Torben J. Herber, Marc Jentsch, Sebastian Zickau

Datenschutz und Dopingkontrollen

Können Privacy-Enhancing Technologies (PETs) tausenden Athleten zu mehr Privatsphäre verhelfen?

Nicht erst seit den jüngsten Dopingenthüllungen stehen alle Athleten im Spitzensport unter einem Doping-Generalverdacht. Der Welt-Anti-Doping-Code hat die Unschuldsvermutung der Athleten schon seit Jahren abgeschafft. Sie können nur durch die Duldung massiver Eingriffe in ihre Privat- und Intimsphäre beweisen, dass sie »sauberen« Sport betreiben. Der Beitrag zeigt auf, dass diese massiven Eingriffe durch die Anwendung von PETs bald der Vergangenheit angehören können.

1 Ausgangssituation[1]

Hierzulande müssen sich etwa 7.000 professionelle Athleten aus unterschiedlichen Sportarten regelmäßig unangekündigten Dopingkontrollen unterziehen. Zur Anbahnung dieser Kontrollen wird von der »Welt Anti Doping Agentur (WADA)« ein System namens »Anti-Doping Admission And Administration System (ADAMS)« empfohlen, das neben Deutschland in über hundert weiteren Nationen eingesetzt wird.[2]

ADAMS stellt eine Online-Schnittstelle zur Verwaltung von Terminen und Aufenthaltsorten bereit. Athleten auf internationalem Leistungsniveau sind verpflichtet, ihre regelmäßigen Aufenthaltsorte – die sogenannten »Whereabouts« – bis zu drei Monate im Voraus einzupflegen und eventuelle Änderungen – auch kurzfristig – nachzuhalten.[3] Dopingkontrolleure greifen auf diese Informationen zu, um jederzeit unangekündigte Kontrollen vornehmen zu können. Die Athleten unterziehen sich diesem strengen Testregime, um an nationalen und internationalen Wettkämpfen teilnehmen zu dürfen.

Aber weshalb finden Dopingkontrollen ohne Terminvereinbarung statt? Das hängt vor allem damit zusammen, dass der Nachweis von Doping im Blut oder Urin zeitabhängig ist; manche Substanzen können über die Einnahme von Medikamenten vor einer Kontrolle »maskiert« oder ausgeleitet werden. Grundsätzlich gilt: Je kürzer die Vorwarnzeit bei Kontrollen, desto weniger Zeit bleibt für Gegenmaßnahmen.[4]

Die Athleten gewähren den jeweiligen Anti-Doping Einrichtungen also, neben Auskünften über ihren Gesundheitsstatus, insbesondere über die Whereabouts auch tiefreichende Einblicke in ihren Lebensalltag. Dabei ist ihnen nicht bekannt, wo ihre Daten gespeichert werden oder für wie lange. Auch die Frage, wer auf die überwiegend sehr persönlichen Informationen zugreifen kann, bleibt unbeantwortet.[5] Dieser einseitige Informationsfluss ist für die meisten Betroffenen, neben der mangelnden

1 Vgl. *Buchner*, DuD 2009, S. 475 ff; *Weichert*, DuD 2011, S. 702 ff.

Torben J. Herber

Diplom-Jurist und Wissenschaftlicher Mitarbeiter am ULD Schleswig-Holstein, Projekt PARADISE. Promoviert zur DSGVO mit Sportbezug.

E-Mail: torben.herber@stu.uni-kiel.de

Dr. Marc Jentsch

Projektmanager am Fraunhofer FIT und Leiter des Projekts PARADISE

E-Mail: marc.jentsch@fit.fraunhofer.de

Sebastian Zickau

Diplom-Informatiker und Wissenschaftlicher Mitarbeiter am Fachgebiet Service-centric Networking (SNET), Leitung Prof. Dr. Axel Küpper, TU Berlin. Promoviert zum Thema Datenschutz- und Sicherheitsregeln mit Lokationsbezug

E-Mail: sebastian.zickau@tu-berlin.de

2 *Plass/Giffeler*, DANA 04/2014, S.158.

3 Art. 1.3 Standard für Meldepflichten der Nationalen Anti Doping Agentur Deutschland, Version 3.0, http://www.nada.de/fileadmin/-DOWNLOADS-/Regelwerke/2015_Standard_fuer_Meldepflichten.pdf (Abruf: 23.3.2017).

4 *Plass/Giffeler*, DANA 04/2014, S. 158.

5 Vgl. *Schlarmann*, ZD 2016, S. 577.

Gebrauchstauglichkeit des bestehenden Verwaltungssystems, ein großes Ärgernis.

2 Datenschutzrechtliche Bewertung

Wie dieses »große Ärgernis« der Athleten aus datenschutzrechtlicher Sicht einzuordnen ist, wird nachfolgend anhand des »Standard-Datenschutzmodells (SDM)«[6] bewertet. Das SDM ist ein durch die Konferenz der Datenschutzbehörden im November 2016 zur Beratung und Prüfung empfohlenes Modell, mit dem sich gesetzliche Anforderungen zur Gewährleistung eines angemessenen Datenschutzes aus dem BDSG und künftig der DS-GVO ableiten lassen.[7] Es findet seine rechtlichen Anknüpfungspunkte in der Pflicht geeignete technische und organisatorische Maßnahmen zum Schutz personenbezogener Daten einzusetzen (§ 9 BDSG).[8] Durch seine Gliederung in die sieben Gewährleistungsziele Datenminimierung, Verfügbarkeit, Integrität, Vertraulichkeit, Nichtverkettung, Intervenierbarkeit sowie Transparenz bietet es jedem Anwender eine eingängige Prüfmethode.[9]

2.1 Datenminimierung

Beginnend mit dem SDM-Gewährleistungsziel der Datenminimierung ist zunächst festzustellen, welche Daten der Athleten überhaupt von ADAMS erhoben, verarbeitet und ob diese für einen legitimen Zweck genutzt werden. Gemäß »Anlage 1 zum Standard für Datenschutz«[10] werden Athletendaten wie Name, Geburtsdatum, Sportart, Kontaktadressen, Informationen über ihren Aufenthaltsort- und die Erreichbarkeit, Ausnahmen zur Verwendung von Medikamenten der Dopingliste aus therapeutischen Gründen (»Therapeutic Use Exemptions – TUEs«), Dopingkontrollunterlagen und Dopingprobenergebnisse sowie der biologische Athletenpass erhoben. Somit handelt es sich bei denen von ADAMS erhobenen Daten sowohl um personenbezogene Daten nach § 3 Abs. 1 S. 1 BDSG als auch um besondere Arten personenbezogener Daten gemäß § 3 Abs. 9 S. 1 BDSG, die einem höheren Schutzniveau unterliegen.

Das Gewährleistungsziel der Datenminimierung steht innerhalb des SDMs dafür, dass nicht mehr personenbezogene Daten erhoben, verarbeitet oder genutzt werden, als für die Erreichung des Zweckes erforderlich sind.[11] Darunter fällt auch, dass Daten im Rahmen einer Löschpflicht nach § 35 Abs. 2 S. 2 Nr. 3 BDSG zu löschen sind, wenn ihre Kenntnis für die Erfüllung des Zweckes der Speicherung nicht mehr erforderlich ist. Der »Nationale Anti-Doping Code 2015 (NADC)«[12] gibt in Art. 5.4.3 als Zweck für die Speicherung der personenbezogenen Daten der Athleten an, dass diese »ausschließlich für die Planung, Koordinierung und Durchführung von Dopingkontrollen […] verwendet« werden. Damit dienen die Whereabouts ausschließlich der Auffindbarkeit der Athleten. Somit entfällt deren Zweck und Erforderlichkeit zum „Auffinden für eine Kontrolle" regelmäßig mit dem Ablauf des betreffenden Tages, spätestens aber mit Abschluss eines konkreten Kontrollauftrags.

Der »Anlage 1 zum Standard für Datenschutz« zufolge werden die Whereabouts – und damit die vollen Bewegungsprofile aller Athleten – in ADAMS aber mindestens weitere 1,5 Jahre gespeichert. Sie sind somit zweckunabhängig von der Erhebung noch lange einseh- und auswertbar für einen Personenkreis, der aus Sicht der Athleten weder bekannt, noch von der Personenanzahl her abschätzbar ist. Unter dem Gesichtspunkt des Gewährleistungsziels der Datenminimierung stellen diese Umstände eine unvertretbare Einschränkung dar.

2.2 Verfügbarkeit

Das SDM-Gewährleistungsziel Verfügbarkeit soll sicherstellen, dass die personenbezogenen Daten zur Verfügung stehen und ordnungsgemäß im vorgesehenen Prozess verwendet werden können.[13] Im Rahmen von ADAMS heißt das, dass die erhobenen Whereabouts es der NADA ermöglichen müssen die Athleten für Dopingkontrollen aufzufinden. Laut NADA kam es im Jahr 2015 zu 258 Meldepflicht- und Kontrollverstößen.[14] Die Gründe dafür sind nicht weiter ausgeführt, lassen aber darauf schließen, dass das ADAMS hier deutlich optimiert werden kann.

2. 3 Integrität

Das SDM-Gewährleistungsziel der Integrität steht unter anderem dafür, dass die zu verarbeitenden Daten unversehrt, vollständig und aktuell bleiben.[15] Wenn es der Hackergruppe »Fancy Bear« über einen für die Olympiade 2016 in ADAMS eingerichteten IOC-Account gelungen ist, TUEs aus dem ADAMS zu veröffentlichen[16], wird der Schritt gefälschte TUEs ins System einzuspielen, zu verändern oder zu löschen zu einem real denkbaren Szenario. Solches würde dazu führen, dass Athleten entweder unberechtigt verbotene Medikamente zur Leistungssteigerung einnehmen könnten, oder aber eines Dopingverstoßes beschuldigt werden, weil deren TUEs aus ADAMS gelöscht worden sind. Nicht zuletzt für die beabsichtigten Zwecke einer effektiven Dopingkontrolle sind diese Integritätsgesichtspunkte durch ein verbessertes System zu adressieren.

2.4 Vertraulichkeit

Unter Vertraulichkeit wird im SDM verstanden, dass keine Person unbefugt personenbezogene Daten zur Kenntnis nehmen kann. Unbefugt ist nicht nur jeder Dritte, der nicht zur verant-

6 Das Standard-Datenschutzmodell Version 1.0, https://datenschutzzentrum.de/uploads/SDM-Methode_V_1_0.pdf (Abruf: 23.3.2017).

7 Tagungsband »Das Standard-Datenschutzmodell – der Weg vom Recht zur Technik«, S. 4, https://www.datenschutzzentrum.de/uploads/sdm/SDM_Tagungsband2015_Hannover.pdf (Abgerufen: 23.3.2017). Das zugrunde liegende Modell wird durch das ULD seit mehreren Jahren in der Beratung eingesetzt.

8 SDM V.1.0, S.18 f.

9 *Rost*, c't – magazin für computertechnik, 2016/02, S.138; vgl. *Bieker/Hansen/Friedewald*, RDV 2016, S. 191 ff.

10 Anlage 1 zum Standard für Datenschutz, http://www.nada.de/fileadmin/-DOWNLOADS-/Regelwerke/2015_Annex_Standard_fuer_Datenschutz.pdf (Abgerufen: 23.3.2017).

11 SDM V.1.0, S.11. Für die Verortung und Bezüge der Gewährleistungsziele zu den Normen des BDSGs und der DS-GVO siehe S. 22 ff.

12 Nationaler Anti-Doping Code 2015, http://www.nada.de/fileadmin/-DOWNLOADS-/Regelwerke/NADA-Code_2015.pdf (Abgerufen: 23.3.2017)

13 SDM V.1.0, S.13.

14 NADA Jahresbericht 2015, S.34, http://www.nada.de/fileadmin/user_upload/NADA_Jahresbericht_2015_deutsch.pdf (Abgerufen 23.3.2017).

15 SDM V.1.0, S.13.

16 WADA, Cyber Security Update: WADA's Incident Response, https://www.wada-ama.org/en/media/news/2016-10/cyber-security-update-wadas-incident-response (Abgerufen: 23.3.2017); Sportler wollen sich nicht mehr nackig machen, Zeit Online: http://www.zeit.de/sport/2016-11/doping-datenbank-alternative-jonas-plass (Abgerufen: 23.3.2017).

wortlichen Stelle gehört, sondern auch interne Personen, die zur Bewältigung ihrer Aufgaben keinen Zugriff auf die detaillierten personenbezogenen Daten benötigen.[17]

Für die in der Dopingkontrollplanung zuständige Person würde das bedeuten, dass sie nur die Tätigkeiten der zu kontrollierenden Athleten sowie eine zum Beispiel auf die Region vergröberte Positionsangabe angezeigt bekommt. Ein »Doping Control Officer (DCO)« benötigt für das Antreffen eines Athleten nur den Zugriff auf die Whereabouts dieser spezifischen Person bis der Dopingkontrollauftrag abgeschlossen ist. Ein umfassender Zugriff auf die Historie und alle künftigen Whereabouts aller registrierten Athleten scheint unter diesen Gesichtspunkten für keinen Beteiligten erforderlich zu sein. Zufolge der Meldungen über die Zugriffe auf die TUEs zahlreicher Athleten verschiedener Nationen und Sportarten durch die Hackergruppe »Fancy Bear« scheint ein solcher Zugriff auf Whereabouts unter dem ADAMS möglich.[18] Auch innerhalb der NADA gibt es derzeit kein ausreichendes Berechtigungskonzept für den Zugriff auf die personenbezogenen Daten der Athleten, das einer Überprüfung unter dem Aspekt der Vertraulichkeit standhalten würde.[19] Jedoch ist positiv anzumerken, dass das Authentisierungsverfahren im ADAMS nachgebessert worden ist und ab sofort die Beantwortung einer Sicherheitsfrage neben der Eingabe der Zugangsdaten erforderlich ist.[20]

2.5 Nichtverkettung

Das SDM-Gewährleistungsziel der Nichtverkettung soll sicherstellen, dass die Daten nur für den Zweck ausgewertet werden können, für den sie auch erhoben worden sind. Insbesondere große Datenbestände bieten die Gefahr, dass sie mit anderen, auch frei zugänglichen Informationen, verknüpft werden können und dadurch neue Erkenntnisse über die Person bringen.[21]

Im ADAMS werden große Datenmengen, vor allem durch das Erheben der Whereabouts aggegiert. Diese Whereabouts sagen auf dem ersten Blick nur aus, wann sich ein Athlet wo befinden wird. Sieht man sich aber die korrigierten Whereabouts der letzten 18 Monate sowie des kommenden Quartals an, lassen sich detaillierte Bewegungsprofile der Athleten abzeichnen. Diese Bewegungsprofile können dann wiederrum Rückschlüsse auf den gewöhnlichen Tagesablauf und dadurch auf persönliche Vorlieben und Neigungen der Athleten geben.[22] Ist eine oft besuchte Adresse eine religiöse Einrichtung, kann auf die Religionszugehörigkeit, bei einem regelmäßigen Übernachtungsort auf eine persönliche Beziehung und beim Aufsuchen von Beratungsstellen auf persönliche Probleme des Athleten geschlossen werden. Diese Verkettung von Daten wird von ADAMS durch die anlassunabhängige und detaillierte Abfrage von Whereabouts begünstigt.

Neben den Whereabouts sind die Urin- oder Blutproben aber genauso geeignet weitere intime Auskünfte über die Athleten preis zu geben. So wurde erst kürzlich bei einer Dopingkontrolle eines Fußballers festgestellt, dass dieser an einer schweren Tumorerkrankung litt.[23] Auch Schwangerschaften lassen sich feststellen. Daher bedürfen diese Arten besonders persönlicher Daten auch unter dem Gesichtspunkt der Verkettbarkeit eines erhöhten Schutzniveaus.

2.6 Intervenierbarkeit

Die Intervenierbarkeit stellt innerhalb des SDMs sicher, dass den Betroffenen die ihnen zustehenden Benachrichtigungs- und Auskunftsrechte jederzeit wirksam gewährt werden und die verarbeitende Stelle in der Lage ist in die Datenverarbeitung von der Erhebung bis zur Löschung der Daten einzugreifen.[24] Bei dem in Kanada gehosteten ADAMS gibt es keine bekannten Regelungen zu Auskunftsrechten und zur Löschung von Daten.[25] Vielmehr wird für die Auskunftserteilung auf die jeweils zuständigen »nationalen Anti-Doping-Organisationen (NADOs)« verwiesen,[26] was darauf schließen lässt, dass sich die WADA selbst nur als Auftragsdatenverarbeiter versteht. In diesem Fall müssten die das System nutzenden NADOs Vorkehrungen getroffen haben, um sämtliche Betroffenenrechte jederzeit umfassend gewähren zu können. Damit ist die Intervenierbarkeit faktisch nicht gegeben.

2.7 Transparenz

Schließlich hat das ADAMS die Anforderungen des SDM-Gewährleistungsziels der Transparenz zu erfüllen. Unter Transparenz wird verstanden, dass sowohl Betroffene als auch Betreiber erkennen können, welche Daten für welchen Zweck in einem Verfahren erhoben und verarbeitet werden. Dazu gehört auch zu wissen, welche Systeme und Prozesse dafür genutzt werden und wer auf die jeweiligen Daten Zugriff hat.[27]

Mangels Mitarbeiter-Berechtigungskonzept und einheitlichen Regelungen zum Auskunftsrecht liegt beim ADAMS keine Transparenz vor. Die Athleten können nicht nachvollziehen, wer wann zu welchem Zweck auf ihre Daten zugegriffen hat.

2.8 Ergebnis der Überprüfung

Die Bewertung des ADAMS anhand des SDMs offenbart erhebliche Verbesserungsmöglichkeiten bei der Verarbeitung der personenbezogenen Daten der Athleten. Ein wünschenswertes Doping-Kontrollsystem bedarf für alle der sieben Gewährleistungsziele erhebliche Verbesserungen technischer und organisatorischer Maßnahmen – setzt man dabei die nach der DS-GVO ab 2018 geforderten Designprinzipien Privacy by Design und Privacy by Default an, sind für einen grundrechtskonformen und effektiven Einsatz umfassende Optimierungen möglich und notwendig. Das ADAMS wird den Anforderungen an die Datenerhebung, -verarbeitung und –nutzung in diesem besonders sensiblen Bereich unter keinem der sieben Schutzziele gerecht.

17 SDM V.1.0, S.13 f.

18 WADA News, Cyber Security Update: WADA's Incident Response, https://www.wada-ama.org/en/media/news/2016-10/cyber-security-update-wadas-incident-response (Abgerufen: 23.3.2017).

19 NADA Jahresbericht 2015, S.23, http://www.nada.de/fileadmin/user_upload/NADA_Jahresbericht_2015_deutsch.pdf (Abgerufen: 23.3.2017).

20 NADA News, Neue Sicherheitsabfrage in ADAMS, http://www.nada.de/de/nada/aktuelles/news/newsdetail/?tx_news_pi1%5Bnews%5D=731&tx_news_pi1%5Bcontroller%5D=News&tx_news_pi1%5Baction%5D=detail&cHash=c78d60ad79f821f687c628dadbd431b4 (Abgerufen: 23.3.2017).

21 SDM V.1.0, S.14.

22 Vgl. *Schlarmann*, ZD 2016, S. 575.

23 Krebsdiagnose nach Dopingtest, Stern Online, http://www.stern.de/gesundheit/marco-russ-krebs-diagnose-nach-dopingtest--was-bedeutet-ein-erhoehter-hcg-wert--6857558.html (Abgerufen: 23.3.2017)

24 SDM V.1.0, S.15.

25 NADA Jahresbericht 2014, S.33. http://www.nada.de/fileadmin/user_upload/nada/Recht/160802_Datenschutz2014_DE.pdf (Abgerufen: 23.3.2017).

26 WADA contact page: https://www.wada-ama.org/en/contact-us (Abgerufen: 23.3.2017).

27 SDM V.1.0, S.15.

3 Lösungsansatz

3.1 Das Projekt PARADISE

Die beschriebenen Unzulänglichkeiten im Anti-Doping-System haben betroffene Sportler zum Anlass genommen das Projekt PARADISE[28] ins Leben zu rufen. PARADISE ist ein zweijähriges Forschungsprojekt mit dem Ziel den Datenschutz im Dopingkontrollprozess zu untersuchen und Lösungen zur Verbesserung dieses Datenschutzes zu erarbeiten. Gleichzeitig soll gewährleistet bleiben, dass Dopingkontrollen so zuverlässig und für Athleten unvorhersehbar wie bisher durchgeführt werden können. Ein weiteres Ziel des Projekts, neben der Erhöhung des Datenschutzes, ist eine verbesserte Nutzbarkeit der verwendeten Tools.

3.2 Die PARADISE-Plattform

Die PARADISE-Plattform kombiniert mehrere Ansätze zur Erhöhung des Datenschutzes:

- Reduzierung des Umfangs der aufgenommenen Daten;
- Sicherung der Daten vor unbefugtem Zugriff;
- Nachvollziehbarkeit von Technologie, Datenströmen und Zugriffen für Verantwortliche und Betroffene;
- Zweckgebundener Datenzugriff;
- Wahrung des Kernbereichs privater Lebensführung.

Teil der PARADISE-Plattform sind »Eves Devices«. Hierbei handelt es sich um kleine, tragbare Geräte, deren Position per Fernabfrage bestimmt werden kann. Athleten, die ein Eves Device mit sich tragen, können von einem DCO lokalisiert werden. Was auf den ersten Blick wie eine erhöhte Datenaufnahme aussieht, dient deren Reduzierung. Während Athleten momentan Details über Ihren Aufenthaltsort ins ADAMS eintragen müssen, reicht in Verbindung mit dem Eves Device die Angabe eines vergröberten Aufenthaltsortes, z.B. einer Stadt oder Region. Die Kenntnis über die Stadt oder Region reicht dem DCO, um im Vorhinein seine Reise planen zu können. Am Tag der Kontrolle nutzt der DCO dann die PARADISE-Plattform vor Ort, um den Athleten genau zu lokalisieren. Das erhöht auch die Nutzbarkeit für die Athleten, da sie nicht mehr jede Änderung ihres Aufenthaltsorts im ADAMS nachhalten müssen. Das System stellt sicher, dass Dopingkontrollen weiterhin unangekündigt durchgeführt werden können, da die Athleten die Abfrage ihres Standorts nicht bemerken. Die Verwendung erfolgt auf freiwilliger Basis. Athleten, die kein Eves Device benutzen möchten, können stattdessen weiterhin wie bisher detaillierte Aufenthaltsdaten angeben.

Um die wenigen in der PARADISE-Plattform vorgehaltenen Daten (z. B. Name eines Athleten oder die seinem Eves Device zugeordnete Telefonnummer) vor unbefugtem Zugriff zu schützen, setzt PARADISE verschiedene Sicherheitsmechanismen ein. Dazu wird auf »Attributsbasierte Autorisierung (Attribute-Based-Credentials, ABCs)« und verteilte Attributsdelegierung gesetzt, um das Rollenmodell im Projektkontext realitätsnah abzubilden. Ziel ist es beispielsweise, nur berechtigen Dopingkontrolleuren den Zugriff zu den entsprechenden Diensten und Informationen zu erlauben. Gleichzeitig sind Dopingkontrolleure Mitarbeiter verschiedener externer Unternehmen und somit nicht Teil einer systeminhärenten Hierarchie. Um die Kontrolle des Zugriffs auf Athletendaten im Rechenzentrum selbst vor vorsätzlichem Handeln seitens des Betreibers zu schützen, verwendet PARADISE versiegelte Cloud-Technologie (Sealed Cloud Technologie). Die Sealed Cloud Technologie stellt durch organisatorische und technische Maßnahmen sicher, dass der Betreiber der Infrastruktur nicht auf unverschlüsselte Daten zugreifen kann.[29]

Dopingkontrollen basieren auf Unvorhersehbarkeit. Wenn Athleten nichts von einer anstehenden Kontrolle wissen, ist es schwieriger Dopingverstöße zu verschleiern. Deshalb lässt die PARADISE-Plattform zum Zeitpunkt einer Standortabfrage Athleten nichts von dieser wissen. Im Anschluss an eine erfolgte Kontrolle können Athleten in der PARADISE-Plattform aber alle Standortabfragen nachvollziehen. Darüber hinaus stellt das PARADISE-Projekt die relevanten Teile seiner Software als Open Source zur Verfügung. Somit kann objektiv überprüft werden, dass die Daten nur für den vorgesehenen Zweck verwendet werden. Diese Nachvollziehbarkeit der Technologie ist für ADAMS nicht gegeben.

Insbesondere auf den Standort der Athleten kann nur zweckgebunden zugegriffen werden. So bietet die PARADISE-Plattform DCOs nur die Standortabfrage für Athleten an, für die die DCOs einen Kontrollauftrag haben, der sich über den Anfragezeitpunkt erstreckt. Die Nachvollziehbarkeit der Standortabfragen für die Athleten schreckt vor missbräuchlicher Mehrfachnutzung ab. Auch die PARADISE-Plattform selber trackt nicht, da die Standortdaten nicht gespeichert werden.

Die PARADISE-Plattform erlaubt es allen Athleten private Datenschutzgebiete (Privacy Geofences) zu erstellen. Das sind Orte, an denen Athleten nicht für eine Dopingkontrolle aufgesucht werden möchten, wie beispielsweise eine Kirche oder ein Friedhof. Befindet sich der Athlet während einer Standortabfrage innerhalb eines solchen Geofences, wird dem DCO ein größeres Polygon anstelle eines exakten Standorts angezeigt. Der DCO kann seine Anfahrt in Richtung dieses Bereichs fortführen und später eine weitere Standortabfrage durchführen. Befindet sich der DCO in der Nähe eines Sportlers in einem Geofence, kontaktiert der DCO ihn mittels Mobiltelefon. Diese Art der Kontaktaufnahme am Zielort ist bereits jetzt übliche Praxis.

3.2.1 Umsetzung mittels Eves Devices

Mit den im Projekt PARADISE als Wearables entwickelten Eves Devices können die Athleten von den DCOs zur Durchführung einer Dopingkontrolle angetroffen werden. Die Lokalisierung des Wearables erfolgt auf Basis der weltweit verfügbaren, globalen Satellitennavigationssysteme, kurz GNSS, die von Sportlern aktuell auch mit Hilfe von Apps in Smartphones zum Beispiel zur Aufzeichnung von Laufstrecken oder zum Navigieren genutzt werden. Solche kommerziell erhältlichen Apps, Smart-Watches und Fitness-Armbänder werden von Datenschützern jedoch als kri-

28 PARADISE wird gefördert vom Bundesministerium für Bildung und Forschung, Referat 525 Kommunikationssysteme und IT Sicherheit, im Rahmen des Förderprogramms „IKT 2020 – Forschung für Innovationen", Ausschreibung „Selbstdatenschutz". Projektpartner sind das Fraunhofer Institut für Angewandte Informationstechnik FIT, das Fraunhofer Institut für Angewandte und Integrierte Sicherheit AISEC, gekko, Gesellschaft für Kommunikation und Kooperation mbH, das Unabhängiges Landeszentrum für Datenschutz Schleswig-Holstein, Technische Universität Berlin und Uniscon.

29 Vgl. Sealed Cloud schließt IT-Sicherheitslücke »Mensch«, DuD 2013, S. 333.

tisch angesehen, da sich die aufgezeichneten Daten oft nicht löschen lassen und über Server der Hersteller geleitet werden.[30]

Das Eves Device zeichnet keinerlei Daten auf sodass auch keine Bewegungsprofile erstellt werden können. Jegliche Kommunikation zwischen Eves Device und PARADISE-Plattform erfolgt drahtlos und AES verschlüsselt über das GSM Netz, sodass selbst mitgeschnittene Daten für unbefugte nicht lesbar sind. Dazu wird in jedes Gerät ein Schlüssel gebrannt, den nur die PARADISE-Plattform kennt. Das Wearable bietet keine Schnittstellen nach außen, sodass ein Auslesen ohne weiteres nicht möglich ist. Die PARADISE-Plattform wird in einer Sealed Cloud implementiert, sodass auch dort niemand unbefugtes an sensible Daten gelangen kann.

Das Eves Device ist klein und handlich, sodass es entweder als Schlüsselanhänger, an die Kleidung geklippt oder in der Tasche verstaut werden kann. Die Akkulaufzeit soll mindestens 24 Stunden betragen und die Aufladung drahtlos über ein Ladepad erfolgen, wie bei aktuellen Smartphones und Tablets.

3.2.2 Selbstdatenschutz durch Geofencing

Auch mit dem Einsatz des Eves Devices muss sichergestellt sein, dass die Athleten die Kontrolle über ihre Daten behalten. Unter ADAMS kann dies nur mit Falschangaben oder dem Weglassen von Einträgen realisiert werden, denn derzeit gibt es keinen Mechanismus, der ausschließen kann, dass auch die Whereabouts von unbeteiligten Dritten, wie die Angaben über Wohnorte von aufgesuchten Personen, mit in der ADAMS Datenbank gespeichert werden.

Die Nutzung des Eves Device ist nicht nur aus Sicht der Benutzerfreundlichkeit begrüßenswert, sondern eröffnet auch Möglichkeiten den Athleten die aktive Kontrolle über die Whereabouts zurück zu geben. Grundsätzlich wird die Position des Devices ermittelt und an den DCO zurückgegeben. Im einfachsten Fall ist das eine Positionsangabe mit möglichst hoher Genauigkeit. Ist allerdings der Fall gegeben, dass die Standortabfrage unter Berücksichtigung des Aufenthaltsorts des DCOs durchgeführt wurde, besteht die Möglichkeit serverseitig die Genauigkeit des Standortes der Athleten zu verschleiern, und zwar wenn beide Standorte weit auseinander liegen und es keine Möglichkeit für eine Durchführung eines Test in absehbarer Zeit gibt. Wenn beide Standorte allerdings nah beieinander liegen, z. B. in derselben Stadt, dann wird die genaue Position des Athleten angezeigt. Es ist dabei auch bedacht worden, dass sich der DCO immer weiter an den Standort des Athleten annähern kann und somit genauere Positionsangaben bei jeder Abfrage bekommt, z. B. erst das Bundesland, dann die Stadt bzw. Stadtteil und zuletzt die präzise GPS Koordinaten. Durch dieses Vorgehen wird auch der zeitliche Aspekt der Athleten geschützt, d. h. dass bei der ersten Abfrage die Position derart verschleiert ist, dass eine Zuordnung von Uhrzeit zu einem spezifischen Ort nicht gegeben ist.

Die serverseitige Auswertung der Standorte ermöglicht es den Athleten im PARADISE-System auch Bereiche zu definieren, die sie als schützenswert, d. h. privat, erachtet. Dies können z. B. Bereiche sein, wie die Wohnung der Lebenspartnerin, spezifische medizinische Einrichtungen, religiöse Stätten oder z. B. der Standort von Selbsthilfegruppen. Das PARADISE-System erlaubt es allen Athleten diese Bereiche für sich zu definieren, die bei der Abfrage des Standorts durch den DCO im System mit berücksichtigt werden. In diesen Fällen würde dem DCO dann zusammen mit einer gröberen Standortangabe, z. B. dem Namen eines Bezirks, eine entsprechende Nachricht angezeigt werden. Diese Technologie basiert auf dem Konzept der Geofences, d. h. virtuelle eingrenzende Bereiche, die im System digital hinterlegt sind und auf einer Karte dargestellt werden können. In PARADISE werden diese Bereiche für jeden Athleten anonym gespeichert und ausgewertet. Im Projektkontext werden diese Geofences als Personal Privacy Gardens (kurz pprivGardens) bezeichnet. Die Athleten können diese Bereiche anlege, editieren und löschen.[31]

Eine generalisierte Form dieses Konzepts sieht PARADISE auch vor. Es können allgemeine Geofences angelegt werden, General Privacy Gardens bzw. gprivGardens, die für alle Athleten im System gleichermaßen gelten. Auch die Privatsphäre der DCOs wird hierbei mitbetrachtet.

Bei der Konzeption des PARADISE-System wird darauf geachtet, dass es nicht dazu genutzt werden kann, eine mögliche Dopingkontrolle mittels der beschriebenen Technologien und Konzepte zu umgehen. In der Regel sind die Athleten und DCOs daran interessiert, dass ein Treffen zustande kommt. Dies wird durch Einschränkungen hinsichtlich der Größe und der Aufenthaltszeit der privGardens realisiert.

3.2.3 Verteilte Attributbasierte Autorisierung

Im Anti-Doping-Kontrollsystem gibt es mit der WADA, den nationalen Anti-Doping-Organisationen (NADOs), wie z. B. der NADA, den Athleten sowie ihren nationalen und internationalen Verbänden eine Vielzahl von Akteuren. Dazu kommen auch noch die eigentlichen Dopingkontrolleure, die nicht von den NADOs, sondern von externen Dienstleistern gestellt werden.

Dieses Geflecht an Akteuren führt dazu, dass sich die einzelnen Rollen der Stakeholder nicht in einer Hierarchie abbilden lassen und die Zuständigkeiten über einzelne Entitäten nicht zentral verwaltet werden können. In solchen Szenarien bietet sich das Konzept der ABCs an, in Verbindung mit Attribut-Basierter-Delegation (ABD) in verteilten Systemen.

Existierende Arbeiten in diesen Forschungsbereichen wie von Rivest[32] oder Li[33] haben gezeigt, dass sich solche komplexen, verteilten Abhängigkeiten und Delegierungen mit ABD durch dessen Flexibilität und Skalierbarkeit einfach ausdrücken und lösen lassen. Ein wichtiger Aspekt bei verteilter ABC und ABD ist der Speicherort von Attributen und Delegationen. Ein zentraler Speicher ist bspw. nur dann sinnvoll, wenn alle Teilnehmer des Attributssystems bekannt sind, und ihnen vertraut werden kann. Insbesondere ist dies der Fall, wenn man hierarchische Rollenmodelle betrachtet.

In unserem Fall könnte eine Attributsdelegation jedoch folgendermaßen aussehen:
(1) PARADISE.user -> WADA.nado.dco

30 Vgl. *Jandt*, DUD 2016, S. 572; Datenschutz-Mängel bei Fitness-Armbändern und Smart Watches, https://datenschutzzentrum.de/artikel/1070-Datenschutzaufsichtsbehoerden-prueften-Wearables-Datenschutz-Maengel-bei-Fitness-Armbaendern-und-Smart-Watches.html (Abgerufen: 23.3.2017).

31 *Zickau*, privGardens – Semantic Privacy Areas in Location-based Data Protection Policies, 13. GI/KuVS-Fachgespräch "Ortsbezogene Anwendungen und Dienste", Logos Verlag (2016)

32 *Rivest/Lampson*, SDSI-a simple distributed security infrastructure, Crypto, 1996; *Dwaine* et al., Certificate chain discovery in SPKI/SDSI, Journal of Computer security 9.4 (2001), S. 285-322.

33 *Ninghui/Winsborough/Mitchell,* Distributed credential chain discovery in trust management, Journal of Computer Security 11.1 (2003), S. 35-86.

(2) WADA.nado -> NADA, USADA, ...
(3) NADA.dco -> DCO1
(4) NADA.dco -> DIENSTLEISTER.dco
(5) DIENSTLEISTER.dco -> DIENSTLEISTER.angestellter
(6) DIENSTLEISTER.angestellter -> DCO2
Eine Delegation wie bei (1) bedeutet, dass ein Teilnehmer »PARADISE« das Attribut »user« an alle Entitäten delegiert, die von einer von der WADA anerkannten NADO das Attribut »dco« erhalten haben. WADA wiederum delegiert das Attribut »nado« an die jeweiligen anerkannten NADOs (2). Bei der Auflösung des Attributs PARADISE.user ist es nun irrelevant, ob bspw. NADA das Attribut »dco« an einen Teilnehmer (3) oder an einen externen Dienstleister delegiert (4). Diese Situation ist jedoch durchaus relevant und kann abgebildet werden,

Die jeweiligen ausgestellten Attribute werden in einem verteilten System gespeichert und entweder dem Aussteller oder dem Ausgestellten zugeordnet. Sobald eine Autorisierungsentscheidung getroffen werden muss, z. B. anhand des Attributs »PARADISE.user«, wird eine Delegationskette gesucht. Ausgehend vom zu autorisierenden Nutzer (DCO2) zum jeweiligen Attribut (PARADISE.user). Dieser Prozess wird als »Credential Chain Discovery«[34] bezeichnet.

Das PARADISE-Projekt verfolgt den Ansatz, Delegationen in einem dezentralen, sicheren Namenssystems[35] zu speichern und diese auch aufzulösen. Durch ein offenes Namenssystem ist es jedem Teilnehmer möglich, beliebige Attribute auszustellen und zu delegieren. Gleichzeitig werden zentrale Speicherinstanzen unnötig. Durch die Auswahl eines geeigneten Namenssystems und der Implementierung effizienter Discovery-Algorithmen besticht die PARADISE-Plattform mit einem modernen attributbasierten Autorisierungskonzept.

3.2.4 Umsetzung der Datenschutzanforderungen mit der Sealed Cloud Technologie

Die PARADISE-Plattform benötigt neben den Eves-Devices für die Athleten und den, auf die verschiedenen Rollen (Athleten, DCO, NADA) zugeschnittene Nutzungsoberflächen, die Möglichkeit einer sicheren Datenverarbeitung. Eine sichere Datenverarbeitung könnte entsprechend herkömmlicher Sicherheitskonzepte mit einer sorgfältigen Rolleneinteilung und weiteren organisatorischen Maßnahmen in einem klassischen Rechenzentrum umgesetzt werden. Bei dieser Vorgehensweise wird versucht, im Wesentlichen mit Maßnahmen der Zutritts- und Zugangskontrolle das Problem der Zugriffkontrolle zu lösen. Eine solche Cloud kann nur für geringere Schutzbedarfe genutzt werden. Ein vorsätzlich handelnder Mitarbeiter des Betreibers der Plattform, sowie Software-Administratoren können bei einer solchen herkömmlichen Cloud immer Kenntnis von (besonders schützenswerten) Daten erlangen.[36] Bei hohem Datenschutzbedarf oder bei der Verarbeitung von Berufsgeheimnissen durch Dritte, wie er im Projekt PARADISE gegeben ist, kann auf Schutz vor vorsätzlichem Handeln beim Betreiber nicht verzichtet werden.[37]

Da vorsätzliches Handeln durch organisatorische Maßnahmen und Strafandrohung nur ungenügend unterbunden werden kann, sind zur Erfüllung der Anforderungen im Projekt PARADISE so genannte PETs auch in Bezug auf die Datenverarbeitung anzuwenden. Eine Sealed Cloud entschlüsselt und verarbeitet die Daten nur innerhalb einer besonders gesicherten, »Data Clean-up Area« genannten, Umgebung. Ein Sealed-Cloud-Datenzentrum ist in mehrere Segmente unterteilt. Jedes dieser Segmente ist logisch und physisch vor Zutritt und Zugang geschützt. Durch elektro-mechanische Sicherungen erhalten Mitarbeiter immer nur zu einem dieser Segmente Zugang. Sowohl bei einem geplanten Zugriff durch Mitarbeiter als auch bei einem ungeplanten Zugriffversuch (Angriff) wird durch entsprechende (fehlersichere) Alarme ein so genannter »Data Clean-Up« ausgelöst. Das bedeutet, dass die aktiven Sitzungen der Cloud-Nutzer auf ein nicht betroffenes Segment des Rechenzentrums verschoben und alle Daten im betroffenen Segment gelöscht werden. Dies erfolgt bei Sealed Cloud so gründlich, dass sogar für 10 Sekunden die Stromversorgung von den Anwendungsservern, ohne persistenten Speicher, genommen wird, damit auch keine Eis-Spray-Attacken auf den flüchtigen Speicher möglich sind. Bei Wiederanlauf erfolgt ein Integritäts-Check über den gesamten Software-Stack, d. h. vom gehärteten Betriebssystem ausgehend über alle Software-Schichten bis zur Anwendungssoftware. Wenn durch einen wartenden Ingenieur nicht-zertifizierte Software eingespielt würde, könnte der Anwendungsserver nach schließen des Segments nicht neu starten. Die Schreibeschlüssel, die verwendet werden, um Daten persistent in Datenbanken oder Dateisystemen zu speichern, werden aus den Geheimnissen, z. B. den Zugangsdaten der Nutzer, dynamisch bei jeder Sitzung neu erzeugt und liegen dem Betreiber oder den Administratoren nicht vor. Anders als bei einem herkömmlichen Serverbetrieb, bei dem der Betreiber die Daten ohnehin lesen könnte, muss bei Sealed Cloud die Verschlüsselung der Übertragung der Daten in die Cloud mit »Perfect Forward Secrecy« ausgestattet sein, sodass auch der Betreiber der Server die übertragenen Daten nicht lesen kann. Niemand außer den vorgesehenen Nutzern kann Zugriff zu den verarbeiteten Daten erlangen.[38]

Bei der Sealed Cloud Technologie sind keine Beschränkung auf bestimmte Anwendungen hinzunehmen. Der ökonomische Vorteil des Sealed Cloud Ansatzes ist, dass nicht mehr Rechenleistung als herkömmlich eingesetzt werden muss, und trotzdem die Vertraulichkeit der Daten auch bei der Verarbeitung gewährleistet werden kann. Auch rechenintensive Datenverarbeitung kann hoch-performant durchgeführt werden.

Alle Server-Komponenten des Projekts PARADISE werden in einer Sealed Cloud betrieben. Die notwendigen Anforderungen an die Software-Komponeten, damit eine Verarbeitung in einer Sealed Cloud möglich ist, entsprechen weitgehend der »best practice« bei der Entwicklung von sicheren Anwendungen.

34 *Dwaine*, et al., Certificate chain discovery in SPKI/SDSI, Journal of Computer security 9.4 (2001), S. 285-322.

35 *Wachs/Schanzenbach/Grothoff*, A censorship-resistant, privacy-enhancing and fully decentralized name system, International Conference on Cryptology and Network Security, Springer International Publishing, 2014; *Wachs/Schanzenbach/Grothoff*, On the feasibility of a censorship resistant decentralized name system, Foundations and Practice of Security, Springer International Publishing, 2014, S. 19-30.

36 Vgl. *Jäger*, et al., Sealed Cloud – A Novel Approach to Safeguard against Insider Attacks, S. 3 ff., https://www.idgard.de/pdf/Sealed_Cloud_for_WS_on_wissenschaftliche_Ergebnisse_von_Trusted_Cloud.pdf (Abgerufen: 23.3.2017).

37 Vgl. *Kroschwald*, in: Taeger (Hrsg.), Law as a Service, Tagungsband DSRI Herbstakademie 2013, S. 301 f.

38 *Jäger*, Compliance durch versiegelte Cloud, in: Industrie Management 29 (2013) 4, S. 28 f.

3.3 Datenschutzrechtliche Bewertung des PARADISE-Lösungsansatzes

Die datenschutzrechtliche Beurteilung des ADAMSs anhand des SDMs ermöglicht nun den Lösungsansatz aus dem PARADISE-Projekt einer vergleichenden Prüfung zu unterziehen.

3.3.1 Datenminimierung

Durch den Einsatz von Eves Devices werden unter dem PARADISE-Lösungsansatz wesentlich weniger detaillierte Whereabouts erhoben als im aktuellen ADAMS. Eine Speicherung der über Eves Devices abgefragten Standorte erfolgt nicht. Unter dem Gesichtspunkt der Datensparsamkeit stellt das Projekt PARADISE folglich eine deutliche Verbesserung zum bisherigen ADAMS dar.

3.3.2 Verfügbarkeit

Trotz des Fehlens umfassender und detaillierter Whereabouts bleibt die Verfügbarkeit der Whereabouts durch die Nutzung von Eves Devices gesichert. Auch bei vergessenen Eintragungen sind Athleten für einen DCO auffindbar. Die Akzeptanz der PARADISE-Plattform steigt durch offensichtliche Transparenz, weshalb die Verfügbarkeit gegenüber dem ADAMS gesteigert wird.

3.3.3 Integrität

Die Sealed Cloud Technologie schützt vor unbefugter Veränderung der Daten. Aufgrund eines transparenten Loggings ist nachvollziehbar was von wem geändert worden ist. Die auf die Bedürfnisse der Akteure zugeschnittenen Zugriffsberechtigungen beugen Missbrauch vor. Somit stellt das Projekt PARADISE – im Gegensatz zu ADAMS – sicher, dass die Integrität der sensiblen Athletendaten gewährleistet wird.

3.3.4 Vertraulichkeit

Um die Vertraulichkeit zu schützen setzt das PARADISE-Projekt – im Gegensatz zu ADAMS – auf einen anlassbezogenen Zugriff auf die Athletendaten, inklusive Whereabouts. Zudem können individuell angelegte Geofences zukünftig den Kernbereich privater Lebensführung wirkungsvoll schützen. Schließlich gewährleistet die Verwendung der Sealed Cloud Technologie eine sichere Datenverarbeitung in EU-Mitgliedsstaaten. Somit würde mit der Umsetzung des PARADISE-Lösungsansatzes überhaupt erst eine dem Schutzbedarf entsprechende Vertraulichkeit hergestellt werden.

3.3.5 Nichtverkettung

Durch die konsequente Datenminimierung und die Vergröberung von Whereabouts bietet das PARADISE-Projekt wesentlich weniger Angriffspunkte für eine Verkettung von Daten. Die anlass- und rollenbezogene Zugriffsberechtigung der verschiedenen Akteure stellt zudem sicher, dass die Verkettung von Daten auf das möglichste Maß erschwert wird.

3.3.6 Intervenierbarkeit

Das transparente Logging und die Nutzung der Sealed Cloud Technologie ermöglicht für die Athleten eine einfach benutzbare Einsicht in Zugriffsdaten und damit umfassende Transparenz. Zudem können für vollständige Auskunftsrechte weitergehende Prozesse leicht implementiert werden.

3.3.7 Transparenz

Durch die Logging Funktion der PARADISE-Plattform können Athleten auch ohne den Rückgriff auf ihre gesetzlichen Auskunfts- und Benachrichtigungsrechte nachvollziehen was mit ihren Daten passiert. Die gleichzeitige Zurverfügungstellung der Software als Open Source stellt die größtmögliche Transparenz für die betroffenen Athleten sicher.

3.3.8 Ergebnis der Überprüfung

Mithilfe des SDMs wird deutlich, dass die PARADISE-Plattform unter Einbindung von Eves Devices dem hohen Schutzstandard der Athletendaten gerecht wird. Wesentliche Mängel des ADAMS können behoben werden ohne unangekündigte Dopingkontrollen zu erschweren. Mit der Verfügbarkeit des PARADISE-Lösungsansatzes ist bei einer Bewertung des stets bestehenden Grundrechtseingriffs durch das – gewollte und für den Sport erforderliche – Dopingkontrollsystem mangels Erforderlichkeit von einer Unverhältnismäßigkeit eines Kontrollsystems ohne gezielten Einsatz von PETs auszugehen.[39]

4 Fazit

Stellvertretend für viele Athleten hat die Langsprinterin Ruth Spelmeyer vom VfL Oldenburg in einem Interview mit der Nordwest-Zeitung zusammengefasst, was sie von der Einführung eines verbesserten Systems hält: »Es würde die Kontrollen vereinfachen, weil man nicht mehr nicht angetroffen werden kann. Außerdem ist man nicht so gebunden und braucht keine Angst haben, dass man beim Eintragen mal was vergisst.« [40]

Das war im Oktober 2014 – noch vor dem offiziellen Startschuss von PARADISE. Die frühzeitige Einbeziehung der Betroffenen, sei es durch breit angelegte Online-Befragungen, die Erhebung von Kontextszenarien oder den persönlichen Austausch, hat den Projektverlauf bis heute maßgeblich geprägt.

Das Hauptaugenmerk der Projektverantwortlichen liegt in der Aufrechterhaltung der Balance aus der Verwendung aktueller Technologien zur Sicherstellung von Datenschutz- und Sicherheitsaspekten und deren rechtlicher und soziologischer Bewertung. Genau diese Art der Zusammenarbeit einzelner sorgt dafür, dass nicht an den Bedürfnissen der Anwender – seien es Athleten oder die verantwortlichen Verbände – vorbei entwickelt wird.

Es bleibt zu hoffen, dass die derzeitige öffentliche Aufmerksamkeit in Sachen Doping die Einführung eines sicheren Systems unter Beachtung der rechtlichen Rahmenbedingungen fördert.

39 Vgl. *Schlarmann*, ZD 2016, S. 575.

40 Sprinter jagt Dopingsündern hinterher, NWZ Online, http://www.nwzonline.de/handball/sprinter-jagt-dopingsuendern-hinterher_a_19,0,2264467928.html (Abgerufen: 23.3.2017).