PARADISE – Wie Ortungstechnologien den Datenschutz im Anti-Doping verbessern können

Jonas Plass und Sebastian Zickau

Mit den Ergebnissen des Forschungsprojekts PARADISE[1] wird eine neuartige, alternative Plattform zum derzeit eingesetzten System ADAMS definiert. In PARADISE wurde die Eignung moderner Positionierungstechnologien für den Einsatz im Anti-Doping-Anwendungsbereich evaluiert. Im Fokus stand hierbei die Frage, wie sich Datenschutz und Gebrauchstauglichkeit für AthletInnen mit unangekündigten Dopingkontrollen an verschiedenen Aufenthaltsorten vereinen lassen. Aktive AthletInnen wurden durch ihre Erfahrungen mit dem derzeitigen System motiviert, ein neue Lösung basierend auf dem derzeitigen Stand der Technik zu konzipieren. Der Artikel stellt diese Ergebnisse vor und zeigt, dass sich Datenschutz und Ortungstechnologien nicht ausschließen.

1. DIE PROBLEME DES AKTUELLEN DOPING-KONTROLLSYSTEMS

In Deutschland, aber auch international, werden AthletInnen, die den Wunsch und das Potential haben, an internationalen Wettkämpfen teilzunehmen, einem der vier Testpools (Registered Testing Pool (RTP), Nationaler Testpool (NTP), Allgemeiner Testpool (ATP) und Team-Testpool (TTP)) zugeordnet. Daran geknüpft ist die Pflicht sich den Anti-Doping-Regularien der World Anti-Doping Agency (WADA) und somit auch der Nationalen Anti-Doping-Agentur Deutschland (NADA) zu unterwerfen. Allein in Deutschland sind dies insgesamt 9.000

1 Projekt-Webseite, https://privacy-paradise.de/

AthletInnen aus unterschiedlichen Sportarten, rund 2500 davon in den beiden höchsten Testpools[2] (RTP und NTP).

Neben dem Verbot der Einnahme bestimmter Substanzen sowie der Nutzung bestimmter Methoden der Leistungssteigerung, bedeutet dies für LeistungssportlerInnen u. a. für Wettkampfkontrollen und unangekündigte Trainingskontrollen nahezu jederzeit zur Verfügung zu stehen. Dazu ist es notwendig, dass AthletInnen ihre künftigen regelmäßigen Aufenthalts- und sämtliche Übernachtungsorte bis zu drei Monate im Voraus über eine Online-Schnittstelle im Anti-Doping Administration and Management System (ADAMS) hinterlegen, damit sie bei einer Kontrolle durch den Doping Control Officer (DCO, Dopingkontrolleur) aufgesucht werden können. Kommen die AthletInnen dem nicht nach oder werden sie innerhalb von 18 Monaten drei Mal nicht am angegebenen Aufenthaltsort angetroffen, zieht dies eine Wettkampfsperre nach sich.

In den meisten Ländern, wie auch in Deutschland, sind DCOs nicht direkt bei den NADOs, sondern bei externen Dopingkontroll-Dienstleistern angestellt. Der DCO bekommt jeweils mit einer Vorlauffrist von einigen Tagen bis Wochen Aufträge zugeteilt und kann diese, soweit nicht genauer spezifiziert, selbstständig zu gewünschten Zeiten durchführen. Mit Hilfe der Aufenthaltsdaten der AthletInnen aus dem ADMAS-System muss der DCO eine unangekündigte Kontrolle initiieren und im besten Fall die AthletInnen ohne vorherige telefonische Kontaktaufnahme antreffen. Die Praxis der unangekündigten Kontrollen hängt hauptsächlich damit zusammen, dass Dopingsubstanzen über sehr unterschiedliche Zeiträume im Blut oder Urin nachgewiesen werden können. Zudem lassen sich, bestimmte Substanzen durch Einnahme von weiteren Mitteln maskieren. Generell sollen damit Täuschungsmanöver seitens der AthletInnen verhindert werden, wie z. B. eine Abgabe von vorher injizierten Fremd-Urin. Da dem Erfindungsreichtum bei der Nachhilfe zur Leistungssteigerung fast keine Grenzen gesetzt sind, ist es wesentlich, dass Kontrollen möglichst nicht unterlaufen werden können, je kürzer die Vorlaufzeit bei Tests ausfällt, desto weniger Zeit bleibt für Täuschungsversuche.

Grundsätzlich ist den *Nationalen Anti-Doping-Organisationen* (NADO) die Nutzung von ADAMS nicht vorgeschrieben. Jedoch greifen die meisten, wie auch die NADA, zur Vermeidung von zusätzlichen Aufwendungen auf das kostenlos von der WADA bereitgestellte System zurück.

Die genauen Anforderungen an das Melde- und Testverfahren sind dabei in dem NADA-Dokument „Standard für Meldepflichten“ dokumentiert. Seit der

2 Informationen auf der Webseite der NADA, https://www.nada.de/doping-kontrollsystem/beteiligte-am-kontrollprozess/athletinnen-athleten/

Einführung von ADAMS im Jahre 2005 (2009 in Deutschland) befindet sich das System in der Kritik. DCOs und AthletInnen bemängeln die Gebrauchstauglichkeit, Datenschützer gleichermaßen die Eingriffe in die Privatsphäre und den Umgang mit den gespeicherten Daten. Darüber hinaus bezweifeln Experten, inwieweit das System überhaupt seiner Aufgabe, unangekündigte Dopingkontrollen zu koordinieren und zu initiieren, nachkommen kann, d. h. ob nach einer Kosten-Nutzen-Abwägung die Eingriffe in die Privatsphäre der AthletInnen gerechtfertigt bzw. angemessen sind.

Dieser Artikel beschreibt, wie die Funktionsweise des derzeitige Anti-Doping-System für AthletInnen dazu geführt hat, Betroffene zu motivieren nach technischen Alternativen zu suchen, die sowohl aus der Sicht des Datenschutzes als auch der Gebrauchstauglichkeit tragbar sind. Es werden sowohl rechtliche Problemstellungen als auch technische Lösungsansätze allgemeinverständlich beschrieben. Diese werden verdeutlichen, dass Datenschutz und Ortungstechnologien sich nicht gegenseitig ausschließen. Zunächst sollen daher nun die einzelnen Kritikpunkte am ADAMS-System genauer beleuchtet werden, um darauf aufbauend die Ideen für eine Neukonzeption eines Systems für die Verwaltung von *Whereabouts* (Aufenthaltsorte) vorzustellen.

1.1 Gebrauchstauglichkeit von ADAMS

Gebrauchstauglichkeit beschreibt das Ausmaß, in dem ein Produkt, System oder ein Dienst durch bestimmte Benutzer in einem bestimmten Anwendungskontext genutzt werden kann, um bestimmte Ziele effektiv, effizient und zufriedenstellend zu erreichen (ISO-9241 2006). Aus Gründen der Vereinfachung sollen hier lediglich die Benutzer *AthletIn* und *Dopingkontroll-Instanz* betrachtet werden.

Eines der grundlegenden Probleme an ADAMS ist, dass es nicht explizit für die Anwendungsdomäne Anti-Doping entwickelt wurde. Stattdessen griff die WADA auf eine bestehende Softwarelösung aus einem anderen Nutzungskontext zurück, die seitdem stetigen Anpassungen unterliegt. Ob dies die Tatsache begründet, dass es keinerlei Schnittstellen zu anderen Systemen bietet oder ob es am Willen der betreibenden Institution (WADA) mangelt, ist nicht bekannt. Grundsätzlich steht es den NADOs frei, ADAMS oder ein vergleichbares System zu nutzen. Da es jedoch vorgeschrieben ist, dass die Aufenthaltsorte der letzten sechs Monate vor Olympischen Spielen von potentiellen TeilnehmerInnen in ADAMS hinterlegt sein müssen, sind NADOs, die ein eigenes System betreiben, gezwungen diese Daten manuell zu über-tragen. Dieser Medienbruch ist nicht nur immens ineffizient und höchst fehleranfällig.

DCOs nutzen zur Planung und Durchführung der Kontrollen die hinterlegten Aufenthaltsorte der AthletInnen. In der Praxis muss jedoch bedacht werden, dass der Grad der Gebrauchstauglichkeit für DCOs zu Lasten der Gebrauchstauglichkeit für AthletInnen geht. Je mehr Informationen dem DCO zur Verfügung stehen, desto leichter ist es die AthletInnen anzutreffen. Wird der Alltag der AthletInnen jedoch nicht detailliert im Vorhinein in ADAMS hinterlegt, reduziert dies die Gebrauchstauglichkeit auf Seiten der DCOs. Dies hat nicht selten unnötig gefahrene Kilometer bzw. Suchen und Warten zur Folge. Darüber hinaus torpediert dies möglicherweise die Effektivität des Gesamtsystems, nämlich dann, wenn der DCO zum Telefon greifen muss, um sich nach dem aktuellen Aufenthaltsort der AthletInnen zu erkundigen und diese somit „vorzuwarnen". In Gesprächen mit DCOs ist zu erfahren, dass diese sich nicht selten zusätzlich zu ADAMS den Profilen der sozialen Medien der zu testenden AthletInnen bedienen, um weitere Informationen über deren Aufenthaltsorte zu erlangen.

AthletInnen selbst empfinden die Meldeerfordernisse als ein Damoklesschwert, das permanent über ihnen zu hängen scheint. Zunächst müssen die Angaben bis zu 3 Monate im Voraus in ADAMS eingepflegt werden. Verpflichtend sind dabei Informationen zu regelmäßigen Tätigkeiten wie Trainingsstätten, Ausbildungs- oder Arbeitsstelle sowie Übernachtungsorte für das gesamte Quartal. Die größere Bürde stellt jedoch das permanente Überarbeiten und Aktualisieren der hinterlegten Daten dar. Da die AthletInnen selbst für die Aktualität ihrer Daten verantwortlich sind und ggf. mit *Missed-Tests* (Versäumter Test) bestraft werden können, verlieren sie Spontanität im Alltag oder müssen ADAMS gezwungenermaßen als ständigen Begleiter „mit sich nehmen".

Unter Beachtung der eingangs erwähnten ISO-Norm, kann eine Bewertung von ADAMS bezüglich seiner Gebrauchstauglichkeit nur nüchtern ausfallen. (Herber 2017)

Datenschutz/Privatsphäre

Da AthletInnen die Unzulänglichkeiten des Systems im Zusammenhang mit der Gebrauchstauglichkeit tagtäglich erleben, rücken die mit dem System in Verbindung stehenden Datenschutzprobleme in den Hintergrund oder werden schlichtweg nicht bedacht. Wie das Datenschutz-Paradoxon vermuten lässt, ist auch AthletInnen der Schutz ihrer Daten grundsätzlich immens wichtig, sie scheinen sich allerdings vielfach mit der aktuellen Situation abgefunden zu haben bzw. "hineingewachsen" zu sein. Verantwortliche Institutionen sollten allerdings dafür Verantwortung tragen, dass der Schutz der Athletendaten gewährt ist. Wird zur datenschutzrechtlichen Analyse das *Standard-Datenschutzmodell* (SDM) herangezogen, lässt sich die äußerst prekäre Situation im Anti-Doping erkennen.

Das SDM beschreibt eine Methode, mit der die Übereinstimmung von Anforderungen des Datenschutzrechts und technisch-organisatorischen Funktionen personenbezogener Verfahren in Deutschland überprüfbar wird.

Datenminimierung

Um feststellen zu können inwiefern dem Gewährleistungsziel der Datenminimierung nachgekommen wird, ist zunächst herauszufinden, welche Daten überhaupt in ADAMS hinterlegt sind. Laut „Anlage 1 zum Standard für Datenschutz" handelt es sich dabei um Athletendaten wie Name, Geburtsdatum, Sportart, Kontaktadressen, aber eben auch detaillierte Angaben zu Aufenthaltsorten und Verfügbarkeit. Über diese personenbezogenen Angaben hinaus werden des Weiteren auch medizinische Informationen wie TUEs (*Technical Use Exceptions* = medizinische Ausnahmeregelungen), Kontrollunterlagen und –Ergebnisse sowie Blutpassdaten gespeichert. Diese unterliegen nach Datenschutzgesetz einem besonderen Schutzniveau. Sofern die Erhebung, Verarbeitung und Vorhaltung dieser Daten zwingend erforderlich sind, d. h. eine Zweckbindung vorliegt, ist sie absolut vertretbar. Jedoch werden die Daten zu Aufenthaltsort und Verfügbarkeit theoretisch 1,5 Jahre, in der Praxis allerdings oftmals auch deutlich länger vorgehalten. Eine Löschung zum Ende des aktuellen Tages oder zumindest nach erfolgreich abgeschlossener Kontrolle würde dem eigentlichen Zweck, der Erhebung und Verarbeitung für ein unange-kündigtes Antreffen der AthletInnen, nicht im Wege stehen. Kritisch anzumerken ist darüber hinaus auch, dass Löschungsrechte, auch deutscher AthletInnen, ausschließlich bei der WADA und nicht bei der NADA selbst liegen. Dem Gewährleistungsziel der Datenminimierung wird demnach im aktuellen System nicht nachgekommen.

Verfügbarkeit

Das SDM-Prinzip der Verfügbarkeit macht es erforderlich, dass die erhobenen und gespeicherten Daten nicht nur der Zweckbindung unterliegen, sondern für diesen auch uneingeschränkt zur Verfügung stehen und ordnungsgemäß im vorgesehenen Prozess eingebunden werden. Im beschriebenen Kontext müssen die erhobenen *Whereabouts* es der NADA bzw. deren Dienstleistern ermöglichen die AthletInnen für unangekündigte Dopingkontrollen aufzufinden. Wie die Jahresberichte der NADA zeigen[3], ist es bei in ca. zehn Prozent der geplan-

3 2014: 8.652 Trainingskontrollen, 642 Nicht erfolgte Kontrollversuche (NEKV), 303 Missed Tests; 2015: 7.835 Trainingskontrollen, 462 NEKV, 258 Missed Tests; 2016: 7.495 Trainingskontrollen, (NEKV nicht angegeben), 365 Missed Tests

ten Dopingkontrollen nicht möglich die AthletInnen anzutreffen. Dies bedeutet einen zusätzlichen administrativen Aufwand.

Integrität

Das Gewährleistungsziel Integrität erfordert die Unversehrtheit, Vollständigkeit und Aktualität der erhobenen und vorgehaltenen Daten. Vor den Olympischen Spielen in Rio veröffentlichte die Hackergruppe *Fancy Bear* TUE-Daten von AthletInnen[4]. Wie bekannt wurde, erhielten die Hacker durch Phishing-Mails Zugriff auf Daten in ADAMS. Da das System keinerlei Schnittstellen besitzt, können hinterlegte Daten nicht einfach verändert oder gefälschte Daten hochgeladen werden. Es wäre jedoch denkbar, dass sich auch hier Hacker über Phishing-Mails Zugang zu den Login-Daten der AthletInnen oder NADOs/ WADA / Kontrolldienstleister verschaffen und hinterlegte Informationen manipulieren. Auch wenn es nach Bekanntwerden der Zugriffe durch Fancy Bear bereits Sicherheitsverbesserungen gab, bedarf es hier weiterer Maßnahmen.

Vertraulichkeit

Das Prinzip der Vertraulichkeit erfordert den Schutz vor Zugriff von Unbefugten auf personenbezogene Daten. Dies beinhaltet nicht nur den Zugriff von unberechtigten Dritten, wie Fancy Bear, sondern zusätzlich ein sinnvolles Rollenkonzept, das Daten vor Zugriffen aus dem Personenkreis der Kontrollinstanzen schütz. Im Besonderen ist hier der Zugriff auf Aufenthaltsdaten der AthletInnen zu erwähnen. Wie die NADA erklärt[5], lassen sich die Zugriffsmöglichkeiten auf Whereabouts-Daten nicht einschränken, womit DCOs lediglich Zugriff auf Daten der von ihnen zu kontrollierenden AthletInnen hätten – geschweige denn ausschließlich im vorgegebenen Kontrollzeitraum. Laut eines frei zugänglichen ADAMS-Handbuches besteht jedoch technisch die Möglichkeit *Kontroll-Missionen* zu planen, einzelnen DCOs zuzuweisen und somit pauschal allen anderen DCOs den Zugriff zu verwehren[6]. Das Gewährleistungsziel Vertraulichkeit erfordert klar eine Einschränkung der Zugriffe auf Athletendaten auf ein

4 https://www.wada-ama.org/en/media/news/2016-10/cyber-security-update-wadas-incident-response

5 Scheler, Hackerangriff gegen ADAMS-Plattform, Doping Magazin 3/2017.

6 „When a Testing Authority issues a Mission Order, the organization defined as the Sample Collection Authority (namely the confirmed Lead DCO) automatically gain access to the whereabouts of the athletes in the Mission Order, but only for the days covered by the Mission Order." http://adams-docs.wada-ama.org/display/EN/Viewing+Whereabouts+of+Athletes+in+the+MO Zugegriffen am: 01.06.2018, 13:25 Uhr

notwendiges Minimum. Vor allem wenn es die technische Möglichkeit dazu gibt, sollte diese auch eingesetzt werden.

Nichtverkettung

Das Erfordernis der Nichtverkettung geht einher mit dem Prinzip der Zweckbindung. Notwendige Daten dürfen nur für den erforderlichen Zweck verwendet werden. Sie dürfen nicht durch Verknüpfung mit anderen frei zugänglichen Daten weitere Schlüsse über die AthletInnen, Gewohnheiten oder Vorlieben schließen lassen. Gerade die anlasslose Erhebung und theoretische Datenvorhaltung von 18 Monaten der sensiblen Aufenthaltsdaten ermöglicht zum Beispiel die Erstellung von Bewegungsprofilen, Ableitung von Gewohnheiten, persönliche Kontaktpersonen, Religionszugehörigkeit u.v.m. Aufgrund der Sensibilität der Daten bedarf es an dieser Stelle einen weitreichenden Nachbesserungsbedarf.

Intervenierbarkeit

Das Prinzip der Intervenierbarkeit innerhalb des SDM stellt sicher, dass die AthletInnen von ihrem Recht auf Benachrichtigung und Auskunft gegenüber der datenerhebenden bzw. verarbeitenden Stelle Gebrauch machen können und ggf. in den Gesamtprozess – von der Erhebung bis zur Löschung – eingreifen dürfen. Fraglich ist hier allerdings, ob die NADA oder die WADA die verantwortliche Institution ist. Die WADA verweist bei Fragen auf die jeweilige NADO, die NADA selbst scheint jedoch keinerlei Rechte bzw. Möglichkeiten zu haben, Daten deutscher AthletInnen zu löschen. Auf eine Anfrage, wann bzw. nach Ablauf welcher Frist die Daten von zurückgetretenen AthletInnen gelöscht werden, erwiderte die WADA lediglich „*athlete accounts are 'retired' when athletes retire (Wenn die AthletIn in den Ruhestand geht, wird auch ihr ADAMS-Zugang stillgelegt.")*.

Den AthletInnen stehen somit im Grunde nur zwei Möglichkeiten zur Intervention zur Verfügung, die *Nicht-Unterzeichnung der Athletenvereinbarung* oder die *Rücktrittserklärung aus dem Hochleistungssport*. Hier kommt jedoch die Unterschriftsverweigerung einer Rücktrittserklärung gleich.

Transparenz

Um der Vorgabe der Transparenz gerecht werden zu können, müssen sowohl AthletInnen als auch Betreiber erkennen, welche Daten für welchen Zweck erhoben und verarbeitet werden. AthletInnen wird in ADAMS jedoch keinerlei Möglichkeit eingeräumt zu erkennen, welche Personen zu welchem Zeitpunkt auf ihre Daten zugegriffen haben. Natürlich ist nachvollziehbar, dass der Zweck der Vorbereitung von unangekündigten Dopingkontrollen oberste Priorität ein-

geräumt wird. Es gibt allerdings technische Möglichkeiten diesem Gewährleistungsziel, wenn auch nicht vollumfänglich, nachzukommen.

Fazit

Wie sich unschwer erkennen lässt, wird ADAMS den Anforderungen zum Umgang mit personenbezogenen Daten der AthletInnen unter keinem der sieben Schutzziele des SDMs gerecht. Was die Situation allerdings noch weiter verschlimmert ist zum einen, dass offensichtlich die technischen Möglichkeiten vorhanden sind, um die Zugriffe der DCOs einzuschränken, diese jedoch nicht genutzt werden, und zum anderen, dass der NADA bei der Durchsetzung der Löschfristen deutscher Athletenprofile die Hände gebunden sind, da sie in der Verarbeitungshoheit der WADA liegt.

Gerade unter Berücksichtigung der ab Mai 2018 europaweit gültigen *Datenschutz-Grundverordnung* (DSGVO) und den dadurch geforderten Prinzipien *Privacy-by-Design* und *Privacy-by-Default* (nähere Informationen in Kapitel 6) wird die Dringlichkeit einer grundlegenden Überarbeitung des Kontrollsystems deutlich.

1.2 Effektivität

Auf der einen Seite stehen AthletInnen, die teilweise aus Gründen der Gebrauchstauglichkeit die bestehenden Regularien so weitreichend wie möglich auslegen und die Angaben meist auf das geforderte Minimum oder in Einzelfällen sogar deutlich weniger beschränken. Auf der anderen Seite stehen DCOs, die mit diesem Minimum an Informationen auskommen müssen, um AthletInnen für unangekündigte Dopingkontrollen (d. h. im besten Falle ohne telefonische Kontaktaufnahme) aufzufinden. Da es sich bei diesen oft um Freiberufler handelt, die nur einige Kontrollen im Monat durchführen, ist es durchaus verständlich, dass diese den für sie einfachsten Weg gehen und die AthletInnen frühmorgens zuhause kontrollieren.

Hat ein Athlet nur einige wenige Angaben hinterlegt, erhöht er dadurch die Wahrscheinlichkeit an „seinem Wunschort" zur „Wunschzeit" kontrolliert zu werden. Verständlicherweise ist kein DCO bestrebt unnötigerweise auf die Suche nach einer AthletIn zu gehen. Alternativ ist auch der Einsatz des Mobiltelefons zur Vereinbarung einer „Kontroll-Verabredung" nicht selten. Unter Berücksichtigung dieser Tatsachen ist jedoch fraglich, in welchem Grade dem Bestreben nach unangekündigten Kontrollen dann wirklich nachgekommen wird.

Diese Unzulänglichkeiten waren Ausgangspunkt für unseren Forschungsansatz zur Schaffung eines – zunächst ergänzenden – Systems *eves* für die Ortsbestim-

mung von AthletInnen, um den Datenschutz und die Anbahnung von Dopingkontrollen zu verbessern.

2. VON EVES ZU *PARADISE*

Vor allem die mangelnde Gebrauchstauglichkeit des Systems auf der Seite der AthletInnen war Ausgangspunkt für Jonas Plass, im Zuge seines Masterstudiums in Medienmanagement und Entrepreneurship, ab 2014 eine Alternative zu konzipieren.

Seit Einführung von ADAMS hat sich der Stand der Technik deutlich weiterentwickelt. Mobile Lösungen und damit verbunden der Einsatz von Lokalisierungstechnologien hatten Einzug in den Alltag genommen. In seinem Business Plan konzipierte Plass das System somit als Smartphone-Anwendung (App). Ein DCO sollten mittels einer kooperierenden Tablet-App in die Lage versetzt werden, den aktuellen Aufenthaltsort der AthletInnen über deren Smartphones abzufragen. Da der Schwerpunkt des Businessplans auf betriebswirtschaftlichen Gesichtspunkten lag, wurde die technische Umsetzung lediglich in Grundzügen skizziert. Zusammen mit dem erfahrenen Startup-Gründer Dr. Denis Giffeler beschlossen sie das Projekt *eves* weiter voran zu treiben. Es folgten Gespräche mit Dr. Michael Sprenger (Gebrauchstauglichkeit), Karin Schuler (Datenschutz) und Mario Hoffmann (Datensicherheit). Gemeinsam gab man der Grundidee *eves* den Feinschliff, auf dem später PARADISE[7] aufbauen sollte. Nachdem das Konzept ausgearbeitet war, wurde es der NADA vorgestellt.

Ziel des Vorgängerprojekts *eves* war es zwischen 2014 und 2016, unter Verwendung bewährter und allgemein verfügbarer Ortungstechnologien das unangekündigte Zusammentreffen zwischen DCO und AthletIn zu vereinfachen. Für die LeistungssportlerInnen sollte durch den Einsatz von *eves* ein Zugewinn an persönlicher Freiheit und durch datensparsamere Meldeerfordernisse ein deutlich verbesserter Schutz der Privatsphäre erreicht werden. Für die nationalen und internationalen Anti-Doping-Institutionen sollte der Einsatz von *eves* eine Zeit- und damit auch eine Kostenersparnis bei der Durchführung von Dopingkontrollen sowie eine erhöhte Akzeptanz bei den AthletInnen bewirken.

Ein sogenanntes *eves-Device* (Gerät) sollte die von den AthletInnen in ADAMS hinterlegten Whereabouts zunächst ergänzen. Es war nicht geplant ein eigenständiges, neues System zu entwickeln. Auch bei Abweichungen zwischen

7 Auf der Projektwebseite, https://privacy-paradise.de/wp-content/uploads/sites/9/2016/11/Dr.-Giffeler.pdf (Aufgerufen 21.10.2018)

den Angaben und dem tatsächlichen Aufenthaltsort, z. B. bei spontanen Reiseänderungen, bei Streik, Krankheit oder familiären Verpflichtungen, sollte der DCO mit Hilfe von *eves* die AthletIn dennoch finden können.

Gleichzeitig sollte der Einsatz von *eves*, die AthletInnen davor schützen aus Angst vor spontanen Aufenthaltsänderungen, potenzielle Aufenthaltsorte in zu großer Zahl in ADAMS zu hinterlegen.

Geplant war eine dafür übliche Client-Server-Architektur mit einem tragbaren Gerät (Wearable) für AthletInnen (Putschli 2017), einer Web-Anwendung für Kontrollinstanzen (Kontrollplaner und DCOs) und einem Server-Backend mit Anbindung an ADAMS.

Das tragbare Gerät sollte speziell an die Bedürfnisse von AthletInnen angepasst werden. Mit seiner Hilfe sollte der autorisierte DCO – und nur dieser – bei einer anstehenden Kontrolle den Aufenthaltsort der AthletIn ermitteln können. Nach Empfang einer Positionsanfrage über einen dedizierten verschlüsselten Kanal sollte es die aktuelle Position mittels Satellitennavigation oder kombinierter Satelliten- und Mobilfunk-Positionierung (GNSS oder AGPS) prüfen. Bei fehlender, aktueller Position, sollte die letzte verfügbare Position oder eine Fehlermeldung auf demselben Weg wie die Anfrage übermittelt werden. Die letzte verfügbare Position sollte in einem internen Speicher für ein Wertepaar, bestehend aus Längen- und Breitenangabe, vorgehalten werden. Lediglich der autorisierte DCO sollte in der Lage sein, eine Standortanfrage zu stellen. Mit der Übermittlung einer neuen Position sollte die vorherige Position überschrieben werden. Die Erstellung von Bewegungsprofilen wäre somit ausgeschlossen worden. Zusätzlich sollten sämtliche Anfragen protokolliert werden und nach einer erfolgreich abgeschlossenen Kontrolle den AthletInnen im System zur Einsicht gewährt werden.

Für DCOs sollte eine Webschnittstelle zur Verfügung gestellt werden, mit der sie sich von zu Hause oder mobil via Tablet über einen Browser in das System einloggen können, ihre Kontrollaufträge in einer Listenansicht angezeigt bekommen hätten und mit einem einfachen Klick den aktuellen Aufenthaltsort der AthletIn abrufen können. Da das *eves*-System lediglich als Ergänzung zu ADAMS angedacht war, hätten DCOs dieses weiterhin zur Planung der Kontroll-Touren nutzen können, um hinterlegte Aufenthaltsorte mit den tatsächlichen Orten abzugleichen.

Das Server-Backend sollte in zertifizierten Rechenzentren betrieben werden. (Herber 2017) Innerhalb des Servers sollte den einzelnen AthletInnen ein eindeutiges Gerät zugeordnet sein. Anfragen sollten über gesicherte Verbindungen (https) entgegengenommen werden. Die Weiterleitung der Anfrage selbst sollte über SMS (Short Message Service) an das jeweilige Endgerät erfolgen. Als

Antwort sollten Längen- und Breitenangaben der letzten Position der AthletIn oder eine Statusmeldung zurückgeliefert werden. Protokolliert werden sollte dabei der Zeitpunkt und Autorisierung des anfragenden DCO, der Status und die Erreichbarkeit des *eves-Devices*. Der Server sollte auch Meldungen des *eves-Devices* zum Zustand des Systems, z.B. bei einem kritischen Ladezustand der Batterie, über SMS entgegennehmen.

Darüber hinaus sollte dem *eves*-Server die wichtige Aufgabe der Zugriffskontrolle zukommen. Lediglich autorisierten DCOs sollte in einem begrenzten Zeitraum eine Positionsanfrage möglich sein.

Um die Umsetzbarkeit und Vorteile eines solch neuartigen Systems zu demonstrieren, war eine erste prototypische Entwicklung geplant. Da die Unterstützung der NADA lediglich auf ideeller Ebene erfolgte, versuchte das Projektteam Gelder aus der Wirtschaft zu akquirieren. Zeitgleich wurden mehrere Anträge zur Unterstützung des Projektes beim IOC-Medical-Funds eingereicht. Die Bestrebungen blieben allerdings ohne Erfolg.

Ende 2014 veröffentlichte das Bundesministerium für Bildung und Forschung (BMBF) die Ausschreibung "Datenschutz: selbstbestimmt in der digitalen Welt" zur Unterstützung von Forschungsinitiativen auf dem Gebiet des Selbstdatenschutzes im Rahmen des Förderprogramms „IKT 2020 - Forschung für Innovationen".

In kurzer Zeit gelang es ein schlagkräftiges Projektteam zusammenzustellen. Mit dem Landesdatenschutzzentrum Schleswig-Holstein (ULD), dem Fraunhofer FIT und dem Fraunhofer AISEC, der Technischen Universität Berlin mit dem Fachgebiet Service-centric Networking, der Uniscon GmbH und der Gekko mbH konnten sämtliche für das Projektvorhaben notwenigen Expertisen vereint werden. Sowohl das Team, als auch der vorliegende Anwendungsfall konnten das BMBF überzeugen. Der offizielle Startschuss für das Projekt PARADISE (*Privacy-enhancing and Reliable Anti-Doping Integrated Service Environment)* fiel im Januar 2016. Das multidisziplinäre Projekt hatte das Ziel, die Privat-sphäre, die Sicherheit und die Gebrauchstauglichkeit der Anti-Doping-Koordinierungsplattform zu verbessern.

3. PARADISE: TECHNISCHE ERGEBNISSE

Im Projekt PARADISE wurde evaluiert, wie sich moderne Positionierungstechnologien für den Einsatz im Anwendungsbereich Dopingkontrollen eignen. Jeder Smartphone-Besitzer kennt die Vorzüge dieser Technologien, sei es bei der Nutzung von Navigations- und Stauinformationen oder bei der Suche nach ei-

nem Restaurant in seiner Umgebung. Die Übertragung von Positionsinformationen an Dritte ist nur einem Teil dieser Nutzergruppe bewusst, dies ist nicht nur bei der Nutzung von Kartendiensten der Fall, sondern auch, wenn man seine Position mit einer Freundin über eine App teilt. Mit der Nutzung von Smartwatches und preiswerten kleinen *Wearables* wurde der Anwendungsbereich für ortsbezogene Dienste noch erweitert. Es werden Dienste angeboten, mit der Hund, Kinder und ältere Menschen digital verfolgt werden können.

Dies wirft zwingend Fragen zum Thema Datenschutz auf, da unter Umständen den Beteiligten und Betroffenen nicht klar ist, welche Informationen durch wen verarbeitet und zugänglich gemacht werden, d. h. welche Firma oder welcher Personenkreis unter Umständen Zugriff auf Ortsdaten von NutzerInnen hat.

Unangekündigte Dopingkontrollen sind seit ihrer Einführung stets im Fokus des Datenschutzes, weil sensible Informationen über AthletInnen einem Benutzerkreis zugänglich gemacht werden über den meist Unklarheit herrscht. Es scheint zunächst, dass die Nutzung von Technologien zum „Orten" der AthletInnen diese Unklarheit und die Implikationen auf den Datenschutz nur noch erhöht.

Im Folgenden wird dargelegt, wie sich ortsbezogene Technologien und sogenannte *Wearables* einsetzen lassen, um den Athletinnen einen höheren Datenschutz zu gewährleisten.

Dabei wird aus technischer Sicht auf folgende Aspekte des Datenschutzes eingegangen: Datenminimierung, Verfügbarkeit, Integrität, Vertraulichkeit, Nichtverkettung, Intervenierbarkeit, Transparenz und Selbst-Souveränität. Die Darstellung der Projektergebnisse von PARADISE beziehen sich in diesem Abschnitt ausschließlich auf die Nutzung von Positionierungstechnologien zur Erhöhung des Datenschutzes (*Privacy-enhancing Technologies, PETs*). Auf die Aspekte der Gebrauchstauglichkeit für AthletInnen und DCOs wird hierbei nur am Rande eingegangen.

Die Grundidee von PARADISE besteht darin, dass die AthletInnen ein Gerät bei sich tragen, welches ihre Position bestimmen kann. Der DCO kann eine Anfrage an dieses Gerät senden und bekommt die aktuelle Position der jeweiligen AthletInnen auf einer Karte angezeigt. Hierbei ergeben sich folgende datenschutzrechtliche Fragestellungen:

- Sendet das Gerät kontinuierlich Positionsdaten an einen Dienst?
- Kann ein DCO oder jemand anderes das System nutzen, um die AthletInnen zu jedem Zeitpunkt zu „verfolgen"?
- Haben die AthletInnen Möglichkeiten diese Anfragen zu unterbinden?
- Welche Dienste und Firmen haben Zugriff auf die Positionsdaten?

- Können die AthletInnen erkennen, wann und vom wem eine Positionsabfrage an das Gerät gesendet wird und somit feststellen, ob evtl. eine Dopingkontrolle bevorsteht?

Bei der Vorstellung der Projektidee kam es oft zu der Annahme, dass das *eves-Device* kontinuierlich in kurzen Zeitintervallen seine Position an einen Dienst sendet und somit Bewegungsprofile der AthletInnen erstellt werden könnten. Diese *pro-aktive* Lösung, dass das Gerät von sich aus Daten sendet, wurde in der Konzeption des PARADISE-Projekts von Beginn an ausgeschlossen. Die PARADISE-Lösung sieht vor, dass eine *re-aktive* Anfrage von außen an das Gerät gestellt werden muss, damit es seine Position an den Dienst sendet. Mit diesem Ansatz wird sichergestellt, dass eine Positionsabfrage tatsächlich nur im Falle einer bevorstehenden Dopingkontrolle durchgeführt werden kann. Der implementierte Ansatz lässt Positionsabfragen nur von DCOs zu, die einen Kontrollauftrag für eine bestimmte Person zugewiesen bekommen und auch angenommen haben (angewendete Prinzipien, Datenminimierung und Nichtverkettung). Nach dem Ablauf einer Frist können die AthletInnen in einem Protokoll des PARADISE-Systems nachvollziehen, wann auf ihre Standortinformationen zugegriffen wurde (Transparenz-Prinzip).

Wenn von dem *eves-Device* gesprochen wird, ist damit ein dediziertes Gerät gemeint, das für die Nutzung durch den PARADISE-Dienst designt und optimiert wurde. Hierfür wurden verschiedene Prototypen entwickelt. Zum einen ist es wichtig, dass die Informationen, die zwischen dem Gerät und dem PARADISE-Dienst ausgetauscht werden, von keiner dritten Instanz abgefangen und gelesen werden können. Zum anderen die Lösung potentiell weltweit einsetzbar sein. Deshalb wurde die Kommunikation mit verschlüsselten Text-nachrichten (umgangssprachlich SMS) abgesichert. Die Nutzung von SMS war auch möglich, da nur wenige Daten übertragen werden. Im Einzelnen sind dies nur Informationen zu GPS- bzw. GSM-Positionen und deren Präzisionswerte.

Ein dediziertes Gerät hat außerdem den Vorteil, dass sich dadurch die Nutzung ohne eine Abhängigkeit von Drittanbietern besser durchführen lässt. Bei der Nutzung einer Smartphone-Applikation, kurz App, ist man abhängig von der Funktionalität sowie den Diensten, die Google mit Android und Apple mit iOS zur Verfügung stellen. Das Betriebssystem und auch die Hardware kann bei einem eigenen dedizierten Gerät selbst gewählt werden, so dass auch nicht proprietäre Software, z. B. in Form von Open-Source-Betriebssystemen, genutzt werden kann. Die Hardwarekomponenten können ebenfalls ausgewählt werden, so dass sie für die Nutzung im vorliegenden Anwendungsfall optimiert werden können, um z. B. Batterielaufzeiten zu erhöhen oder auch Positionierungsproto-

kolle bzw. Standards, die weltweit einsetzbar sind, auszuwählen. Die Absicherung vor Missbrauch durch die AthletInnen kann auf diese Weise ebenfalls besser entgegengewirkt werden.

Die Ausrichtung des PARADISE-Systems ohne Nutzung von Drittanbietern beinhaltet auch die Bereitstellung der Nutzerschnittstelle für AthletInnen, DCOs und NADO-MitarbeiterInnen. Es können eigene PARADISE-Dienste betrieben werden, die das Kartenmaterial zur Verfügung stellen, ohne dabei auf Dienste von anderen Anbietern, wie z.B. *Google Maps*, zurückgreifen zu müssen. Die PARADISE-Server-Dienste wurden im Projekt von einem deutschen Cloud-Anbieter zur Verfügung gestellt, der zusätzliche Absicherungen installiert hat, die es u. a. Mitarbeitern des Unternehmens unmöglich machen, direkt an der Hardware des Dienstes Daten abzugreifen[8]. Beim Zugriff auf das PARADISE-System wurden attributsbasierte Technologien[9] (Schanzenbach 2017) eingesetzt, um Nutzer und Nutzergruppen, anhand einzelner Merkmale unterschiedliche Sichtbarkeiten auf Daten mit den entsprechenden Zugriffsrechten zu gewähren. Zusammen mit der Datenbankstruktur der einzelnen Informationen im System können damit Einschränkungen granular erteilt werden, so dass DCOs oder NADO-MitarbeiterInnen nur die Daten einsehen können, die sie jeweils für ihre Aufgaben zu einem bestimmten Zeitpunkt benötigen (Prinzipien: Datenminimierung, Vertraulichkeit und Integrität).

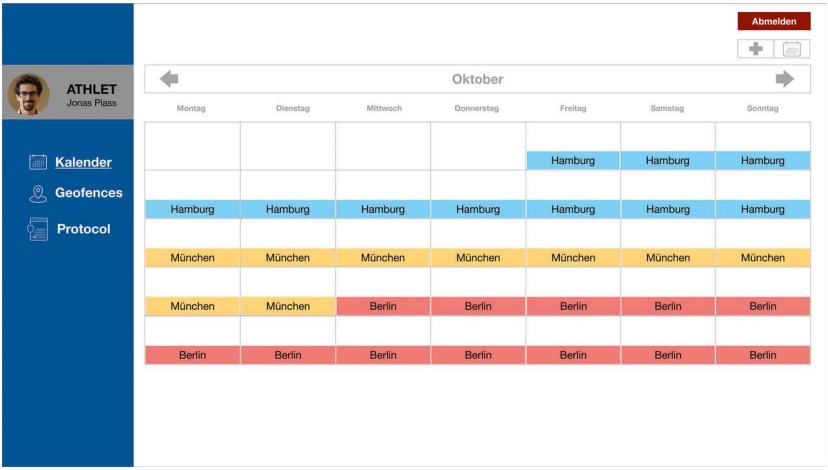
8 Das System kann als *Sealed-Cloud* (versiegelte Cloud) beschrieben werden, siehe dazu auch den Stichpunkt *Vertraulichkeit*.

9 Bei der attributbasierten Zugriffskontroll-Technologien wird der Zugriff auf eine Ressource anhand von Attributen des Benutzers bzw. des Clients, der Ressource, dem Zustand der Systemumgebung, sowie auf diese Attribute angewendeten Sicherheitsregeln gesteuert.

Abbildung 1: DCO-Ansicht, Angabe von Detailinformationen einer Ortsabfrage

Durch dieses Verfahren werden Authentisierung (*Wer sind die NutzerInnen?*) und Autorisierung (*Was dürfen die NutzerInnen?*) geregelt (Ahadipour 2017). Als Beispiel wird hier die Sichtbarkeit der Athletendaten für den DCO beschrieben. Bevor die DCOs einen Kontrollauftrag durchführen können, sehen sie nur sehr grobe Informationen, die helfen sollen einzuschätzen, ob sie den Kontrollauftrag annehmen. Nach Annahme des Auftrags werden weitere Informationen angezeigt und auch die Berechtigung erteilt, nur während des angegebenen Kontrollzeitraums auf die Position der entsprechenden AthletInnen zuzugreifen. Dies könnte noch weiter eingeschränkt werden, in dem z. B. die Anzahl der re-aktiven Abfragen der Position eingeschränkt wurde. Wie bereits erwähnt wird transparent dargestellt, wie oft der Aufenthaltsort der jeweiligen AthletInnen abgefragt wird. Das PARADISE-System wurde unter der Annahme konzipiert, dass eine missbräuchliche Nutzung durch die Aufteilung einzelner Systemkomponenten und Zuständigkeiten verhindert wird und verschiedene Sicherheitsschichten einen Missbrauch ausschließen sollen. Es gibt keinen zentralen Angriffspunkt und Akteur, der dazu genutzt werden könnte, das System entgegen seiner Designentscheidungen zu verwenden, z. B. eine kontinuierliche Ermittlung der Position der AthletInnen. Durch die Verwendung von SMS wird allerdings die Nutzung von Dritten, die Mobilfunk-Anbieter, vorausgesetzt. Diese haben allerdings keinen Einblick in die gesendeten Daten (Verschlüsselung) und haben nur eine eher grobe Einsicht darüber, wer sich wo befindet – ähnlich einer Nutzung von Handys und anderen mobilen Geräten mit SIM-Karte.

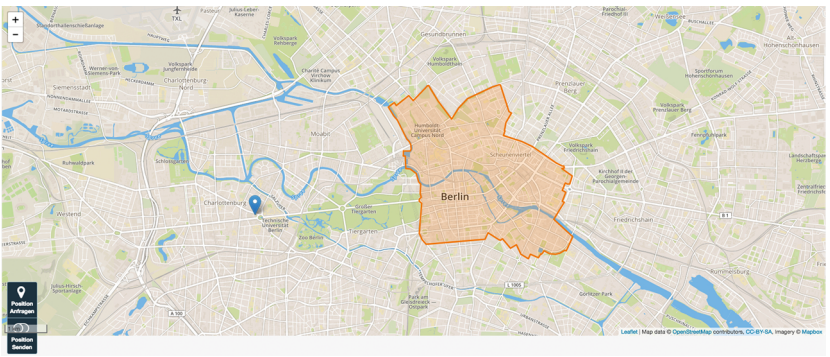
Abbildung 2: DCO-Oberfläche, Whereabouts-Light, d. h. es sind nur Städtenamen bzw. Ortsnamen für den DCO sichtbar, die der Athlet vorher einträgt, um einen ungefähren Aufenthalt anzugeben. Dieses Konzept ist evtl. für die Kontrollplanung nötig und bedarf weiterer Untersuchung.



Im Tagesablauf eines Menschen gibt es Situationen und Orte, die sehr private und sensible Bereiche seines Lebens betreffen, dies können z. B. Arztpraxen, Krankenhäuser, Psychologische Beratungsstellen, religiöse Begegnungszentren, Friedhöfe oder Treffpunkte von Anonymen Alkoholikern sein. Solche Orte können mit sogenannten *Geofences* beschrieben werden. Geofences sind virtuelle Zäune, die aus einer Reihe von GPS-Koordinaten bestehen, welche Polygone beschreiben, die beliebig große Bereiche einer Karte „eingrenzen“ bzw. „einzäunen“. Das System triggert dann Ereignisse je nachdem, ob ein Gerät innerhalb oder außerhalb eines solchen Geofences positioniert ist. In PARADISE wird den AthletInnen die Möglichkeit gegeben diese privaten Zonen bzw. Orte im System anonym zu hinterlegen, so dass bei einer Positionsermittlung mittels *eves-Device*, die Position serverseitig mit den Geofence-Einstellungen verglichen wird und es zu einer Informationseinschränkung für den DCO kommt, sollte sich die AthletInnen innerhalb eines definierten Geofences aufhalten. Um eine neutrale Zuordnung zwischen Ort und Privat-sphären-Raum zu ermöglichen, nutzt PARADISE die Angabe von Postleitzahlengebieten in unterschiedlicher Granularität, d. h. Länge und Kartenbereich zwischen ein bis fünf Stellen der Postleitzahl. Die Zuordnung der Postleitzahlen zu Gebieten in Deutschland ist meist politisch bzw. verwaltungstechnisch motiviert, das heißt es gibt keine semantische Zuordnung von Postleitzahlbereichen zu potentiell sensiblen Orten,

wie Krankenhäusern, Kirchen oder Friedhöfen. Wenn sich die AthletInnen in einem der Geofences aufhalten, wird dem DCO bei einer Positionsabfrage ein fünfstelliges Postleizahlgebiet angezeigt, in dem sich der Athlet mit dem Wearable befindet. Dazu gibt es einen Hinweis, dass die Person sich in einer privaten Zone befindet (Abb. 4). PARADISE sieht vor, dass der DCO entweder versucht die AthletInnen anzurufen, wie es im jetzigen System schon praktiziert wird oder zu einem späteren Zeitpunkt versucht, die AthletIn nochmals genau zu lokalisieren. In PARADISE wurden zwei Notationen von Geofences implementiert. *Allgemeine Geofences*, die gleichermaßen für alle AthletInnen gelten, in denen u. a. Krankenhäuser und religiöse Stätten eingegrenzt sind und *persönliche Geofences*, die die AthletInnen um private Orte legen können. Die letzteren sind in der Anzahl und Größe begrenzt, damit sie nicht dazu „genutzt werden sich vor DCOs zu verstecken“. Die allgemeinen Geofences sollten bei einem Einsatz von PARADISE dann von den jeweiligen NADOs bestimmt werden. Eine AthletIn hat auch die Möglichkeit allgemeine Geofences zu deaktivieren, sollte dies wünschenswert sein, z. B. wenn das Krankenhaus der Arbeitsplatz ist und an diesem Ort auch kontrolliert werden darf (Prinzipien, Intervenierbarkeit und Selbst-Souveränität) (Abb. 5).

Abbildung 3: DCO-Ansicht, grobe Positionsangabe mittels eines Postleitzahl-Gebiets

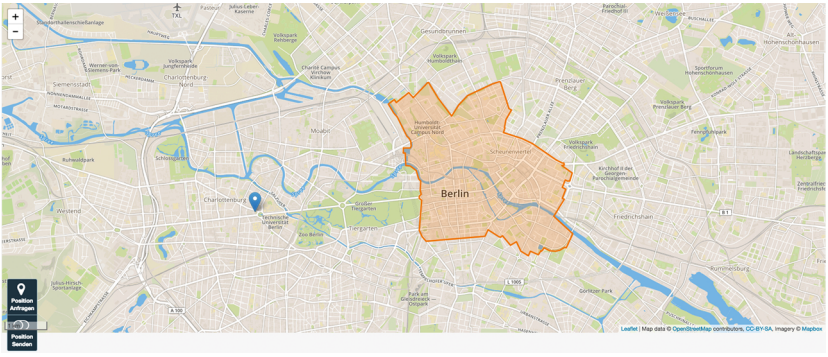


Ein weiterer Einsatz von Postleitzahlgebieten in Bezug auf den Datenschutz von Aufenthaltsorten ist der Vergleich der Position des DCO relativ zu den AthletInnen. Ist die Entfernung der beiden Positionen groß wird dem DCO unabhängig von Geofences nur ein ein- bis fünfstelliges Postleitzahlgebiet angezeigt (Abb. 3), dem er sich im Laufe zusätzlicher Positionsabfragen nähern kann, um eine genauere Position zu erhalten. Hierbei sind die Prinzipien Datenminimierung und Nichtverkettung adressiert, indem nur Informationen angezeigt werden, die für die jeweiligen Situation ausreichend sind. Hält sich der Athlet beispielsweise in

der Mitte Berlins auf und der DCO startet in Potsdam wird dem DCO nur eine grobe Angabe der Position mittels PLZ-Gebiet angezeigt. Nähert er sich dem Athleten an und startet eine neue Abfragen werden wiederum die PLZ-Stellen verglichen, sobald er sich relativ nahe dem Athleten aufhält (z. B. im gleichen fünf-stelligen PLZ-Gebiet oder näher als vier Kilometer) wird die genaueste mögliche Position angezeigt (Abb. 1). Dies ist dann eine GPS- oder GSM-Position mit Präzisionsangabe . Bei sehr großen Entfernungen kann dies dazu führen, dass nur ein einstelliges PLZ Gebiet angezeigt wird, in diesem Fall ist es praktisch ausgeschlossen, dass eine Dopingkontrolle unmittelbar bevorsteht.

Bzgl. Auswertung der zwei Positionen bestehen noch weitere Möglichkeiten, die im Ansatz in PARADISE evaluiert worden sind. Bei einer erfolgreichen telefonischen Kontaktaufnahme des DCO mit AthletInnen ist es üblich ein 60 minütiges Zeitfenster zu setzen, in dem es zu einem Zusammentreffen der beiden Personen kommen muss bzw. soll, um zu gewährleisten, dass den AthletInnen keine Möglichkeiten gegeben wird vor der Dopingkontrolle noch Stoffe einzunehmen, die ein negatives Resultat bewirken würden. Im Kontext von Kartenanwendungen gibt es dafür die sogenannten Erreichbarkeitskarten, auch *isochrone* Karten genannt, die dem DCO anzeigen, wie viel Zeit er benötigt, um zum Zielort der AthletIn zu gelangen. Er kann also z. B. feststellen, ohne die genaue Position der AthletIn angezeigt zu bekommen, wie viele Minuten er mit einem bestimmten Verkehrsmittel benötigt, um die AthletIn zu erreichen. Dies kann ihn bei seiner Entscheidung unterstützen die AthletInnen telefonisch zu kontaktieren. Es ist zu verdeutlichen, dass die telefonische Kontaktaufnahme vor einer Dopingkontrolle nur in Ausnahmefällen genutzt werden soll.

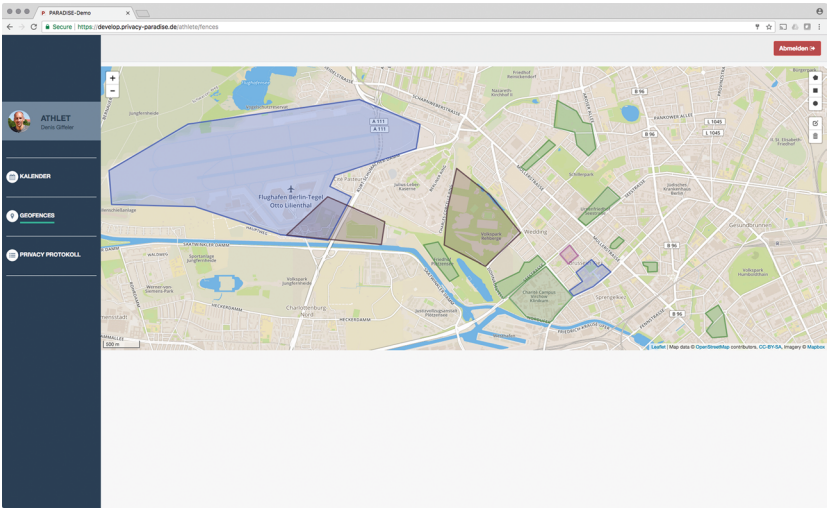
Abbildung 4: DCO-Ansicht, mit dem Hinweis, dass sich ein Athlet in einem Datenschutzgebiet befindet, PLZ-Ortsangabe (rot)



Weiterhin können Geofences dem DCO Zusatzinformationen anzeigen, bevor eine Kontrolle in die Wege geleitet wird. Es können z. B. Positionen des *Wear-*

ables mit den Daten von Bahnhöfen und Flughäfen abgeglichen werden. Dies geht auch mit anonymen Positionsdaten. Im Falle einer Übereinstimmung kann dem DCO angezeigt werden, ob der Athlet bzw. die Athletin evtl. zeitnah in einen Zug oder in ein Flugzeug steigt.

Abbildung 5: Athletenschnittstelle von persönliche und generelle Geofences Gebiete (rot und grün) und Gebiete, in den diese nicht erstellt werden dürfen (blau)



Im Kontext des Projekts wurde auch eine iPad-App für DCOs entwickelt, die neben den genannten Funktionalitäten auch eine selbstentwickelte Navigationssoftware bereitstellt, bei der die Position der AthletInnen bis kurz vor dem Zusammentreffen anonym bleibt. Die beschriebenen technischen Umsetzungen im PARADISE-Projekt sollen verdeutlichen, dass es Konzepte und Technologien gibt, die eine datenschutzfreundliche Nutzung von ortsbasierten Diensten und Wearables für AthletInnen garantieren. Mit den am Beginn des Abschnitts beschriebenen pro-aktiven Tracking-Anwendungen oder sogenannten Fußfesseln hat die PARADISE-Lösung nichts gemein.

4. PARADISE AUS SICHT DER ATHLETINNEN, DCOS UND NADOS

Der vorherige Abschnitt verdeutlicht, wie ein aus Datenschutzsicht entwickeltes Ortungssystem technisch gestaltet werden kann, und wie signifikant es sich von

gängigen Vorstellungen solcher Systeme abgrenzt. In diesem Abschnitt werden bestimmte Nutzergruppen und ihre Aufgaben betrachtet, AthletInnen, DCOs und NADO-KontrollplanerInnen unter Berücksichtigung der Fragestellung, was sich in ihrem täglichen Ablauf jeweils durch den Einsatz des neuen Systems ändern würde.

4.1 Nutzergruppe AthletInnen

Die Lösung ein *eves-Device* ständig mitzuführen, würde AthletInnen dazu verpflichten dieses Gerät einmal täglich aufzuladen, vorbehaltlich von Verbesserungen in der Technologie, die dieses Intervall verlängern könnten. *Eves* als Applikation auf einem Smartphone zu installieren würde hingegen die Akzeptanz stark erhöhen. Während der Projektlaufzeit wurde auch angedacht das *eves-Device* mit einem Smartphone zu koppeln, über das dann Informationen, z. B. zum Batteriestand, der Positionierungstechnologie oder dem allgemeinen Status des Geräts, ausgelesen werden könnten. Zusätzliche Aufgaben sind eine Abschaltung auf Flugreisen, z. B. durch ein Einlegen in ein entsprechendes Gehäuse, damit keine Schalter am Gerät angebracht werden müssten.

Neben diesen Tätigkeiten sind auch Angaben auf der PARADISE-Plattform durchzuführen. Diese beinhalten die Angaben zu Whereabouts-Light (Abb. 2, Erklärung hierzu in Unterkapitel 4.3), sollten diese eingesetzt werden. Hierbei ist davon auszugehen, dass dies z. B. monatlich einmal durchgeführt wird bzw. wenn sich spontan eine größere Änderung, wie z. B. eine Auslandreise, ergibt. Bei den Angaben zu persönlichen Geofences oder die Deaktivierung der allgemeinen ist davon auszugehen, dass diese einmal getätigt werden und sich dann über einen Zeitraum von Monaten nicht oder nur sehr gering ändern.

4.2 Nutzergruppe DCOs

Der Tagesablauf eines DCOs würde beim Einsatz von PARADISE dadurch geprägt sein, dass er eine voraussichtliche Planung mit z. B. Whereabouts-Light macht und damit sehen kann, ob sich die zu prüfenden AthletInnen in ihren Städten oder Landkreisen befinden. Für den Kontrollzeitraum besteht die Möglichkeit mit Abfrage der Position zu einer Entscheidungsfindung zu kommen, ob die AthletInnen an diesen Tagen kontrolliert werden können oder nicht. Hierbei können Informationen über die Entfernung, eine mögliche Zuordnung zu seiner Trainingsstätte, einem Bahnhof oder Flughafen unterstützend wirken, auch in Bezug auf Abwägung einer Kontaktaufnahme per Telefon. Die Erfahrung zeigt, dass viele DCOs ihre zu kontrollierenden LeistungssportlerInnen über die Zeit

auch persönlich kennen. Damit einhergehend sind den DCO auch oft die Sportstätte, der Arbeitsplatz und die Wohnadresse der AthletInnen bekannt. Sie können somit immer noch abschätzen, wie groß die Chancen für ein Zusammentreffen und damit für eine abgeschlossene Kontrolle sind. Insgesamt wird versucht das Risiko für einen erfolglosen Kontrollversuch (Nicht erfolgter Kontrollversuch, NEKV) auch aus wirtschaftlichen Aspekten zu minimieren. Mit ADAMS werden vermehrt Zeitfenster genutzt, in der AthletInnen mit einer hohen Wahrscheinlichkeit anzutreffen sind. Mit PARADISE erhöht sich die Qualität der Kontrollen, da es keine „schwarzen Flecken" der Whereabouts gibt, die LeistungssportlerInnen gezielt setzen können um eine Wahrscheinlichkeit der Kontrollen zu verringern. Gespräche mit DCOs haben gezeigt, dass es durch die Einführung der PARADISE-Ideen zu veränderten Abläufen im Tagesgeschäft kommen würde, eine abschließende Beurteilung steht jedoch noch aus. PARADISE hat auch als Ziel das Zusammentreffen zwischen DCO und AthletInnen nach einer Kontaktaufnahme zu verkürzen, da sich die DCOs in der Regel den AthletInnen bis auf kurze Distanz nähern können. Dies soll die Gefahr von Manipulationen verringern. Es ist hier nochmal festzuhalten, dass eine telefonische Kontaktaufnahmen generell die Ausnahme bleiben sollen. Die DCOs fänden es praktisch, wenn man Kalenderdaten zwei bis drei Tage vor und nach dem Kontrollzeitraum einsehen könnte. Manchmal passiert es, dass man einen Kontrollauftrag bekommt und die LeistungssportlerInnen in diesem Zeitraum für die DCOs unerreichbar sind. Wenn die AthletInnen aber zwei bis drei Tage vor oder nach dem angegebenen Kontrollzeitraum in Reichweite sind, wird der Kontrolltermin in Absprache mit der NADO evtl. angepasst.

4.3 Nutzergruppe NADO-KontrollplanerInnen

NADO-KontrollerplanerInnen können im ADAMS-System auf alle Einträge des gesamte Kalenders der AthletInnen zugreifen. Dies nutzen die PlannerInnen, um den beauftragten Kontrollunternehmen, u. a. PWC in Deutschland[10], detaillierte Auskünfte über die Aufenthaltsorte der zu kontrollierenden AthletInnen zu übertragen, die daraufhin ihre Kontrollplanung ausrichten und DCOs bestimmen, die sich in der Nähe befinden. In einigen Fällen werden auch DCOs in andere Regionen und Länder geschickt, in denen Wettkämpfe stattfinden oder sich Trainingslager befinden.

Die Angaben über die Aufenthaltsorte werden allerdings von den NADO-KontrollplanerInnen auch dazu genutzt, um Auffälligkeiten bei den Einträgen

10 Professional Worldwide Controls GmbH, http://www.pwc-gmbh.de

bzw. Änderungen der Whereabouts zu identifizieren, die dann mit in die Entscheidung über angesetzte Kontrollen einfließen. Ein Beispiel für eine Auffälligkeit ist die kurzfristig getätigte Änderung des Übernachtungsorts der Athletin oder des Athleten. Dies soll der evtl. missbräuchlichen Nutzung des ADAMS-Whereabouts-Systems zur Verschleierung von möglichen Dopingaktivitäten entgegenwirken und fließt deshalb mit in die Dopingkontroll-Entscheidungen ein (ähnlich zu Auffälligkeiten bei Blutwerten[11]).

Im PARADISE-Kontext wurde auch darüber nachgedacht, wie ein neues System den organisatorischen Anforderungen der NADO-KontrollplanerInnen genügen kann. Angedacht wurden eventuelle Angaben der AthletInnen hinsichtlich eines groben Aufenhaltsortes für die jeweilige Zeit, in der sie sich in einer Region oder Stadt befinden. Zum Beispiel könnten sie Angaben zu den Bundesländern, Gemeinden, Städten oder Postleitzahlgebieten machen, in denen sie sich über mehrere Tage aufhalten. Im Projekt wurden diese Whereabouts, wie bereits beschrieben, mit Whereabouts-Light bezeichnet. Dieser Ansatz widerspricht allerdings den Anforderungen, dass die AthletInnen mit einem neuen System möglichst wenig Interaktion haben sollten (Elmasllari 2017). Weitere Ideen, wie die Angabe von Ausnahmen, z. B. bei Reisen oder anderen merklichen Ortswechsel, wurden im Projekt besprochen.

Bei der Einführung eines neuen Systems ist allerdings zu prüfen, inwieweit sich die derzeitigen Arbeitsabläufe, die NADO-MitarbeiterInnen und KontrolleurInnen und ihre Arbeitgeber durchführen, nicht grundsätzlich ändern müssten. Dies könnte zu einer Einführung von neuen Vorgängen führen, die mit dem jetzigen System, nicht umsetzbar wären. So könnten unterbeauftragte Kontrollfirmen die Ortsabfrage der *eves-Devices* tätigen und die Ergebnisse an die entsprechenden MitarbeiterInnen weiterleiten. Damit müsste sich auch der Modus ändern, wie KontrolleurInnen entscheiden, ob sie sich zu einem Zielort bewegen oder nicht, der zur Zeit darauf ausgelegt ist, die Chance auf das Antreffen zu maximieren.

5. PARADISE IM LICHTE DES DATENSCHUTZES UND DER DSGVO

Am 25. Mai 2018 wurde die DSGVO wirksam. Die Verordnung löste die Datenschutzrichtlinie 95/46/EG aus dem Jahr 1995 ab und regelt den Datenschutz in

11 https://www.stern.de/gesundheit/marco-russ-krebs-diagnose-nach-dopingtest--was-bedeutet-ein-erhoehter-hcg-wert--6857558.html

den Mitgliedsstatten der EU. Sie sieht u. a. eine Harmonisierung in den Mitgliedstaaten vor, die zuvor historisch-bedingt sehr heterogen ausgeprägt war und gibt eine klarere Definition und damit ein besseres Verständnis des Begriffs personenbezogene Daten. In diesem Abschnitt wird kurz erläutert, wie sich exemplarisch einige der 99 DSGVO-Artikel zu den Systemen ADAMS und PARADISE verhalten (Herber 2017).

Die DSGVO hat den Anspruch EU-BürgerInnen vor Datenmissbrauch durch Firmen und Einrichtungen zu bewahren und wird auch für Angebote wirksam, deren Unternehmen und Dienst-Anbieter keinen EU-Sitz haben, aber für EU-BürgerInnen angeboten werden. Somit ist die DSGVO auch wirksam für Daten, die nicht in der EU gespeichert werden (Art. 3, Räumlicher Anwendungsbereich). In Bezug auf ADAMS heißt das, dass EU-AthletInnen unabhängig davon, wo ihre Daten verarbeitet werden, dem Schutz der DSGVO unterliegen. Konkret heißt dies, dass die Prinzipien *Datenschutz durch Technik* (*data protection by design*) und datenschutzfreundliche Voreinstellungen (*data protection by default*) durch entsprechende Maßnahmen des Dienstanbieters Genüge getan werden muss (Art. 25, Datenschutz durch Technikgestaltung und durch datenschutzfreundliche Voreinstellungen). Der Schutz der persönlichen Daten und deren Erarbeitung muss nach Artikel 32 (Sicherheit der Verarbeitung) unter Berücksichtigung des Stands der Technik umgesetzt werden. Auch ist es verpflichtend für den Datenverarbeitungsprozess eine Datenschutz-Folgenabschätzung zu erstellen (Art. 35).

Die durch PARADISE propagierte Datenminimierung findet sich in der DSGVO in Artikel 5 wieder, dort heißt es *„Personenbezogene Daten müssen [...] dem Zweck angemessen und erheblich sowie auf das für die Zwecke der Verarbeitung notwendige Maß beschränkt sein (Datenminimierung)“*. Dies wird in PARADISE durch die Nutzung der genauen Positionsdaten nur zum Zeitpunkt einer bevorstehenden Kontrolle erzielt, wie auch durch das Konzept der Whereabouts-Light für die Tätigkeit der Kontrollplanung durch die NADA.

Im Absatz 1(a) des Artikel 5 heißt es weiterhin „Personenbezogene Daten müssen [...] in einer für die betroffene Person nachvollziehbaren Weise verarbeitet werden“ (Transparenz). AthletInnen wird durch die PARADISE-Audit-Funktion die Möglichkeit gegeben nachzuvollziehen, welcher Nutzer wann auf seine (Positions-) Daten zugegriffen hat. Das ADAMS-System ist für AthletInnen in dieser Hinsicht undurchsichtig.

Das Konzept der granularen Ortsinformationen, die der DCO erhält, wenn ein Kontrollauftrag durchgeführt wird, basiert auf dem Prinzip der Datenminimierung in Artikel 5 (1)(c) „Personenbezogene Daten müssen dem Zweck

angemessen und erheblich sowie auf das für die Zwecke der Verarbeitung notwendige Maß beschränkt sein“ (Datenminimierung).

In Artikel 5 (1)(f) heißt es *„[..] Schutz vor unbefugter oder unrechtmäßiger Verarbeitung [...] durch geeignete technische und organisatorische Maßnahmen („Integrität und Vertraulichkeit“)*. Dies wird in PARADISE durch die Nutzung der Sealed Cloud Technologie[12], u. a. für die Abwehr von internen Administratoren der Systeme, sowie dem Einsatz von attributsbasierter Zugriffskontrolle und Delegation (Schanzenbach 2016, Rivest 1996) gewährleistet. In Ansätzen wurden dabei auch Konzepte und Techniken integriert, die bei aktuellen Blockchain- und Distributed-Ledger-Anwendungen zum Einsatz kommen und Datenmanipulationen durch Verkettung ausschließen.

Wiederkehrende Verstöße können mit bis zu 20 Million EUR oder im Fall eines Unternehmens von bis zu 4 % seines gesamten weltweit erzielten Jahresumsatzes des vorangegangenen Geschäftsjahrs geahndet werden (Art. 83, Allgemeine Bedingungen für die Verhängung von Geldbußen).

Die Erwägungsgründe

- 6. „[...] *Zunehmend machen auch natürliche Personen Informationen öffentlich weltweit zugänglich. [...]“, der Erläuterungen in Erwägungsgrund;*
- 4 *„[...] insbesondere Achtung des Privat- und Familienlebens, der Wohnung und der Kommunikation, Schutz personenbezogener Daten, Gedanken-, Gewissens- und Religionsfreiheit, Freiheit der Meinungsäußerung und Informationsfreiheit [...]“;*
- sowie 7 *„[...] Natürliche Personen sollten die Kontrolle über ihre eigenen Daten besitzen. [...]“*

haben PARADISE motiviert den AthletInnen aktiv ihrer informationellen Selbstbestimmtheit zu entsprechen und ihnen Werkzeuge, u. a. in Form von persönlichen Geofences (Zickau 2016), zur Verfügung zu stellen, um ihre Privatsphäre auch beim Einsatz eines ortsbestimmenden *Wearables* zu schützen.

Auf das Thema Datenübertragung bei der internationalen Bekämpfung von Doping im Sport wird direkt im Erwägungsgrund 112 eingegangen, der für den Artikel 49 (1)(d) (Ausnahmen für bestimmte Fälle) erklärt *„[...] die Übermittlung ist aus wichtigen Gründen des öffentlichen Interesses notwendig [...] zur Verringerung und/oder Beseitigung des Dopings im Sport“*. Dies bedeutet allerdings nicht, dass das Datenschutzrecht der DSGVO für Athletendaten ausgenommen wird.

12 „Sealed Cloud schließt IT-Sicherheitslücke ‚Mensch‘“, DuD 2013, S. 333.

6. AKTUELLE ENTWICKLUNGEN

Ende Februar 2018 lief die Projektförderung durch das BMBF aus. Die Weiterentwicklung der PARADISE-Plattform wurde somit eingestellt. In den letzten beiden Projektmonaten fanden vielversprechende Gespräche mit der WADA statt. Zum einen stand die Einführung der neuen, europäischen Datenschutzgrundverordnung kurz bevor, zum anderen bestanden Bestrebungen seitens der WADA eine von Grund auf neue Kontrollplattform zu entwickeln. In den Gesprächen wurde darauf hingewiesen, dass man nicht an eine Lösung unter Einbezug von Lokalisierungstechnologien glaube, aber dennoch großes Interesse am Backend von PARADISE habe. Dies scheint jedoch genau der Wunsch von AthletInnen weltweit zu sein. Neben eigenen Umfragen, in denen sich 60 Prozent für eine GPS-Lösung aussprachen ohne genaue Projektdetails zu kennen, bekam in den USA eine solche Lösung von rund 70 Prozent der AthletInnen Zuspruch.

Ein für März 2017 geplantes Treffen in Lausanne wurde von der WADA aus „terminlichen Gründen" kurzfristig abgesagt. Einige Tage später sprach sich das Ethics-Panel der WADA gegen jeglichen Einsatz von Ortungstechnologien zur Vorbereitung bzw. Initiierung von Dopingkontrollen aus. Grund dafür sei der unverhältnismäßige Eingriff in die Privatsphäre der AthletInnen. Ein Austausch mit dem Projektteam hat jedoch leider zu keinem Zeitpunkt bestanden. Da es sich hier lediglich um eine Empfehlung des Ethics-Panels handelt, ist es nun am Executive Board zu entscheiden, inwiefern diese Entscheidung in die neuen WADA-Regularien einfließen wird (Borry 2018).

Aufgrund der Wichtigkeit und Dringlichkeit der Thematik, im Besonderen im Zusammenhang mit der neuen Datenschutzgrundverordnung, befindet sich die FDP-Fraktion aktuell in der Vorbereitung einer *kleinen Anfrage* an die Bundesregierung. Hier wurden bereits rund zwei Dutzend Fragen gesammelt, mit denen sich auch das Projektkonsortium in den zurückliegenden Jahren beschäftigt hat, konfrontiert sah bzw. deren abschließende, präzise Beantwortung durch die verantwortlichen Institutionen bislang ausblieb.

7. FAZIT UND AUSBLICK

Als Fazit des Projekts lassen sich vier Aspekte hervorheben.

Durch die Entwicklung eines Alternativsystems durch das Projektkonsortium und die gute Medienresonanz, gerieten die verantwortlichen Institutionen unter Erklärungsnot. Es mussten Argumente gefunden werden, warum an ADAMS

festgehalten wird. Das letztendliche Hauptargument, dass es durch Ortungstechnologien zu Eingriffen in die Privatsphäre der AthletInnen kommt, ist jedoch nicht nachvollziehbar. Vor allem vor dem Hintergrund, dass das Gegenteil das eigentliche Ziel Vorhabens war, welches auch durch unsere Forschungsergebnisse und dem Lösungsansatz verdeutlicht wurde.

Bislang scheint es, als würden Wünsche und Anliegen einzelner Nationen bzw. NADOs von der WADA nicht ernst genommen bzw. NADOs bei der Umsetzung mit den Vorgaben der WADA alleine gelassen. Nicht selten kommt es hier zu Überschneidungen mit nationalen Gesetzgebungen. Es wäre wünschenswert, dass die DSGVO alle EU-NADOs vereint und neue Gespräche mit der WADA auf Augenhöhe ermöglicht.

Die aktuell in Vorbereitung befindliche kleine Anfrage an die Bundesregierung sollte von deutschen Sportjournalisten genutzt werden, das Thema Anti-Doping und Datenschutz in die Gesellschaft zu tragen. Leider beschränken sich die Berichterstattungen beim Anti-Doping oft auf positive Analyseergebnisse. Welche Bürde AthletInnen mit dem aktuellen Kontrollsystem tagtäglich zu tragen haben, ist nur wenigen bekannt. Es bleibt zu hoffen, dass ein Medienecho auch dazu führt, dass sich AthletInnen vermehrt öffentlich zur Thematik äußern und nicht mehr dem üblichen Motto „gehört halt zum Spitzensport“ hingeben.

Auch über die Anwendungsdomäne Anti-Doping hinaus, lässt sich die Infrastruktur von PARADISE in andere Client-Server-Architekturen übertragen. Gerade der Einsatz von Geofencing-Lösungen für ortsbezogene Anwendungen ist richtungsweisend in den (Forschungs-)Themen Datenschutz, *Ubiquitous Computing* und *Internet of Things* (IoT).

LITERATUR

Ahadipour, Ava, und Schanzenbach, Martin. (2017). A Survey on Authorization in Distributed Systems: Information Storage, Data Retrieval and Trust Evaluation. In *Trustcom/BigDataSE/ICESS, 2017 IEEE*, pp. 1016-1023. IEEE..

Borry, P., Caulfield, T., Estivill, X., Loland, S., McNamee, M., und Knoppers, B. M. (2018). Geolocalisation of athletes for out-of-competition drug testing: Ethical considerations. *Position statement by the WADA ethics panel. British Journal of Sports Medicine*, 52: 456–459.

Elmasllari, Erion, und Plass, Jonas. (2017). Domain and requirements for a wearable-based doping control system. *Datenschutz und Datensicherheit-DuD* 41, no. 12: 717-720.

Herber, Torben J., Jentsch, Marc und Zickau, Sebastian.(2017) Datenschutz und Dopingkontrollen. *Datenschutz und Datensicherheit-DuD* 41, no. 7: 427-433.

Herber, Torben J. (2017). Datenschutzrechtliche Grenzen des deutschen Dopingkontrollsystems. *Datenschutz und Datensicherheit-DuD* 41, no. 12: 735-739.

ISO, DIN En. 9241: Ergonomics of Human System Interaction. *Geneva: International Organization for Standardization* 18 (2006).

Jäger, Hubert A., Abdullah, Lamya und Quintero, Juan. (2017). Vertrauenswürdiges Backend. *Datenschutz und Datensicherheit-DuD* 41, no. 12: 729-734.

Putschli, Clemens. (2017). Wearables und Datenschutz. *Datenschutz und Datensicherheit, DuD* 41, no. 12: 721-723.

Rivest, Ronald L., und Lampson, Bulter. (1996). SDSI-a simple distributed security infrastructure. Crypto..

Schanzenbach, Martin, und Banse, Christian. (2016). Managing and presenting user attributes over a decentralized secure name system. In *Data Privacy Management and Security Assurance*, pp. 213-220. Springer, Cham..

Schanzenbach, Martin, und Zickau, Sebastian. (2017). Identity and access management in a doping control use case. *Datenschutz und Datensicherheit-DuD* 41, no. 12: 724-728.

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