. Wichtig ist einfach, dass die Liste möglichst vollständig ist und regelmässig aktualisiert ist. Nachdem das Verzeichnis einmal erstellt ist, ist die regelmässige Aktualisierung nicht mehr ein grosser Aufwand.

D. Datensicherheit und Meldung von Verletzungen der Datensicherheit

[46] Gemäss Art. 8 Abs. 1 DSG müssen der Verantwortliche und der Auftragsbearbeiter durch geeignete technische und organisatorische Massnahmen eine dem Risiko angemessene Datensicherheit gewährleisten. Technische Massnahmen können z.B. *firewalls*, Antivirusprogramme, Zugriffsbeschränkungen, Multi-Faktor-Authentifizierungen, Protokollierung von Datenbearbeitungen in Logfiles, Verschlüsselung von Daten etc. sein. Organisatorische Massnahmen umfassen z.B. das allgemeine Zugriffsmanagement, *Data Breach Response*-Prozesse, die regelmässige Überprüfung der Massnahmen oder die Schulung von Mitarbeitenden (vgl. zum Ganzen: Leitfaden zu den TOM; SHK DSG-Beariswyl, Art. 8 N 33 ff.; OFK DSG-Gordin/Egli, Art. 8 N 1 und 8 ff.). Die technischen und organisatorischen Massnahmen für automatisierte Datenbearbeitungen werden in Art. 3 DSV konkretisiert. Das Ziel besteht darin, Datensicherheitsverletzungen zu vermeiden (Art. 8 Abs. 2 DSG). Sportverbände müssen für alle Datenbearbeitungen angemessene Datensicherheitsmassnahmen einführen, diese idealerweise dokumentieren und regelmässig überprüfen und anpassen.

[47] Nach Art. 24 Abs. 1 DSG besteht eine Meldepflicht des Verantwortlichen an den Eidgenössischer Datenschutz- und Öffentlichkeitsbeauftragten (EDÖB) im Falle einer Verletzung der Datensicherheit, welche voraussichtlich zu einem hohen Risiko für die Persönlichkeit oder die Grundrechte der betroffenen Person führt. Eine Verletzung der Datensicherheit liegt gemäss

Legaldefinition von Art. 5 lit. h **DSG** vor, wenn sie dazu führt, dass Personendaten unbeabsichtigt oder widerrechtlich verlorengehen, gelöscht, vernichtet oder verändert werden oder Unbefugten offengelegt oder zugänglich gemacht werden (SHK DSG-Blonski, Art. 24 N 10 f.).

[48] Die Meldepflicht besteht jedoch nicht bei jeder geringfügigen Verletzung der Datensicherheit. Es wird verlangt, dass ein hohes Risiko für die Persönlichkeit oder die Grundrechte der betroffenen Person entsteht. Aus diesem Grund ist zu beurteilen welche Personendaten betroffen sind und wie schwer die potenziellen Auswirkungen für die betroffene Person ausfallen (OFK DSG-Bieri/Powell, Art. 24 N 3 ff.; SHK DSG-Blonski, Art. 24 N 13). Ein hohes Risiko kann beispielsweise bestehen, wenn finanzielle Risiken ausgelöst werden, ein Risiko für Identitätsdiebstahl besteht, besonders schützenswerte Daten wie z.B. Gesundheitsdaten betroffen sind etc. Das hohe Risiko ist stets einzelfallabhängig zu prüfen (OFK DSG-Bieri/Powell, Art. 24 N 5; SHK DSG-Blonski, Art. 24 N 13). Gemäss Art. 33 DSGVO muss hingegen eine Meldung erfolgen egal, wie hoch das daraus entstehende Risiko wiegt.

[49] Kommt ein Verantwortlicher zum Schluss, dass eine Meldung gegenüber dem EDÖB erfolgen muss, dann müssen die Angaben gemäss Art. 24 Abs. 2 **DSG** i.V.m. Art. 15 Abs. 1 DSV dabei gemacht werden (u.a. Art der Verletzung, Risiken, ergriffene Massnahmen). Zu beachten bleibt, dass Art. 24 Abs. 1 **DSG** besagt, dass die Meldung so rasch wie möglich erfolgen muss. Aus diesem Grund wird eine schnelle Reaktionsfähigkeit vorausgesetzt, damit die Folgen minimiert werden können. Grundsätzlich sollte eine Meldung innert 72 Stunden seit Kenntnis der Verletzung im Einklang mit der DSGVO angemessen sein (vgl. Art. 33 Abs. 1 DSGVO; OFK DSG-Bieri/Powell, Art. 24 N 7; SHK DSG-Blonski, Art. 24 N 16). Die Meldung kann per Brief oder mittels **online Formular des EDÖB** erfolgen und gestaffelt vorgenommen werden, wenn nach einer ersten Analyse noch nicht alle Informationen geliefert werden können (Art. 15 Abs. 2 DSV). Verletzungen müssen dokumentiert und während zwei Jahren seit der Meldung aufbewahrt werden (Art. 15 Abs. 4 DSV). Es empfiehlt sich jedoch, auch Verletzungen zu dokumentieren, die gemäss der internen Analyse nicht gemeldet werden müssen.

[50] Ausserdem besteht eine Meldepflicht gegenüber den betroffenen Personen, wie z.B. Athleten*innen oder Fans, wenn dies ihrem Schutz dient bzw. sie konkrete Schritte vornehmen können, um die entstandenen Risiken einzudämmen (z.B. Sperrung der Kreditkarte oder des Bankkontos, Änderung von *Login-Credentials*, Meldung an Bank oder Versicherung etc.) (Art. 24 Abs. 4 **DSG**; OFK DSG-Bieri/Powell, Art. 24 N 16; SHK DSG-Blonski, Art. 24 N 35 ff.). Gemäss Art. 34 DSGVO sind die betroffenen Personen zu informieren, wenn die Verletzung zu einem hohen Risiko für ihre Grundfreiheiten führen kann. Sowohl das DSG als auch die DSGVO sehen gewisse Ausnahmen zur Meldung gegenüber den betroffenen Personen vor, nicht aber gegenüber den Aufsichtsbehörden (Art. 24 . Abs. 5 **DSG** bzw. Art. 34 Abs. 3 DSGVO).

[51] Aus praktischer Sicht empfiehlt sich für die Sportverbände – gleich wie für jedes Unternehmen – vorgängig Handlungs- und Reaktionsprozesse (sog. *Data Breach Notification Plans* oder Notfallpläne) vorzubereiten und die Mitarbeitenden entsprechend auszubilden, damit eine Verletzung der Datensicherheit vermieden oder möglichst früh erkannt und sofort gemeldet werden kann. Bei kleineren Verbänden ist es v.a. wichtig, dass sie intern eine Person haben, die sich solchen Vorfällen annimmt und genau weiss, wer sie dann kontaktieren muss (Rechtsberater, IT-

Spezialisten, Cyber-Versicherung etc.), damit der Vorfall untersucht und, sofern notwendig, entsprechend gemeldet wird.

E. Auftragsdatenbearbeitung

[52] Eine Auftragsdatenbearbeitung liegt, wie erwähnt, bei einer Auslagerung von Datenbearbeitungsprozessen an Dritte vor (SHK DSG-Baeriswyl, Art. 9 N 1). Bei Sportverbänden kann eine solche Auslagerung beispielsweise dadurch erfolgen, dass Personendaten auf einem *Cloud-Server* gespeichert werden, ein *Tool* von einem externen Anbieter eingekauft wird, um Leistungsdaten auszuwerten und auf einem *Dashboard* zu publizieren oder wenn zur Durchführung einer Sportveranstaltung ein externes Ticketingsystem betrieben wird. In all diesen Fällen ist der jeweilige externe Anbieter ein Auftragsdatenbearbeiter des Verbandes. Eine Auftragsdatenbearbeitung kann auch gegeben sein, wenn ein lokaler Verein, der einen Wettkampf durchführt, im Auftrag eines Verbands die Resultate von Dopingtests sammelt und diese für den Verband auswertet, ohne diese Daten selber zu nutzen.

[53] Damit eine Auftragsdatenbearbeitung zulässig ist, muss gemäss Art. 9 Abs. 1 **DSG** eine vertragliche Vereinbarung getroffen werden (sog. Auftragsdatenbearbeitungsvertrag oder *Data Processing Agreement*). Darüber hinaus muss sich der Auftraggeber – also hier der Sportverband – vergewissern, dass der Auftragsbearbeiter angemessene Datensicherheitsmassnahmen implementiert hat, um die Daten, die im Auftrag des Sportverbands bearbeitet werden, genügend geschützt sind (SHK DSG-Baeriswyl, Art. 9 N 55 ff.; OFK DSG-Lezzi, Art. 9 N 13 ff.). Ausserdem darf ein Auftragsbearbeiter einen Dritten (sog. Unterbeauftragter) nur auf Genehmigung des Sportverbands hinzuziehen, was als spezifische oder allgemeine Genehmigungspflicht im *Data Processing Agreement* vereinbart wird (SHK DSG-Baeriswyl, Art. 9 N 59 f.; OFK DSG-Lezzi, Art. 9 N 16). Schliesslich darf die Auslagerung der Datenbearbeitungsprozesse gemäss Art. 9 Abs. 3 **DSG** nicht gegen gesetzliche oder vertragliche Geheimhaltungspflichten verstossen.

[54] Eine ähnliche Pflicht besteht auch in der EU (Art. 28 DSGVO). Art. 28 Abs. 3 DSGVO legt ausserdem genau fest, was im Vertrag explizit geregelt sein muss. Hierzu gehört beispielsweise das Weisungsrecht des Verantwortlichen (lit. a), die Gewährleistung der Vertraulichkeit bzw. Verschwiegenheitspflicht (lit. b), die Ergreifung der Massnahmen zur Sicherstellung der Sicherheit der Bearbeitung (gemäss Art. 32 DSGVO) (lit. c) oder die Löschung oder Rückgabe von Personendaten nach Abschluss der Auftragsbearbeitung (lit. g). In der Schweiz richten sich Organisationen oft nach den Vorgaben der EU für die Verträge, damit ein einheitlicher Standard angewendet werden kann und sowohl das DSG wie auch die DSGVO eingehalten sind. Insbesondere für europäische oder internationale Sportverbände ergibt das Sinn, da viele ihrer Mitglieder in der EU sind und ohnehin unter die DSGVO fallen.

[55] In der Praxis verwenden Sportverbände für die Auslagerung von Datenbearbeitungstätigkeiten häufig einen standardisierten Auftragsdatenbearbeitungsvertrag. Grössere Anbieter, wie Microsoft oder Salesforce, setzen oft ihre Standardverträge durch. Diese sind in der Regel schwer verhandelbar.

[56] Was oft vergessen wird, aber wichtig ist, ist dass der Sportverband einen Prozess implementieren sollte, um die Datensicherheit und Einhaltung des Datenschutzes bei seinen

Auftragsbearbeitern zu überprüfen. Dies kann anhand eines *Audits*, der Einholung von Berichten oder Informationen direkt beim Auftragsbearbeiter oder mit einem Fragebogen, welcher vom Auftragsbearbeiter ausgefüllt wird, sichergestellt werden.

F. Auslanddatentransfers

[57] Insbesondere im internationalen Sport sind sog. Auslanddatentransfers häufig. Ein solcher Transfer liegt vor, wenn Personendaten ins Ausland übermittelt, auf Servern im Ausland gespeichert werden oder wenn aus dem Ausland auf Daten in der Schweiz zugegriffen wird.

[58] Solche Auslanddatentransfers sind grundsätzlich nur zulässig, wenn im Empfängerland ein ähnliches Datenschutzniveau wie in der Schweiz besteht (Art. 16 **DSG**). Aus Schweizer Sicht besteht ein angemessener Standard z.B. in allen EU-Mitgliedstaaten, Israel, gewissen Provinzen Kanadas, dem Vereinigten Königreich oder Uruguay (eine Liste aller Länder, die gemäss DSG einen ähnliches Datenschutzniveau, wie die Schweiz haben, findet sich in Anhang 1 zur DSV). Das bedeutet, dass ein Auslanddatentransfer in diese Länder grundsätzlich zulässig ist, solange die Datenschutzgrundätze und weiteren Pflichten im DSG eingehalten sind (Anleitung Datenübermittlungen mit Auslandsbezug, S. 4).

[59] Ist eine Übermittlung in ein Empfängerland geplant, das keinen ähnlichen Datenschutzstandard wie die Schweiz hat, wie z.B. die USA, die Türkei, Australien, China, Indien usw., ist die Übermittlung nur zulässig, wenn zusätzliche Massnahmen ergriffen werden. Diese Schutzmassnahmen sind in Art. 16 Abs. 2 **DSG** aufgelistet. In der Regel empfiehlt es sich für einen Sportverband, die *EU Standard Contractual Clauses* (SCC) zu verwenden (OFK DSG-Kunz, Art. 16 N 28). Damit diese SCC aber auch nach Schweizer Recht ausreichend sind, ist zudem ein Anhang erforderlich, um bestimmte Abweichungen gemäss DSG zu integrieren (OFK DSG-Kunz, Art. 16 N 29). In diesen Fällen muss jedoch vorgängig immer auch eine Risikoanalyse durchgeführt werden, um festzustellen, welchen Risiken die betroffenen Personen ausgesetzt sind, wenn ihre Daten in das entsprechende Empfängerland übermittelt werden. Liegt keine Vereinbarung zwischen dem Verantwortlichen bzw. Auftragsbearbeiter und dem Vertragspartner vor, können Personendaten in Einzelfällen auch in solche "unsicheren" Empfängerländer übermittelt werden, wenn die betroffene Person, also z.B. ein*e Athlet*in, explizit eingewilligt hat oder wenn die Datenübermittlung für die Erfüllung eines Vertrages oder im Rahmen eines gerichtlichen oder behördlichen Verfahrens im Ausland zwingend notwendig ist (SHK DSG-Husi-Stämpfli, Art. 17 N 1 und 3 ff.; OFK DSG-Kunz, Art. 17 N 1 ff.; die vollständige Liste dieser Ausnahmen findet sich in Art. 17 **DSG**).

G. Data Protection Impact Assessments

[60] Bringt die Bearbeitung von Personendaten seitens des Verantwortlichen ein hohes Risiko für die Persönlichkeit oder die Grundrechte der betroffenen Person mit sich, trifft den Verantwortlichen die Pflicht, eine Datenschutz-Folgenabschätzung (DSFA) bzw. ein *Data Protection Impact Assessment* vorgängig durchzuführen (Art. 22 Abs. 1 **DSG**). Eine solche Abschätzung erfordert eine Datenschutz-Risikoanalyse und dient der frühzeitigen Erkennung von Datenschutzrisiken einer bestimmten Datenbearbeitung, deren Bewertung und der Festlegung der Massnahmen für die Vermeidung oder Verringerung der identifizierten Risiken (vgl. Art. 22 Abs. 3

DSG) (SHK DSG-Blonski, Art. 22 N 1; OK DSG-Harasgama/Haux, Art. 22 N 2 und 8; OFK DSG-Widmer, Art. 22 N 4).

[61] Nach Art. 22 Abs. 2 **DSG** bemisst sich das massgebende Risiko nach der Art, dem Umfang, den Umständen und dem Zweck der Bearbeitung (insb. beim Einsatz neuer Technologien). Diese Bestimmung nennt zwei beispielhafte Fälle, bei denen ein hohes Risiko bestehen kann, und zwar bei der umfangreichen Bearbeitung besonders schützenswerter Personendaten sowie bei der systematischen umfangreichen Überwachung öffentlicher Bereiche. Zudem können auch die folgenden Tatbestände ein hohes Risiko darstellen: Die Bearbeitung grosser Datenmengen, die Übermittlung von Daten in Drittstaaten, *Profiling* mit hohem Risiko, das Fällen von automatisierten Einzelentscheidungen, KI-basierte Tools oder die Zugriffsmöglichkeit auf die Daten seitens einer grossen Vielzahl von Personen (**BBl 2017 7060**; SHK DSG-Blonski, Art. 22 N 10 ff.; OK DSG-Harasgama/Haux, Art. 22 N 16; OFK DSG-Widmer, Art. 22 N 28 ff.).

[62] Diese Pflicht entfällt, wenn die Bearbeitung auf einer gesetzlichen Pflicht beruht (Art. 22 Abs. 4 **DSG**), wenn eine Zertifizierung i.S.v. Art. 13 **DSG** vorliegt oder wenn der Verantwortliche einen Verhaltenskodex i.S.v. Art. 11 **DSG** einhält, welcher die Anforderungen nach Art. 22 Abs. 5 lit. a -c **DSG** erfüllt (Art. 22 Abs. 5 **DSG**; SHK DSG-Blonski, Art. 22 N 7; OK DSG-Harasgama/Haux, Art. 22 N 31 ff.; OFK DSG-Widmer, Art. 22 N 53 ff.).

[63] Ausserdem statuiert Art. 23 Abs. 1 **DSG** eine Konsultationspflicht mit dem EDÖB, wenn sich aus der DSFA ergibt, dass die Datenbearbeitung trotz der identifizierten und implementierten Massnahmen weiterhin ein hohes Risiko für die Persönlichkeit und die Grundrechte der betroffenen Person zur Folge hat (SHK DSG-Blonski, Art. 23 N 1; OK DSG-Harasgama/Haux, Art. 23 N 1; Widmer, OFK, Art. 23 DSG N 9). Es muss keine Konsultation vorgenommen werden, sofern ein Datenschutzberater (sog. *Data Protection Officer*) ernannt und gemeldet wurde (Art. 23 Abs. 4 **DSG**) (SHK DSG-Blonski, Art. 22 N 32; OK DSG-Harasgama/Haux, Art. 23 N 25; OFK DSG-Widmer, Art. 23 N 33).

[64] Die DSGVO sieht in Art. 35 auch eine Pflicht zur Durchführung von Datenschutz-Folgenabschätzungen vor, welche ähnlich wie die Pflicht gemäss Art. 22 **DSG** ist (OK DSG-Harasgama/Haux, Art. 22 N 40). Es wird jedoch darauf hingewiesen, dass die Aufsichtsbehörden der Mitgliedstaaten der EU, eine Pflicht haben, Listen über Bearbeitungstätigkeiten, die zwingend eine DSFA verlangen, zu führen, was in der Praxis natürlich sehr hilfreich sein kann (Art. 35 Abs. 4 DSGVO; OK DSG-Harasgama/Haux, Art. 22 N 43; vgl. z.B. die **Liste des Europäischen Datenschutzbeauftragten** oder die Liste der Deutschen Datenschutzkonferenz (DSK)). Der EDÖB hat bisher keine solchen Hilfestellungen zur Verfügung gestellt.

[65] Sportverbände bearbeiten teilweise in grösserem Umfang besonders schützenswerte Personendaten, z.B. Daten über die Gesundheit i.S.v. Art. 5 lit. c Ziff. 2 **DSG** in Zusammenhang mit Doping-Kontrollen und bestimmten Verfahren (siehe nachstehend Rz. 83 ff.). Ausserdem setzen Verbände mehr und mehr KI-basierte Tools ein, woraus sich ebenfalls ein hohes Risiko ergeben kann. Daraus folgt, dass Sportverbände teilweise eine Pflicht zur Durchführung einer DSFA treffen kann und im Zweifelsfall eine solche eher durchgeführt werden sollte. Es empfiehlt sich für jeden Verband, Prozesse und Checklisten einzuführen, damit die zuständigen Abteilungen einschätzen

können, ob sie für eine bestimmte Datenbearbeitungstätigkeit eine DSFA durchführen müssen und wie sie dabei vorzugehen haben.

H. Datenschutzberater

[66] Die Ernennung von Datenschutzberatern*innen (sog. *Data Protection Officer*) im Privatbereich ist unter dem DSG freiwillig (Art. 10 Abs. 1 **DSG**). Die Aufgabe der Datenschutzberater*innen sind die Schulung und Beratung des Verantwortlichen sowie die Mitwirkung bei der Anwendung der Datenschutzvorschriften (Art. 10 Abs. 2 **DSG**; SHK DSG-Fey, Art. 10 N 17 ff.; OFK DSG-Sury, Art. 10 N 8 f.). Ein praktischer Vorteil der Ernennung von Datenschutzberatern*innen kann darin liegen, dass von der Konsultationspflicht des EDÖB im Rahmen von Datenschutz-Folgenabschätzungen abgesehen werden kann, sofern eine solche DSFA für einen Verband überhaupt relevant ist (siehe vorstehend Rz. 63).

[67] Die DSGVO statuiert in Art. 37 ff. eine Pflicht, einen Datenschutzbeauftragten zu ernennen, wenn die Kerntätigkeit des Verantwortlichen z.B. in der Durchführung von Bearbeitungsvorgängen besteht, welche eine umfangreiche regelmässige und systematische Überwachung von betroffenen Personen oder von Personendaten über strafrechtliche Verurteilungen und Straftaten umfasst (SHK DSG-Fey, Art. 10 N 9; OFK DSG-Sury, Art. 10 N 5 und 62).

[68] Aus dem Blickwinkel des **DSG** stellt sich für Sportverbände daher primär die Frage, ob sie einen bzw. eine Datenschutzberater*in einsetzen wollen. Noch wichtiger scheint aus praktischer Sicht indes die Prüfung, ob ein Sportverband die Voraussetzungen der DSGVO für die (dann obligatorische) Ernennung eines Datenschutzbeauftragten erfüllt, damit sie eine allfällige Ernennungspflicht nicht verletzen.

V. Welche Rechte haben die betroffenen Personen?

[69] Das DSG verfolgt das Ziel, die Persönlichkeit und die Grundrechte von Personen, deren Personendaten bearbeitet werden, zu schützen (vgl. Art. 1 **DSG**). Zur Verwirklichung dieses Schutzes statuiert das DSG eine Reihe von Rechten, welche den betroffenen Personen grundsätzlich zustehen, wenn Daten über sie bearbeitet werden oder ihre Persönlichkeit verletzt wird.

[70] Die Rechte der betroffenen Personen sind u.a. (vgl. zum Ganzen: Husi-Stämpfli/Morand/Sury, Rz. 486):

> Auskunftsrecht (Art. 25 ff. **DSG** und Art. 16 ff. DSV), d.h. das Recht der betroffenen Person Auskunft zu verlangen, ob Personendaten über sie bearbeitet werden und wie die Bearbeitung erfolgt, damit sie ihre übrigen Rechte ausüben kann
>
> Recht auf Datenherausgabe bzw. -übertragung (Art. 28 f. **DSG** und Art. 20 ff. DSV)
>
> Recht auf Berichtigung der Personendaten (Art. 32 Abs. 1 **DSG**)

Widerspruchsrecht zur Datenbearbeitung oder -bekanntgabe (Art. 32 Abs. 1 lit. a und b **DSG**)

Recht auf Löschung oder Vernichtung von Personendaten (Art. 32 Abs. 2 lit. c **DSG**)

Klagerecht vor einer unabhängigen Behörde (Art. 32 Abs. 2 **DSG**)

Informationsrecht und Recht zur Stellungnahme im Rahmen von automatisierten Einzelentscheidungen (Art. 21 **DSG**)

[71] Die DSGVO sieht in Art. 15-22 ähnliche Rechte vor.

[72] Sportverbände sollten entsprechende Prozesse einführen, um sicherzustellen, dass sämtliche Rechte der betroffenen Personen gewährleistet werden können, oder dass ggf. die Voraussetzungen für deren Einschränkungen klar begründet werden können, damit das Risiko minimiert wird, dass eine allfällige Verletzung stattfindet. Ausserdem sollten eine oder mehrere zuständige Personen definiert werden, welche diese Prozesse leiten, wenn eine betroffene Person ein Recht ausüben will. In der Regel müssen Anfragen zur Ausübung der Rechte innert 30 Tagen beantwortet werden.

VI. Bussen und Sanktionen

[73] Beim Vorliegen von genügenden Anzeichen für einen allfälligen Verstoss gegen die Datenschutzvorschriften eröffnet der EDÖB eine Untersuchung (Art. 49 Abs. 1 **DSG**). Bei Bagatellfällen kann der EDÖB nach Art. 49 Abs. 2 **DSG** von der Untersuchungseröffnung absehen.

[74] Wird eine Verletzung des DSG festgestellt, kann der EDÖB die vollständige oder teilweise Anpassung, Unterbrechung oder Abbruch der Bearbeitung verfügen oder die Löschung oder Vernichtung von Daten mittels verbindlicher Verfügung anordnen (Art. 51 Abs. 1 **DSG**). Daneben kann der EDÖB eine Reihe von anderen Verwaltungsmassnahmen nach Art. 51 Abs. 2 -5 **DSG** treffen.

[75] Neben den Verwaltungsmassnahmen, die administrativen und somit hauptsächlich präventiven Charakter aufweisen, enthält das DSG in den Art. 60 ff. Strafbestimmungen, welche für gewisse vorsätzliche Verhaltensweisen (auf Antrag) Bussen bis zu CHF 250'000.- androhen (Husi-Stämpfli/Morand/Sury, Rz. 570). Die folgenden Straftatbestände werden geahndet:

Verletzung von Informations-, Auskunfts- und Mitwirkungspflichten (Art. 60 **DSG**), wobei hauptsächlich auf die Pflichten nach Art. 19 , 21 und 25 -27 **DSG** verwiesen wird;

Verletzung von Sorgfaltspflichten (Art. 61 **DSG**), welche aus Art. 8 f. und 16 f. **DSG**

entspringen;

Verletzung der beruflichen Schweigepflicht (Art. 62 DSG), welche die Offenbarung von geheimen Daten betrifft;

Missachten von Verfügungen der EDÖB oder Entscheide der Rechtsmittelinstanzen (Art. 63 DSG).

[76] Die in der DSGVO vorgesehenen Sanktionen sind erheblich strenger. Art. 83 DSGVO legt fest, dass Bussen bis zu EUR 20'000'000.00 oder 4% des gesamten weltweit erzielten Jahresumsatzes betragen können. Dies liegt daran, dass in der EU die Organisation – der Verantwortliche oder der Auftragsbearbeiter – selbst gebüsst wird und in der Schweiz die verantwortliche natürliche Person innerhalb der Organisation.

VII. Ausgewählte Themen

[77] Die nachfolgenden Ausführungen befassen sich mit ausgewählten Themen und Fragestellungen, welche sich im Zusammenhang mit Sport und Datenschutz stellen können. Konkret behandelt werden der Austausch von Daten zwischen Verbänden, der Kampf gegen Doping, die Datenbearbeitung bei gemeldeten Regelverstössen im Zusammenhang mit Missbrauchsfällen, sowie ausgewählte Themen zum Kampf gegen Hooliganismus.

A. Austausch von Daten zwischen dem Dachverband und lokalen Verbänden, Vereinen oder Mitgliedern

[78] Aus verschiedenen Gründen tauschen Sportverbände oder -Vereine sowie deren Mitglieder mit ihren Dachverbänden Personendaten aus. Dieser Datenaustausch wird teilweise sogar zwingend verlangt und in den Statuten oder Reglementen des Verbands verankert. Auch ein derartiger Austausch von Daten ist datenschutzrechtlich relevant und muss den datenschutzrechtlichen Anforderungen genügen.

[79] So muss der Austausch von Personendaten zunächst mit sämtlichen Datenschutzgrundsätzen vereinbar sein, und es gilt, die "Spielregeln" im Umgang mit den ausgetauschten Daten in einem Datenaustauschvertrag oder in Datenschutzklauseln in einem anderen Vertrag zwischen dem Datenempfänger und dem Datenexporteur zu vereinbaren. Dies, obwohl sich aus dem Gesetz keine solche Pflicht ergibt. Ziel dieser Datenschutzklauseln oder Datenaustauschverträge ist es, sicherzustellen, dass die Datenschutzgrundsätze eingehalten werden (denn als Verein dürfen Personendaten nur austauscht werden, wenn z.B. die Zweckbindung eingehalten wird und der Austausch verhältnismässig und transparent ist), die Rollen der Parteien geklärt sind sowie der Umfang der Datenbearbeitung festgelegt ist und die Parteien gegenseitige Informations- und Unterstützungspflichten vereinbart haben. So können diese Verträge bestimmen, wozu die Daten ausgetauscht werden sollen, wer für die Information der betroffenen Personen und die Gewährung der Datenschutzrechte der betroffenen Personen zuständig ist, wer die Einwilligung in die Bearbeitung und den Austausch der Daten einholen muss, wie der Zugriff auf die Daten geregelt

sein soll, ob die Daten ins Ausland übermittelt werden dürfen, ob Dritte hinzugezogen werden dürfen und wie sich die Parteien, bei Anfragen von betroffenen Personen oder Behörden oder im Falle von einem *Data Breach* gegenseitig informieren und unterstützen sollen. Im Anhang zu solchen Verträgen werden typsicherweise die Kategorien der bearbeiteten Daten, die Art der betroffenen Personen sowie die Rollen der beteiligten Personen festleget – wie z.B. ob nur der Dachverband ein Verantwortlicher ist und die anderen Parteien nur Auftragsbearbeiter oder auch Verantwortliche oder gar gemeinsame Verantwortliche sind. Darüber hinaus müssen die Parteien die Voraussetzungen für die Auftragsdatenbearbeitung gemäss Art. 9 **DSG** sowie für Auslanddatentransfers gemäss Art. 16 und 17 **DSG** einhalten, wenn sie gegenseitig Personendaten austauschen.

[80] All diese Punkte können unterschiedlich ausgestaltet werden und hängen vom konkreten Anwendungsfall ab:

> Werden Daten im Rahmen einer bestimmten Sportveranstaltung ausgetauscht, können die datenschutzrechtlichen Klauseln direkt in den jeweiligen vertraglichen Vereinbarungen vereinbart werden.
>
> Wenn Daten in einer eher allgemeinen Weise und für unterschiedliche Zwecke und Ziele ausgetauscht werden, empfiehlt es sich, den Austausch in einem Rahmenvertrag, einem sog. Datenaustauschvertrag (oder *Data Sharing Agreement*) zu regeln.
>
> Wenn z.B. ein lokaler Verein ein Ticketing-System für die anderen Mitglieder im Rahmen einer Veranstaltung betreibt und zur Verfügung stellt, kann es sein, dass dieser lokale Verein als Auftragsdatenbearbeiter qualifiziert und deshalb ein Auftragsdatenbearbeitungsvertrag (*Data Processing Agreement,* DPA) zwischen allen Parteien abgeschlossen werden muss (Art. 9 **DSG**) (die EU Kommission stellt einen **Mustervertrag** für solche Verträge gemäss Art. 28 DSGVO zur Verfügung).
>
> Wenn im Rahmen der Zusammenarbeit Daten ins Ausland übermittelt werden, muss das Datenschutzniveau im Ausland geprüft werden, und es sind je nach Ausgang dieser Prüfung zusätzliche Massnahmen für den Auslandtransfer zu ergreifen.

[81] Die verschiedenen Verträge können kombiniert werden und somit können das DPA oder die SCC in einen Vertrag integriert werden oder als Anhang zum Hauptvertrag ausgestaltet werden.

[82] In der Praxis kommt es auch vor, dass ein Verband ein Reglement erlässt, das den Austausch bestimmter Daten mit dem Verband und/oder zwischen den Verbandsmitgliedern verbindlich vorschreibt. Deckt ein solches Reglement alle der vorstehend genannten Punkte ab, kann auch ein solches Reglement die erforderlichen rechtlichen Rahmenbedingungen für den Datenaustausch schaffen.

B. Der Kampf gegen Doping

[83] Umgangssprachlich besteht Doping im Einsatz von Mitteln oder Methoden, um die Leistungsfähigkeit von Athleten*innen zu steigern und ihnen damit einen unrechtmässigen Wettkampfvorteil zu verschaffen (Jäggi, § 25 N 2).

[84] Mit dem Kampf gegen Doping werden legitime Interessen der Verbände, der Sportler*innen sowie der Allgemeinheit verfolgt (insb. Schutz der Integrität des Sports und Schutz der Gesundheit der Sportler*innen sowie Wahrung ihrer Vorbildfunktion; Nolte, S. 309). Zahlreiche Länder haben staatliche Anti-Doping-Gesetze verabschiedet. Auch die Schweiz hat im Sportförderungsgesetz (SpoFöG) gewisse gesetzliche Grundlagen für den Kampf gegen Doping geschaffen (Art. 19 ff. **SpoFöG**; siehe nachstehend Rz. 89 ff.).

[85] Auf Ebene der Sportverbände gelten ebenfalls strikte Regeln. Die *World Anti-Doping Agency* (WADA) ist eine internationale Organisation, die als Stiftung unter schweizerischem Recht organisiert ist, welche Doping primär durch den Erlass einer weltweit einheitlichen Regelung, dem sog. *World Anti Doping Code* (**WADA-Code**), und anhand sog. *International Standards* bekämpft (Hügi, § 26 N 6). Die Umsetzung der von der WADA geschaffenen Regeln obliegt den *National Anti-Doping Organizations* (NADOs) sowie den nationalen und internationalen Sportverbänden (Hügi, § 25 N 12 und 18; vgl. zur gesamten Thematik von Anti-Doping: Contat et al., S. 159 ff.).

[86] Doping wird in Art. 1 WADA-Code als Verletzung einer der Anti-Doping-Regeln nach Art. 2.1 bis Art. 2.11 WADA-Code definiert. In der Praxis wohl häufigstes Beispiel ist das Vorhandensein einer verbotenen Substanz in der Dopingprobe von Athleten*in (Art. 2.1 WADA-Code).

[87] Um bestimmen zu können, ob eine Verletzung der Anti-Doping-Regeln begangen worden ist, müssen Dopingkontrollen durchgeführt werden. Die Durchführung dieser Tests setzt das Vorhandensein und Bearbeiten von bestimmten Informationen voraus, welche in der Regel allesamt Personendaten sind (z.B. Name, Vorname, Aufenthaltsort, Wohnort eines Athleten*in usw.). Oft umfassen sie auch besonders schützenswerte Personendaten, beispielsweise Informationen über Verletzungen, Krankheiten und deren Behandlung durch Medikamente (Schmidt/Hermonies, S. 340; Striegel, S. 6 f.). Athleten*innen müssen überdies Informationen über ihre sog. *Whereabouts* teilen, d.h. sie müssen ihre wöchentlichen (Sports-)Pläne offenlegen sowie mitteilen, an welchen Wettkämpfen sie teilnehmen (Nolte, S. 309 f.). Auch derartige Informationen stellen grundsätzlich immer Personendaten dar. Dadurch soll ermöglicht werden, dass auch ungeplante Kontrollen und Stichproben der Athleten*innen vorgenommen werden können, damit effektiv gegen Doping vorgegangen werden kann.

[88] Aus datenschutzrechtlicher Sicht ist insbesondere die Thematik betreffend die Pflicht zur Bekanntgabe der sog. *Whereabouts* beachtenswert. Datensammlungen, wie sie im Rahmen der *Whereabouts* erstellt werden, können unter Umständen als *Profiling* mit hohem Risiko (i.S.v. Art. 5 lit. g **DSG**) qualifizieren, da aus diesen Informationen weitreichende Einblicke in wesentliche Aspekte der Persönlichkeit der betroffenen Athleten*innen möglich sind und allenfalls auch Daten aus verschiedenen Quellen zusammengeführt werden (vgl. OK DSG-Glatthaar/Schröder, Art. 5 lit. f und g N 17 ff., für eine detaillierte Erläuterung der Definition von *Profiling* mit hohem Risiko). Es stellt sich somit die Frage, ob eine derart weitreichende Datenbearbeitung verhältnismässig ist, d.h.,

ob die Sammlung all dieser Informationen über die Athleten*innen geeignet, erforderlich und zumutbar sind, um wirkungsvoll gegen Doping im Sport vorzugehen. Wird diese Frage verneint, ist zu prüfen, ob ein gültiger Rechtfertigungsgrund vorliegt. Unseres Erachtens sind Rechtfertigungen auf drei Ebenen möglich, doch ist zu beachten, dass zu den entscheidenden Fragestellungen mehrheitlich noch keine Rechtsprechung ergangen ist.

1. Gesetzliche Grundlage

[89] Die Schweiz hat sich sowohl dem Übereinkommen gegen Doping des Europarats (Europaratsübereinkommen; seit dem 1. Januar 1993 für die Schweiz in Kraft, AS 1993 1238) sowie dem internationalen Übereinkommen gegen Doping im Sport des UNESCO (UNESCO-Übereinkommen; seit dem 1. Dezember 2008 für die Schweiz in Kraft, **AS 2009 521**) angeschlossen, welche auf internationaler Ebene wegweisend für die Dopingbekämpfung waren.

[90] Zudem hat die Schweiz das Sportförderungsgesetz erlassen, welches festlegt, dass der Bund Massnahmen unterstützt und ergreift, um gegen den Missbrauch von Doping im Sport vorzugehen (Art. 19 Abs. 1 **SpoFöG**). Dabei wird auch festgehalten, dass der Bund die Kompetenz, Massnahmen gegen Doping zu ergreifen, an nationale Agenturen übertragen kann (Art. 19 Abs. 2 **SpoFöG**). Das SpoFöG besagt ausserdem, dass Dopingkontrollen von Sportverbänden, Agenturen oder Veranstaltern von Sportanlässen durchgeführt werden dürfen (Art. 21 Abs. 2 **SpoFöG**) und schafft eine gesetzliche Grundlage für die Bearbeitung und den Austausch von besonders schützenswerten Daten, wie Gesundheitsdaten, auf nationaler und internationaler Ebene (Art. 21 Abs. 3 sowie 25 Abs. 1 **SpoFöG**). Das Gesetz hält jedoch ausdrücklich fest, dass die Daten grenzüberschreitend nur ausgetauscht werden dürfen, wenn dies für die Bearbeitung von medizinischen Anträgen oder zur Ausstellung von medizinischen Bewilligungen, zur Meldung von Resultaten von Dopingkontrollen und zur Planung, Koordination und Durchführung von Dopingkontrollen bei den Athleten*innen notwendig ist und diese bzw. dieser dem Austausch ausdrücklich zugestimmt hat (siehe nachstehend Rz. 95 ff.; Art. 25 Abs. 2 **SpoFöG**). Im letzteren Fall dürfen dabei nur Personalien und sachliche sowie örtliche Hinweise geteilt werden, aber nicht mehr (Art. 25 Abs. 3 **SpoFöG**). Ausserdem hat die zuständige Stelle in der Schweiz sicherzustellen, dass die Daten keinen unberechtigten Dritten zugänglich gemacht werden und die Vorgaben für Auslanddatentransfers gemäss Art. 16 und 17 **DSG** eingehalten werden (siehe vorstehend Rz. 57 ff.).

[91] Entsprechend liegt für die Bearbeitung von Personendaten im Rahmen von Dopingtests eine generelle gesetzliche Grundlage vor, welche gemäss den Prinzipien der Verhältnismässigkeit und Zweckbindung ausgestaltet ist. Diese gesetzliche Grundlage dürfte zwar relativ umfassend sein und auch die Bearbeitung von *Whereabouts*-Informationen abdecken, jedoch muss auch, wenn eine gesetzliche Grundlage vorliegt, eine Datenbearbeitung stets verhältnismässig sein (siehe nachstehend Rz. 92 ff.).

2. Überwiegendes Interesse und Verhältnismässigkeit

[92]

Unabhängig vom Vorliegen einer gesetzlichen Grundlage spricht sehr viel dafür, dass sich Doping-Kontrollen sowie die damit einhergehende Datenbearbeitung (inkl. Sammlung der *Whereabouts*-Informationen) auf ein überwiegendes öffentliches und privates Interesse stützen können, namentlich auf den Schutz der Integrität des Sports, die Ausgeglichenheit und Fairness sportlicher Wettkämpfe, die Vorbildfunktion des Sports für die Jugend, die Gesundheit der Athleten*innen usw. (vgl. hierzu: Contat et al., S. 160). Doch auch dann muss die Bearbeitung verhältnismässig sein.

[93] So stellt sich auch hier die Frage, ob eine derart umfassende Datenbearbeitung, wie sie die Sammlung von *Whereabouts*-Informationen darstellt, in jedem Fall verhältnismässig ist. Athlet*innen müssen häufig relative genaue Informationen über ihren Aufenthaltsort sowie detaillierte weitergehende Informationen zu ihren sportlichen Aktivitäten zur Verfügung stellen. Aus rechtlicher Sicht zu prüfen ist, ob diese Datenbearbeitung geeignet, erforderlich und zumutbar ist, um Doping wirkungsvoll zu bekämpfen und ob das Interesse an einem wirkungsvollen Kampf gegen Doping gegenüber dem Interesse der einzelnen Athleten*innen am Schutz ihrer Persönlichkeit zu überwiegen vermag.

[94] Klar ist zunächst, dass die Sammlung der *Whereabouts*-Informationen geeignet ist, Doping zu bekämpfen, denn sie erlaubt unangekündigte Tests, unabhängig vom Aufenthaltsort der jeweiligen Athleten*innen. Auch die Frage, ob solche weitreichende Datenbearbeitungen erforderlich sind, ist wohl zu bejahen, da nur mit überraschenden Tests auch ausserhalb von Wettkämpfen sichergestellt werden kann, dass auch Doping mit Kleinstmengen *(micro-dosing),* das oft und gerade in Trainingsphasen stattfindet, effektiv bekämpft werden kann. Auch wenn Doping-Kontrollen vor, während und nach Sportveranstaltungen durchgeführt werden können, ist unerlässlich, dass Athleten*innen auch während ihren Trainingseinheiten getestet werden können. Derartige Tests sind nur möglich, wenn die Kontrolleure*innen eben über die genauen *Whereabouts*-Informationen verfügen. Es lässt sich nicht verneinen, dass die Systematik der *Whereabouts*-Informationen insgesamt eine Datenbearbeitung in erheblichem Umfang und, damit einhergehend, eine nicht unbedeutende Einschränkung von Persönlichkeitsrechten darstellt. Für einen wirkungsvollen Kampf gegen Doping ist sie jedoch sicherlich erforderlich. Zuletzt stellt sich also die Frage, ob diese weitgehende Datenbearbeitung auch zumutbar ist. Auch wenn dies unter einem strengen Datenschutzgesichtspunkt nicht unbedingt eindeutig zu bejahen ist, steht doch fest, dass unangekündigte Tests bzw. Stichproben stets möglich sein müssen, auch wenn damit *Profiling* betrieben wird und Athleten*innen in ihrer Freiheit dadurch eingeschränkt werden.

3. Einwilligung

[95] Der WADA-Code statuiert das Recht der WADA zur Bearbeitung von Personendaten in Art. 6.8 und dasjenige der *Anti-Doping Organizations* in Art. 14.6. Die nationalen Sportverbände sind als *signatories* des WADA-Code verpflichtet, ihre Mitglieder statutarisch den WADA-Regeln zu unterwerfen. Daraus folgt, dass in den meisten Fällen eine statutarische Klausel vorhanden ist, welche die Athletene*innen an die Doping-Regeln (mittelbar) bindet, damit sie an den nationalen und internationalen Wettkämpfen teilnehmen können.

[96] Nicht nur auf mitgliedschaftlichem, sondern auch auf vertraglichem Weg können die Sportverbände die Einwilligung der Athleten*innen für die Durchführung von Doping-Kontrollen

einholen, z.B. in den Arbeitsverträgen von Fussballer*innen (**AVB zum Arbeitsvertrag für Nichtamateur-Spieler der Klubs des SFV**) (Nolte, S. 311 f.). Die Athleten*innen bestätigen damit auch ihre Unterstellung unter den WADA-Code.

[97] Dabei ist zu beachten, dass eine Einwilligung nach Art. 6 Abs. 6 **DSG** nur dann gültig ist, wenn sie für eine bestimmte Bearbeitung nach angemessener Information freiwillig erteilt wird. Die Freiwilligkeit besteht, wie oben erwähnt, darin, dass die Entscheidung der betroffenen Person ohne Druck erfolgt, d.h. wenn der Nachteil ohne Einwilligung keinen unzulässigen Druck auf die Person darstellt (SHK DSG-Baeriswyl, Art. 6 N 94 f.).

[98] Aus allgemeiner Sicht dürfte generell eine informierte und ausdrückliche Einwilligung vorliegen, wenn Sportler*innen im Rahmen eines Vertragsschlusses oder bei der Registrierung bzw. Lizenzierung als Profisportler*in einer Datenbearbeitung zustimmen. Es stellt sich jedoch die Frage, ob diese Einwilligung auch tatsächlich freiwillig erfolgt. Athleten*innen können in der Regel nicht wählen, ob sie sich den jeweiligen Regelwerken unterstellen wollen, wenn sie an einer bestimmten Sportveranstaltung teilnehmen wollen und eine professionelle Karriere verfolgen wollen (Nolte, S. 311 f.). Allerdings wissen insb. Profisportler*innen heutzutage sehr genau, dass sich alle Athleten*innen denselben Regeln unterstellen müssen, einschliesslich den Regeln zum Kampf gegen Doping.

C. Meldung von Vorfällen

[99] In den letzten Jahren wurden vermehrt physische wie auch psychische Missbrauchsfälle in verschiedenen Sportarten öffentlich bekannt. Aus diesem Grund haben und hatten zahlreiche Sportverbände Plattformen, Meldestellen oder Kanäle geschaffen, über welche Missbrauchsfälle gemeldet werden können (siehe z.B. **BKMS System**).

[100] Seit 2022 haben verschiedene Verbände mit Fokus auf die Schweiz jedoch ihre Disziplinarbefugnis an die Swiss Sport Integrity (SSI) abgegeben. Diese untersucht nun t unter dem Dachverband Swiss Olympic die gemeldeten Regelverstösse und erstellt Berichte samt Anträgen (d.h. Sanktion oder Verfahrenseinstellung), welche der Disziplinarkammer des Schweizer Sports (DK) vorgelegt werden. Die DK fällt dann schliesslich einen Entscheid über eine allfällige Massnahme (siehe Art. 5.1 ff. des **Ethik-Statuts des Schweizer Sports vom Swiss Olympic**; Ethik-Statut). Ab Sommer 2024 wird das Schweizer Sportgericht die DK ersetzen und für die Urteilsfällung zuständig sein. (**Medienmitteilung des Bundesrats zum Schutz vor Gewalt im Sport: Bundesrat schafft verbindliche Vorgaben für ethisches Verhalten**).

[101] Ziel dieser Massnahmen und Meldestellen ist es, alle Athlet*innen sowie insgesamt die Integrität des Sports zu schützen und einen sicheren und regelkonformen Sport zu fördern.

[102] Im Rahmen der Meldung solcher Vorfälle können Personendaten, einschliesslich besonders schützenswerte Personendaten, gesammelt und bearbeitet werden. Zu den besonders schützenswerten Personendaten gehören z.B. Gesundheitsdaten (z.B. Daten über Verletzungen, körperliche Übergriffe, sexuelle Übergriffe, Missbrauch, Belästigung usw.), Daten, die Straftaten oder Verurteilungen betreffen (z.B. Untersuchungen zu sexuellen/körperlichen Übergriffen, Belästigungen usw.) oder ausnahmsweise Daten, die sich auf das Sexualleben oder die sexuelle Ausrichtung einer Person beziehen (dazu gehören insb. Meldungen über sexuelle Übergriffe).

[103] Wenn sich die erhobenen Daten direkt auf die meldende Person beziehen, z.B. den Athleten*innen, ist dies grundsätzlich unproblematisch und ein Verband kann sich, soweit notwendig, auf die Einwilligung dieser Person zur Bearbeitung ihrer Daten berufen. Wenn jedoch eine Drittperson eine Meldung vornimmt, wie z.B. die Eltern von noch nicht volljährigen Sportler*innen, oder die meldende Person auch Informationen über einen Dritten, wie z.B. den Täter, offenlegt, muss geprüft werden, ob die Bearbeitung dieser Daten rechtmässig und mit Datenschutzgrundsätzen vereinbar ist. Im Rahmen der SSI stellen sich ausserdem dieselben Fragen, wenn die Verbände gestützt auf Art. 5.2 des Ethik Statuts Meldungen und Vorfälle der SSI weitergeben (müssen) und dabei allfällige besonders schützenswerte Daten von den Athlet*innen oder Dritten betroffen sind. Auch in diesen Fällen sind die Datenschutzgrundsätze stets einzuhalten.

Rechtfertigungsgründe gemäss DSG

[104] In der Schweiz dürfen Personendaten bearbeitet werden, wenn die Datenschutzgrundsätze eingehalten werden (siehe vorstehend Rz. 20 ff.). Wenn diese Grundsätze nicht erfüllt sind oder besonders schützenswerte Daten an Dritte weitergegeben werden, ist die Datenbearbeitung bzw. die Datenweitergabe mittels (ausdrücklicher) Einwilligung, gesetzlicher Pflicht oder einem überwiegenden privaten oder öffentlichen Interesse zu rechtfertigen (Art. 31 Abs. 1 **DSG**). In der EU bedarf jede Datenbearbeitung einer Rechtsgrundlage gemäss Art. 6 DSGVO (siehe vorstehend Rz. 30).

[105] Im Rahmen derartiger Meldungen stellt sich somit die Frage, ob die Bearbeitung von Personendaten über Dritte durch die Verbände oder für die Schweiz spezifisch die Weitergabe der Daten durch die Verbände an die SSI insbesondere mit den Grundsätzen der Transparenz, Zweckbindung und Verhältnismässigkeit vereinbar ist. Diese Frage ist zu bejahen, solange folgende Massnahmen vom Verband umgesetzt werden:

> In den Verbandsregeln muss klar festgehalten sein, dass Personendaten, wie z.B. Name, Kontaktadresse, meldender Vorfall, Gesundheitsdaten oder potenziell strafrechtlich relevante Informationen direkt oder indirekt gesammelt werden können, um die Integrität des Sports zu schützen und einen sicheren und regelkonformen Sport zu fördern. Es ist klar zu umschreiben, was mit den Daten gemacht wird (z.B. Untersuchung des Vorfalls, Austausch mit und Offenlegung gegenüber anderen Verbandsmitgliedern und dem Dachverband bzw. SSI, Erstellung eines Berichts, Erlass von Sanktionen, evtl. Publikation der Sanktionen zusammen mit Namen und Funktion in einem Register, wobei dies teilweise heikel sein kann) und die übrigen Informationen gemäss der in Art. 19 **DSG** verankerten Informationspflicht.
>
> Die Daten dürfen nur für die beschriebenen Zwecke verwendet werden. Dafür sollte der Verband klare interne Richtlinien für die Gremien oder Organisationen im Umgang mit

den erhobenen Personendaten implementieren.

Darüber hinaus ist die Verhältnismässigkeit zu wahren, indem z.B. der Zugriff auf die erhobenen Daten nur einem eingeschränkten Kreis von Personen zugänglich ist, die Daten nur mit dem Dachverband oder anderen Mitgliedern geteilt wird, sofern das absolut notwendig ist und die Daten gelöscht werden, sobald sie nicht mehr gebraucht werden.
Bei der Meldung von Vorfällen wird es hingegen schwierig sicherzustellen, dass nur die Daten erhoben werden, die für die Untersuchung notwendig sind, da es der meldenden Person i.d.R. offensteht, zu entscheiden, was sie alles in der Meldung aufnimmt. In dieser Hinsicht ist es also möglich, dass die Verhältnismässigkeit nicht von Vorneherein stets gewahrt werden kann. In solchen Fällen gilt jedoch zudem, dass die Bearbeitung dieser Daten aller Regel nach ohnehin im überwiegenden Interesse des Verbands oder gar der Öffentlichkeit liegt, nämlich im Interesse, einen sicheren und integren Sport zu gewährleisten und weitere Vorfälle zu verhindern bzw. Regelverstösse wirkungsvoll sanktionieren zu können.

In Bezug auf die Weitergabe der gemeldeten Vorfälle inkl. der darin enthaltenen Personen an die SSI muss ausserdem sichergestellt werden, dass die Weitergabe zulässig ist. Dies ist insbesondere wichtig, weil die Weitergabe von besonders schützenswerten Daten an Dritte gemäss Art. 30 Abs. 2 lit. c **DSG** gerechtfertigt sein muss. In Frage kommt entweder die Einwilligung der betroffenen Personen für die Weitergabe oder ein überwiegendes Interesse des Verbands die übergreifenden Verbandsregeln einzuhalten und am Schutz der betroffenen Athlet*innen und der Integrität des Sports. U.E. sollte das überwiegende Interesse greifen, denn es wird schwierig sein die Einwilligung aller betroffenen Personen (insbesondere der Personen, die etwas falsch gemacht haben) in die Weitergabe einzuholen.

2. Rechtfertigungen gemäss DSGVO

[106] Die oben genannten Punkte gelten grundsätzlich auch unter der DSGVO. In der EU braucht es jedoch, wie bereits erwähnt, immer eine Rechtsgrundlage gemäss Art. 6 DSGVO (Einwilligung, gesetzliche Pflicht, überwiegendes Privatinteresse, Notwendigkeit für die Abwicklung oder den Abschluss eines Vertrages, überwiegendes öffentliches Interesse oder Notwendigkeit für den Schutz von lebenswichtigen Interessen etc.), um Personendaten rechtmässig zu bearbeiten. Die Rechtsgrundlagen in Art. 6 DSGVO stimmen im Grunde genommen mit den Rechtfertigungsgründen von Art. 31 Abs. 1 **DSG** überein. Hier macht es jedoch einen Unterschied, ob es sich um Personendaten oder besonders schützenswerte Daten handelt. U.E. lässt sich die Bearbeitung und Weitergabe der Personendaten, die nicht besonders schützenswert

sind, auch wiederum durch die Einwilligung (wenn eine betroffene Person einen Vorfall selber meldet, aber nur in Bezug auf ihre eigenen Daten) und dem überwiegenden Interesse des Verbands am Schutz der Integrität des Sports und die Förderung eines sicheren und regelkonformen Sports für die Personendaten Dritter, die in einer Meldung enthalten sind, rechtfertigen. Dabei sind die oben erwähnten Massnahmen stets zu berücksichtigen.

[107] Art. 9 Abs. 2 DSGVO zählt die Rechtsgrundlagen für die Bearbeitung von besonders schützenswerten Daten auf. Diese sind nicht mit den Rechtsgrundlagen nach Art. 6 DSGVO identisch und ein überwiegendes Interesse kann in Bezug auf die Daten der Drittpersonen, wie z.B. Gesundheitsdaten, nicht als Rechtsgrundlage dienen. Für die Bearbeitung von besonders schützenswerten Daten liegt auch keine ausdrückliche Einwilligung der betroffenen Dritten vor. Aus diesem Grund muss für diese Fälle eine andere Rechtsgrundlage herangezogen werden, sofern die DSGVO anwendbar ist. In Frage kommen aus unserer Sicht die Folgenden:

> Zweckgebundene interne Bearbeitung durch Stiftungen, Vereine oder gemeinnützige Organisationen (nachfolgend: «Interne Bearbeitung durch den Verein»; Art. 9 Abs. 2 lit. d DSGVO)
>
> Zur Geltendmachung, Ausübung oder Verteidigung von Rechtsansprüchen (nachfolgend: «Durchsetzung von Rechtsansprüchen»; Art. 9 Abs. 2 lit. f DSGVO)
>
> Erhebliches öffentliches Interesse (nachfolgend: «Erhebliches öffentliches Interesse»; Art. 9 Abs. 2 lit. g DSGVO)

a. Interne Bearbeitung durch den Verein

[108] Art. 9 Abs. 2 lit. d DSGVO erlaubt die Bearbeitung von besonders schützenswerten Daten, wenn (i) geeignete Garantien zum Schutz der Personendaten umgesetzt sind, (ii) eine politisch, weltanschaulich, religiös oder gewerkschaftlich ausgerichtete Stiftung, Vereinigung oder sonstige Organisation ohne Gewinnerzielungsabsicht die Daten bearbeitet, (iii) die Bearbeitung im Rahmen ihrer rechtmässigen Tätigkeiten erfolgt, (iv) sich die Bearbeitung ausschliesslich auf die Mitglieder oder ehemalige Mitglieder der Organisation oder auf Personen, die im Zusammenhang mit deren Tätigkeitszweck regelmässige Kontakte mit ihr unterhalten, bezieht und (v) die Daten nicht ohne Einwilligung der betroffenen Personen nach aussen offengelegt werden (Beck DSGVO Kommentar-Schulz, Art. 9 N 29 f.).

[109] Unserer Ansicht nach können die gegründeten Gremien oder Organisationen der Sportverbände, welche die Meldungen von Vorfällen entgegennehmen, als gemeinnützige Organisationen qualifiziert werden und ihr Zweck ist es, Vorfälle zu untersuchen und allfällige Sanktionen bzw. Disziplinarmassnahmen auszusprechen. Somit würde die Bearbeitung im Zweck des Gremiums oder der Organisation liegen. Auch lässt sich unseres Erachtens gut argumentieren, dass sowohl die Sportler*innen als auch ihren Manager*innen oder Trainer*innen als Mitglieder oder Personen gelten, die regelmässig mit diesen Gremien und Organisationen Kontakt halten, auch wenn dies allenfalls nur indirekt über die Verbandsregeln sichergestellt ist. Problematisch

könnte das Verbot des Austauschs der Daten mit Dritten ohne gültige Einwilligung der betroffenen Person sein, da es oft vorkommt, dass solche Meldungen im Rahmen der Untersuchung mit lokalen Verbandsmitgliedern geteilt werden. Dies könnte jedoch im Rahmen der Verträge zwischen den lokalen Verbänden und den jeweiligen Athleten*innen, Manager*innen, Trainer*innen etc. geregelt werden, wobei sich dann auch hier wieder die Frage stellt, ob eine so eingeholte Einwilligung freiwillig wäre.

b. Durchsetzung von Rechtsansprüchen

[110] Gemäss Art. 9 Abs. 2 lit. f DSGVO dürfen besonders schützenswerte Daten bearbeitet werden, wenn dies der Durchsetzung von Rechtsansprüchen dient. Der Begriff "Rechtsansprüche" ist nicht auf laufende, formelle Gerichtsverfahren beschränkt (Beck DSGVO Kommentar-Schulz, Art. 9 N 34). Nach Angaben des britischen ICO umfasst dieser Begriff die Datenbearbeitung, die für (a) aktuelle oder künftige Gerichtsverfahren, (b) die Einholung von Rechtsrat oder (c) die Begründung, Ausübung oder Verteidigung von vertraglichen oder gesetzlichen Rechtsansprüchen auf andere Weise erforderlich ist.

[111] Daher sind wir der Ansicht, dass es gute Argumente dafür gibt, dass die Bearbeitung von besonders schützenswerten Daten im Rahmen einer Untersuchung eines möglichen Verstosses gegen die Verbandsregeln oder gar strafrechtliche Bestimmungen und die Vorbereitung eines möglichen Disziplinarverfahrens gegen die beschuldigte Person in den Anwendungsbereich dieser Bestimmung fallen könnte. In allen Fällen, in denen das Ergebnis einer Untersuchung vernünftigerweise dazu führen könnte, dass der Verband oder das Gremium ein Disziplinarverfahren gegen einen nationalen Verband, Trainer*innen oder Sportler*innen einleitet, könnte diese Rechtsgrundlage u.E. im Prinzip herangezogen werden, da die Verbandsregeln i.d.R. Sanktionen für fehlerhaftes Verhalten vorsehen. Athleten*innen und Trainer*innen verpflichten sich vertraglich zur Einhaltung dieser Verbandsregeln, weshalb die Sanktionen der Durchsetzung der vertraglich vereinbarten Verhaltensregeln dienen. Es ist jedoch nicht auszuschliessen, dass eine Behörde oder ein Gericht zum Schluss kommen könnte, dass diese Rechtsgrundlage untauglich wäre.

c. Erhebliches öffentliche Interesse

[112] Art. 9 Abs. 2 lit. g DSGVO erlaubt die Bearbeitung von besonders schützenswerten Daten, wenn dies zur Wahrung eines wichtigen öffentlichen Interesses erforderlich ist. Der Begriff "öffentliches Interesse" deckt ein breites Spektrum von Werten und Grundsätzen in Bezug auf das öffentliche Wohl ab. Ein wesentliches öffentliches Interesse kann insbesondere darin bestehen, die öffentliche Sicherheit zu gewährleisten oder Gefahren für bestimmte Rechtsgüter abzuwenden, wie etwa den Schutz der physischen und psychischen Integrität des Einzelnen insgesamt (Beck DSGVO Kommentar-Schulz, Art. 9 N 37). Damit ein erhebliches öffentliches Interesse hier greifen kann, muss dieses öffentliche Interesse im nationalen Recht eines EU-Mitgliedstaates verankert sein (Beck DSGVO Kommentar-Schulz, Art. 9 N 37.), wobei es unklar ist, ob beispielsweise ein nationales Strafgesetzbuch, dass die Nötigung als Straftat verankert, bereits ausreicht, oder ob das öffentliche Interesse spezifischer sein müsste, z.B. indem es den Schutz von Athleten*innen gegen Übergriffe

beinhaltet. In anderen Ländern wird der Begriff der Rechtsgrundlage immerhin weit gefasst. Im Vereinigten Königreich beispielsweise sind die Bekämpfung von Doping, der Schutz von Kindern und gefährdeten Personen, die Vorbeugung oder Aufdeckung rechtswidriger Handlungen oder Verhaltensnormen im Sport allesamt Rechtsgrundlagen, welche die Berufung auf ein erhebliches öffentliches Interesse für die Bearbeitung von besonders schützenswerten Daten erlauben können. Darüber hinaus hat der EuGH in einem Urteil aus dem Jahr 2019 angedeutet, dass in diesem spezifischen Fall die Meinungsfreiheit ein erhebliches öffentliches Interesse im Zusammenhang mit der Bearbeitung von besonders schützenswerten Daten durch eine Suchmaschine sein könnte (Entscheid des EuGH C-136/17 vom 14. September 2019 Rn. 61 ff.). Dies deutet daraufhin, dass eine Rechtsgrundlage für ein erhebliches Interesse auch ein Verfassungsrecht sein könnte und somit ein sehr breit gefasstes Recht – wie beispielsweise der Schutz der öffentlichen Gesundheit – bereits ausreichen würde, um sich auf diese Rechtsgrundlage zu stützen. Somit gibt es u.E. gute Argumente dafür, dass dieses Rechtsgrundlage greifen könnte.

[113] Es lässt sich aufgrund fehlender Rechtsprechung und Praxis nicht abschliessend beurteilen, welches dieser drei Rechtsgrundlagen in der EU tatsächlich anwendbar wäre. In diesem Sinne verbleibt eine gewisse Rechtsunsicherheit gemäss Rechtmässigkeit der Bearbeitung von Daten Dritter unter der DSGVO, es sei denn das lokale Recht eines Mitgliedstaates bietet eine spezifische Rechtsgrundlage. Dennoch sind wir der Ansicht, dass sowohl die interne Bearbeitung durch den Verein (Art. 9 Abs. 2 lit. d DSGVO) sowie das erhebliche öffentliche Interesse (Art. 9 Abs. 2 lit. g DSGVO) Rechtsgrundlagen sind, die im Prinzip gelten könnten.

D. Hooliganismus

[114] Die Bekämpfung von Gewalttaten und Ausschreitungen (Hooliganismus) im Zusammenhang mit Sportanlässen ist nach wie vor von grosser Bedeutung. Bund, Kantone und Gemeinden teilen sich dabei bestimmte Kompetenzen. Nach Art. 57 Abs. 1 **BV** sorgen der Bund und die Kantone für die Sicherheit des Landes und den Schutz der Bevölkerung. Daraus folgt, dass die Kantone Rechtssetzungskompetenz im Rahmen der Gewährleistung der inneren Sicherheit (u.a. im Polizeibereich) auf ihrem Hoheitsgebiet haben (Bericht Bekämpfung Hooliganismus, S. 9 f.). Gleichzeitig stellen sich auch in diesem Bereich verschiedene datenschutzrechtliche Fragen, die nachfolgend kurz erörtert werden.

[115] Im Rahmen der Bekämpfung von Hooliganismus ist zu beachten, dass in aller Regel Behörden die erhobenen Daten bearbeiten. Im Gegensatz zur Bearbeitung von Personendaten durch private Personen, wie Sportverbände, bedarf es bei einer Datenbearbeitung durch Behörden stets einer gesetzlichen Grundlage (Art. 34 Abs. 1 **DSG** für Bundesbehörden sowie statt vieler: §8 Gesetz über die Information und den Datenschutz des Kantons Zürich für kantonale Behörden).

1. Gesetzliche Grundlage

[116] Die Massnahmen gegen Hooliganismus waren ursprünglich im Bundesrecht verankert, und zwar im Bundesgesetz über Massnahmen zur Wahrung der inneren Sicherheit (BWIS). Mittlerweile wurden sie ins Konkordat über Massnahmen gegen Gewalt anlässlich von Sportveranstaltungen

(**Hooligan-Konkordat**) überführt, wobei gewisse Normen bzgl. der eingesetzten Informationssysteme weiterhin im BWIS verankert sind.

[117] Das BWIS, die Verordnung über verwaltungspolizeiliche Massnahmen des Bundesamtes für Polizei und über das Informationssystem HOOGAN (VVMH) sowie das Hooligan-Konkordat enthielten bzw. enthalten repressive und präventive Massnahmen wie z.B. Stadionverbote, Rayonverbote, Meldeauflagen, Polizeigewahrsam und Ausreisebeschränkungen (siehe Art. 24c **BWIS**, Art. 4 ff. **VVMH** und Art. 3b ff. des Hooligans-Konkordats). Die Durchsetzung erfolgt durch die Kantons- oder Stadtpolizei (Bericht Bekämpfung Hooliganismus, S. 12).

[118] Neben den erwähnten Massnahmen wird gemäss Art. 24a Abs. 1 **BWIS** vom Bund ein elektronisches Informationssystem (sog. HOOGAN) geführt, in das Daten über Personen aufgenommen werden, die sich anlässlich von Sportveranstaltungen im In- und Ausland gewalttätig verhalten haben. Das HOOGAN wird von Fedpol betrieben. Die Aufnahme in das HOOGAN erfolgt, wenn ein Stadionverbot, ein Rayonverbot, eine Meldeauflage, Polizeigewahrsam oder eine Ausreisebeschränkung verfügt wird (Art. 8 Abs. 1 i.V.m. Art. 6 Abs. 2 lit. a und Art. 7 **VVMH**).

[119] Die Daten, die bei der Datenbank HOOGAN bearbeitet werden (hierzu gehören gemäss Art. 24a Abs. 3 **BWIS** u.a.: Foto, Name, Geburtsdatum, Heimatort, Wohnadresse, Massnahmen etc.), sind u.a. Daten über verwaltungs- und strafrechtliche Verfolgungen oder Sanktionen, d.h. sie sind besonders schützenswerte Daten. Aus diesem Grund wird gemäss Art. 34 Abs. 2 lit. a **DSG** eine Grundlage in einem Gesetz im formellen Sinn für deren Bearbeitung vorausgesetzt. Diese Grundlage befindet sich vorliegend in Art. Art. 24a Abs. 5 **BWIS**, gemäss welchem die Vollzugsbehörden ermächtigt werden, besonders schützenswerte Personendaten zu bearbeiten, soweit es die Durchführung ihrer Aufgaben erfordert.

2. Öffentliches Interesse und Verhältnismässigkeit

[120] Die Bearbeitung von Personendaten seitens einer Bundesbehörde bedingt neben der gesetzlichen Grundlage auch das Vorliegen eines öffentlichen Interesses sowie die Gewährleistung der Verhältnismässigkeit. Das öffentliche Interesse ist u.E. bei der Führung der HOOGAN grundsätzlich gegeben, da die Führung der HOOGAN der Gewährleistung der inneren Sicherheit und den Schutz der körperlichen Unversehrtheit der Bevölkerung dient (Studer, S. 66 f.). Eine solche Datenbank ist zudem geeignet, ein solches Ziel zu erreichen, weil es ermöglicht, die Massnahmen effizient und zeitnah zu erfassen. In Anbetracht der weiterhin bestehenden Problematik der Gewalttaten im Rahmen von Sportveranstaltungen (Tagesanzeiger vom 17.10.2023 **Neue Studie zu Fangewalt: Trotz Hooligan-Konkordat randalieren Chaoten weiter**) ist die Führung der HOOGAN auch erforderlich und zumutbar, obwohl in der Lehre teilweise Bedenken betreffend der Schwere des Eingriffs in die Persönlichkeitsrechte der Fans bestehen (Studer, S. 67).

[121] Vorliegend kann sich der Bund also auf eine gesetzliche Grundlage für die Führung von HOOGAN stützen. Jedoch haben auch dann der Bund oder ein Sportverband, dass solche Datenbanken führen, trotz gesetzlicher Grundlage die Datenschutzgrundsätze und die anderen Pflichten gemäss DSG einzuhalten. Andernfalls kann dies zu Reputationsschäden, Untersuchungen oder gar Bussen führen.

3. Einhaltung der Datenschutzgrundsätze und Gewährleistung der Datensicherheit

[122] Im Jahr 2023 wurde der Bund von einem Hacker-Angriff betroffen. Dabei wurde auf Daten eines externen IT-Dienstleisters (Xplain) zugegriffen, und Einträge aus dem HOOGAN von über 700 Personen wurden anschliessend im *Darknet* veröffentlicht (Inside IT vom 12. Juli 2023 **Xplain-Hack legt offen: Einträge aus Hooligan-Datenbank wurden nicht gelöscht**). Problematisch war in diesem Fall insbesondere, dass gewisse Einträge im HOOGAN offenbar einerseits nicht mehr aktuell waren und deshalb hätten gelöscht werden müssen und andererseits, dass Xplain ungenügende Datensicherheitsmassnahmen zum Schutz der Daten vor solchen Angriffen implementiert hatte (Inside IT vom 12. Juli 2023 **Xplain-Hack legt offen: Einträge aus Hooligan-Datenbank wurden nicht gelöscht**).

[123] Ersteres ist problematisch, weil der Bund eine Pflicht hat, Personendaten derjenigen, die sich nicht mehr unauffällig verhalten, spätestens drei Jahre nach einer Massnahme zu löschen (Art. 12 **VVMH**). Die Löschung wurde offenbar jedoch nicht in allen Fällen vorgenommen. Ein Verstoss gegen diese Grundätze kann zivilrechtliche Folgen auslösen, wie z.B. Löschungsansprüche oder eine Untersuchung durch den EDÖB. Eine derartige Untersuchung ist derzeit hängig (**Medienmitteilung der EDÖB zur Untersuchung gegen fedpol und BAZG vom 16. Mai 2023**). Vor diesem Hintergrund ist für Sportverbände oder Behörden, die im Rahmen der Bekämpfung des Hooliganismus in der Schweiz ähnliche Datenbanken führen, von erheblicher Bedeutung, dass stets sichergestellt ist, dass sämtliche Datenschutzgrundsätze lückenlos eingehalten werden (namentlich, was die Löschung von Daten betrifft) sowie dass die jeweiligen Datenbanken höchste Sicherheitsstandards erfüllen.

[124] Im vorliegenden Fall gilt der Bund als Verantwortlicher im Sinne des DSG und der externe IT-Dienstleister grundsätzlich als Auftragsbearbeiter. In einer solchen Konstellation hat der Auftragsbearbeiter genauso wie der Bund eine Pflicht, angemessene technische und organisatorische Sicherheitsmassnahmen zu implementieren (vgl. Art. 8 **DSG**). Der Bund hat aber nach Art. 9 Abs. 2 **DSG** eine Pflicht, sich über die Angemessenheit der vom Auftragsbearbeiter implementierten Datensicherheitsmassnahmen zu vergewissern, was vom Bund gemäss den Medienberichten jedoch nicht sichergestellt wurde (Inside IT vom 12. Juli 2023 **Xplain-Hack legt offen: Einträge aus Hooligan-Datenbank wurden nicht gelöscht**).

[125] Es ist somit wichtig, dass Sportverbände oder Behörden, die solche Datenbanken betreiben (oder generell Personendaten bearbeiten) und dabei einen Teil der Datenbearbeitung an einen Dritten auslagern, stets Prozesse einführen, um die Datensicherheitsmassnahmen des Drittanbieters zu prüfen, ansonsten sie selber das Risiko eingehen, gegen Art. 8 und 9 **DSG** zu verstossen. Ein Verstoss gegen Art. 8 und Art. 9 **DSG** kann zu einer Busse führen (vgl. vorstehend Rz. 75).