

Der Verbraucher als Datenlieferant

Rechtliche Aspekte von „smarten“ Produkten

Barbara Kolany-Raiser

DOI 10.15501/978-3-86336-912-5_3

Abstract

Die Entwicklung der letzten Jahre zeigt, dass immer mehr Produkte „smart“ werden – das Fitnessarmband animiert uns zu mehr Bewegung, der Kühlschrank bestellt eigenständig Lebensmittel nach. Für diese vom Verbraucher generierten Daten interessieren sich beispielsweise Krankenkassen, die den Kauf von Fitnessarmbändern subventionieren und Bonusprogramme einrichten. Neben dem datenschutzrechtlichen Aspekt soll es auch um vertragliche und haftungsrechtliche Fragestellungen rund um die „smarten“ Geräte gehen.

Besonderer Dank für die Mitarbeit geht an die studentischen Hilfskräfte Clara Berisch, Sandra Dittmer und Lucas Werner.

Dieser Beitrag erscheint unter der Creative-Commons-Lizenz: Namensnennung – Weitergabe unter gleichen Bedingungen 3.0 Deutschland | CC BY-SA 3.0 DE
Kurzform | <http://creativecommons.org/licenses/by-sa/3.0/de/>
Lizenztext | <http://creativecommons.org/licenses/by-sa/3.0/de/legalcode>

1 Einleitung

Nach einer im April 2015 durchgeführten Umfrage des Meinungsforschungsinstitutes Forsa, die im Auftrag der Verbraucherzentrale Bundesverband erfolgte, sind 81 Prozent der befragten Verbraucherinnen und Verbraucher der Meinung, dass ihnen aus der Sammlung und Auswertung persönlicher Daten durch Unternehmen im Netz mehr Nachteile als Vorteile erwachsen (vzbv 2015). Viele Daten entstehen dadurch, dass der Kunde selbst sogenannte Smart Devices wie zum Beispiel Smartphones, Smartwatches oder Fitnessarmbänder verwendet, um damit Daten über seine Vitalwerte, seine Ernährung oder sein Schlafverhalten zu sammeln. Dies spiegelt den Trend der Selbstüberwachung zur Selbstoptimierung wider. Die zunehmende Vernetzung von Gegenständen sowohl im geschäftlichen als auch im privaten Bereich birgt aber gleichzeitig enorme Herausforderungen – insbesondere für das Recht.

2 Vertragliche Fragestellungen

Für die vertragliche Einordnung beim Kauf smarterer Produkte ist zunächst der Begriff des typengemischten Vertrags von Bedeutung. Darunter versteht man Verträge, bei denen Elemente unterschiedlicher Vertragstypen vorliegen.

Dem Käufer kommt es beim Kauf eines intelligenten Kühlschranks oder einer Smartwatch nicht allein darauf an, die klassischen Funktionen eines Kühlschranks oder einer Uhr zu nutzen, sondern auch die „intelligenten“ Zusatzdienste in Form der serverbasierten Dienste¹ in Anspruch nehmen zu können. Neben den kaufvertraglichen Elementen stellt sich die Frage, wie diese Dienstvertragsmerkmale einzuordnen sind.

1 Der Kühlschrank erinnert z. B. an das Verfallsdatum der Lebensmittel, macht Rezeptvorschläge und schickt Einkaufslisten an das Smartphone.

Wie Solmecke und Vondrlik feststellen, fehlt es im Normalfall an einer ausdrücklichen Regelung für diesen für das smarte Produkt notwendigen Serverdienst. Dies gilt sowohl für den Verkauf von smarten Produkten in Großmärkten als auch beim Onlinevertrieb. (Solmecke und Vondrlik 2013, 756) Unklar ist vor allem, inwiefern von einer stillschweigenden Willenserklärung hinsichtlich des Abschlusses eines Dienstvertrages ausgegangen werden kann.

Für das Vorliegen einer stillschweigenden Willenserklärung ist der Erklärungsgehalt eines objektiven Betrachters zum Zeitpunkt des Vertragsabschlusses maßgeblich. Sowohl im Großmarkt als auch im Falle des Onlineshops handelt es sich bei den ausgestellten und beworbenen Waren um kein verbindliches Angebot. Vielmehr soll der Kunde dazu aufgefordert werden, sein Kaufangebot abzugeben. Ein Kaufangebot wird vom Kunden durch das Auf-das-Kassenband-Legen der Ware oder durch das Abschicken einer Bestellung im Onlineshop abgegeben. Die Vertragsannahme erfolgt durch den Verkäufer (Busche 2016, Rn. 11, 12), entweder ausdrücklich oder stillschweigend durch Übersendung der Ware an den Käufer oder durch das Kassieren des Personals. Der objektive Erklärungsgehalt des vom Käufer abgegebenen Angebotes wird dabei wesentlich durch die sowohl in den Verkaufsräumen als auch im Onlineshop vorhandene Werbung beeinflusst. Der Käufer soll doch gerade zu den in der Werbung dargestellten Bedingungen dem Verkäufer ein Angebot unterbreiten. Wird der serverbasierte Dienst in der Werbung für das smarte Produkt mitbeworben, ist davon auszugehen, dass der Kunde neben dem Erwerb des Eigentums an diesem smarten Produkt auch die Verwendung dieser Zusatzdienste anstrebt und er daher mit seinem Antrag auch den Betrieb des Serverdienstes als Vertragsbestandteil ansieht. (Solmecke und Vondrlik 2013, 756)

Hier stellt sich die Frage, inwieweit der Verkäufer für die serverbasierte Leistung einzustehen hat. Dem Verkäufer ist das offensichtliche Interesse des Kunden an diesem Serverdienst bekannt. Denn auch wenn der Käufer eine Einmalzahlung für den Kaufpreis leistet, kann daraus für ihn nicht geschlossen werden, dass der Verkäufer sich nicht zur Erbringung des Serverdienstes verpflichten möchte (Solmecke und Vondrlik 2013, 755). Daher müsste der Verkäufer die Kundschaft darauf hinweisen, dass er rechtlich nicht für diesen Dienst eintreten will.

Beim Erwerb eines Fitnessarmbandes ist der Zusatzdienst in Form von Pulsmesser und Bewegungstracker der eigentliche Grund für den Kauf des Produktes, weshalb hier davon auszugehen ist, dass der Kaufvertrag in Kombination mit dem serverbasierten Zusatzdienst abgeschlossen werden soll. Dabei ist es unerheblich, ob der Verkäufer den Dienst selbst betreibt oder dieser durch einen Dritten betrieben wird.

Bei unserem Beispiel des smarten Kühlschranks bestehen verschiedene server- und internetbasierte Nutzungsmöglichkeiten. Manche Modelle erlauben nicht nur die Nutzung von Diensten des Herstellers, sondern auch offener Plattformen Dritter.² Internetdienste für die laufenden Bestellungen oder andere Funktionen können insofern auch durch vom Verkäufer unabhängige Anbieter erbracht werden. Zudem verbleibt dem Kühlschrank auch ohne zusätzliche serverbasierte Dienste die eigenständige und hauptsächliche Funktion, Lebensmittel zu kühlen und aufzubewahren. Daher ist in diesem Fall davon auszugehen, dass im Kaufrecht und nicht im Dienstvertragsrecht der Schwerpunkt des Vertrages liegt (Bräutigam und Klindt 2015, 1138).

Nachdem geklärt ist, dass der Verkäufer für die Erbringung des serverbasiereten Dienstes einstehen muss, stellt sich die Frage der Dauer dieser Leistungspflicht. Es ist anzunehmen, dass die Vertragsparteien bei Kenntnis der Rechtslage auch eine Regelung über die Vertragsdauer getroffen hätten.³ Da das smarte Produkt ohne den intelligenten Zusatzdienst einen wesentlichen Teil seiner Funktionen einbüßt und damit erheblich an Wert verliert, dürfte dem Verbraucher an einer möglichst langen Vertragsdauer gelegen sein. Auch für den Verkäufer ist eine möglichst lange Vertragsdauer erstrebenswert, wenn er eine Strategie der intensiven Kundenbindung verfolgt. Wichtig ist für den Kunden neben der langen Vertragsdauer jedoch auch die Festschreibung eines Kündigungsverzichtes durch den Verkäufer, da andernfalls eine jederzeitige

2 So beispielsweise Samsungs RF4289, auf dem neben hauseigenen Funktionen wie Samsungs „Grocery Manager App“ auch Dienste wie „Twitter“ oder „Evernote“ genutzt werden können.

3 Zur Auslegung des Vertrages siehe § 157 BGB.

Kündigung des Dienstvertrages durch den Verkäufer möglich wäre.⁴ Da es keine allgemeingültige Regelung für die Festlegung einer Mindestleistungsdauer gibt, empfiehlt sich die Orientierung an der Verjährungsfrist, die bei Sachmängeln zwei Jahre gemäß § 438 Abs. 1 Nr. 3 BGB beträgt (Solmecke und Vondrlik 2013, 757).

3 Haftungsrechtliche Fragestellungen

Durch die Einstellung des Serverdienstes wird der smarte Gegenstand entweder komplett funktionslos oder verliert einen Teil seiner Gebrauchsfähigkeit. Dies führt zu einer Wertminderung gegenüber einem Smartprodukt mit funktionsfähigem Serverdienst. Zu klären ist daher, inwieweit dem Käufer Ansprüche aus der vertraglichen oder deliktischen Haftung gegenüber dem Verkäufer erwachsen können.

3.1 Vertragliche Haftung

Durch Abschluss der vertraglichen Vereinbarung wird – wie gezeigt – zum einen die Pflicht, den serverbasierten Dienst zu betreiben, begründet. Zum anderen können aus dem Nichtbetrieb aber auch weitere Ansprüche, wie zum Beispiel Nacherfüllungs- oder Schadensersatzansprüche, erwachsen.

4 Vgl. §§ 620 Abs. 2 i.V.m. 621 Abs. 5 BGB. Solmecke und Vondrlik haben dabei eine Liste von Kriterien erstellt, die bei der Festlegung der Leistungsdauer berücksichtigt werden sollten. So spielt neben dem Äquivalenzinteresse des Käufers auch die Erwartung des Käufers in Bezug auf die Einstellung des Serverdienstes sowie der Produktzyklus oder auch die Preisgestaltung des Produktes oder dessen Funktionsfähigkeit ohne den Serverdienst eine Rolle.

3.1.1 Ansprüche aus Kaufvertrag/Kaufrechtliche Gewährleistung

Sofern ein Sachmangel vorliegt, d. h. die Ist- von der Sollbeschaffenheit abweicht, kommen Gewährleistungsansprüche in Betracht. Beim Fitnessarmband wäre die Sollbeschaffenheit das Funktionieren der smarten Trackingdienste. Wenn diese nicht mehr funktionieren, weicht die tatsächliche, also die Istbeschaffenheit, negativ von der Sollbeschaffenheit ab.

Zwar würden unsere Beispielsprodukte, d. h. der smarte Kühlschrank wie auch das Fitnessarmband, zweifellos durch Einstellung des Serverbetriebes eine wertbildende Eigenschaft verlieren, was grundsätzlich einem Sachmangel entspräche. Dieser Mangel entsteht regelmäßig jedoch erst mit der Einstellung des Serverbetriebes, d. h. erst nach Übergabe des jeweiligen Produktes und somit auch erst nach dem Gefahrübergang.⁵ Da im Zeitpunkt des Gefahrübergangs die vereinbarte Beschaffenheit gegeben ist, kann der Käufer keine Gewährleistungsansprüche geltend machen.

Eine Ausnahme gilt jedoch für Verbrauchsgüterkäufe, also Verträge, die zwischen einem Verbraucher und einem Unternehmer über den Kauf einer beweglichen Sache zustande kommen, vgl. § 474 Abs. 1. BGB. Absatz 1 dieser Norm erweitert den Anwendungsbereich des Verbrauchsgüterkaufs explizit auf Verträge, bei denen neben dem Kauf der beweglichen Sache auch die Erbringung einer Dienstleistung Teil des Vertrages wird. Für diese Verträge gilt mitunter die Vorschrift des § 476 BGB. Danach wird vermutet, dass die Sache bereits bei Gefahrübergang mangelhaft war, sofern sich der Mangel innerhalb von sechs Monaten nach Gefahrübergang zeigt. Der Europäische Gerichtshof hat in seinem Urteil vom 4. Juni 2015⁶ die Position des Verbrauchers zusätzlich

5 Hierunter versteht man den Zeitpunkt, in dem das Risiko einer Verschlechterung oder der Verlust einer Sache vom Schuldner auf den Gläubiger übergeht.

6 EuGH, Urteil vom 6. Juni 2015, Rs. C-497/13. <http://curia.europa.eu/juris/document/document.jsf?text=&docid=164727&pageIndex=0&doclang=DE&mode=req&dir=&occ=first&part=1> (Zugriff: 23. November 2015).

dahin gehend gestärkt, dass die Vermutung nicht nur in zeitlicher,⁷ sondern auch in sachlicher Hinsicht wirkt. Der Verbraucher braucht folglich innerhalb der ersten sechs Monate nach Gefahrübergang nur noch zu beweisen, dass überhaupt ein Mangel vorliegt. Dies ist insbesondere dann von Vorteil, wenn sich nicht nachweisen lässt, ob der Mangel auf unsachgemäße Bedienung zurückzuführen ist oder ob er schon vor Gefahrübergang vorlag und sich nur zu einem späteren Zeitpunkt gezeigt hat.

Jedenfalls im Bereich des Verbrauchsgüterkaufs kann das kaufrechtliche Gewährleistungsrecht somit für Ansprüche des Käufers eröffnet sein.

3.1.2 Ansprüche aus Dienstvertrag

Beim Dienstvertrag⁸ besteht die vertraglich geschuldete Leistung in der ordnungsgemäßen Erbringung der vereinbarten Dienstleistung – für unsere Beispiele wären dies die serverbasierten Dienste. Im Dienstvertragsrecht gibt es, anders als im Kaufrecht, kein eigenes Gewährleistungsrecht, sondern es gilt das allgemeine Leistungsstörungenrecht der §§ 280 ff. BGB.

Durch das Leistungsstörungenrecht wird der Empfänger einer nicht ordnungsgemäßen Leistung umfassend geschützt. Einerseits werden ihm Schäden ersetzt, die direkt daraus resultieren, dass er die Leistung eben nicht oder nicht ordnungsgemäß erhält, andererseits werden ihm Schäden ersetzt, die an seinem restlichen Vermögen dadurch entstehen, dass die Sache nicht ordnungsgemäß ist. Letzteres wäre zum Beispiel der Fall, wenn aufgrund eines Fehlers am smarten Kühlschrank weitere Küchengegenstände oder sich im Kühlschrank befindliche Lebensmittel beschädigt werden.

Wird der serverbasierte Dienst eines Fitnessarmbands eingestellt, ist die Leistung nicht mehr ordnungsgemäß. Der Verkäufer kann sich nach den obigen

7 So nämlich die ständige Rechtsprechung des BGH, erstmals in der „Zahnriemen“-Entscheidung vertreten. BGH, Urteil vom 2. Juni 2004, Az. VIII ZR 329/03 („Zahnriemen-Entscheidung“). <https://openjur.de/u/197445.html> (Zugriff: 23. November 2015).

8 Geregelt in den §§ 611 ff. BGB.

Ausführungen Schadenersatzansprüchen wegen Nicht- oder nicht vertragsgemäßer Leistung ausgesetzt sehen. (Solmecke und Vondrlik 2013, 758)

Wenn aufgrund technischer Probleme die Erbringung des Dienstes unmöglich wird, stellt sich die Frage, ob der Käufer Schadenersatzansprüche gegen den Vertragspartner geltend machen kann (Solmecke und Vondrlik 2013, 758). Erhält das Produkt aufgrund der Störungen keine Antwort mehr vom Server, kann dies dazu führen, dass die smarten Dienste ausfallen. Das Fitnessarmband würde in der Konsequenz aufhören zu tracken beziehungsweise die Ergebnisse nicht speichern können. Oder der Kühlschrank würde nicht mehr selbstständig den Bedarf ermitteln sowie Lebensmittel auf deren Haltbarkeit überprüfen.

Die Frage ist, was der Käufer in einem solchen Fall ersetzt bekommt. Grundsätzlich ist der Geschädigte bei Eintritt eines Schadens so zu stellen, wie er stünde, wenn das schädigende Ereignis ausgeblieben wäre (Oetker 2015, Rn. 18). Der Schaden beträgt somit den Wertverlust, den das Produkt durch die Einstellung des serverbasierten Dienstes erleidet. Konkret bedeutet dies, dass der Wert des Kühlschranks mit und ohne den serverbasierten Dienst verglichen werden muss (Solmecke und Vondrlik 2013, 758). Dies gilt unabhängig davon, ob die Nutzbarkeit des Gegenstands völlig oder nur teilweise aufgehoben wird.

3.2 Deliktische Haftung

Ungeachtet möglicher vertraglicher Ansprüche ist zu prüfen, ob auch Schadenersatzansprüche gemäß § 823 Abs. 1 BGB entstanden sein könnten. Schadenersatzpflichtig ist hiernach, wer bedeutende Rechte oder Rechtsgüter⁹ eines anderen widerrechtlich verletzt, wenn letzterem dadurch ein Schaden entsteht.

Da die meisten Anspruchsvoraussetzungen einzelfallbezogen sind, soll hier vor allem auf das Kriterium der Rechtsverletzung eingegangen werden.

9 Geschützt werden vor allem Eigentum, Besitz und weitere Rechte, nicht aber das Vermögen.

Als verletztes Recht kommt insbesondere das Eigentum in Betracht. Eine Eigentumsverletzung liegt immer dann vor, wenn in die Befugnisse des Eigentümers nach § 903 BGB eingegriffen wird. Mögliche Beeinträchtigungen sind die Verletzung der Sachsubstanz, der Entzug der Sache oder die Beeinträchtigung ihrer Nutzungs- und Gebrauchsfähigkeit (Staudinger 2014, Rn. 12). Bei letzterem ist die Abgrenzung zu einem Vermögensschaden, der nach § 823 BGB gerade nicht ersetzt wird, umstritten. Wird die Nutzung einer Sache beeinträchtigt, ohne dass überhaupt körperlich auf sie eingewirkt wird, kommt es nach der Rechtsprechung auf die Intensität der Nutzungsbeeinträchtigung an. Eine Eigentumsverletzung wird daher bejaht, soweit die Verwendungsfähigkeit einer Sache praktisch aufgehoben wird. Geht es dagegen nur um eine bestimmte Verwendungsmöglichkeit, die das Einsatzpotential der Sache nicht erschöpft, liegt keine Verletzung vor (Wagner 2014, Rn. 180).

In Bezug auf smarte Produkte würde dies bedeuten: Fällt ein serverbasierter Dienst aus, muss geprüft werden, ob die Gebrauchs- und Nutzungsfähigkeit beeinträchtigt ist. Für das Fitnessarmband lässt sich wohl nach allen Meinungen eine erhebliche Intensität der Beeinträchtigung und somit eine Eigentumsverletzung bejahen.

Bezüglich des Kühlschranks, der infolge des Dienstausfalls keine Haltbarkeitsdaten mehr anzeigt, muss eine differenziertere Betrachtung erfolgen. Festzuhalten ist nämlich, dass der Kühlschrank auch bei Ausfall des Zusatzdienstes seine Kernaufgabe – die Kühlung seiner Inhalte – weiterhin erfüllt. Der serverbasierte Dienst fällt der Rechtsprechung nach lediglich unter eine Verwendungsmodalität, die das verbleibende Einsatzpotential des Geräts unberührt lässt. Die Literatur kommt zu unterschiedlichen Ergebnissen. Ein hinreichender Intensitätsgrad an Beeinträchtigung kann wohl nicht angenommen werden. Jedoch ist es durchaus denkbar, dass der Marktwert der Sache dadurch herabgesetzt wird, was einigen für eine Eigentumsverletzung genügen würde.

4 Datenschutzrechtliche Fragen

Wie eingangs schon ausgeführt, werden durch smarte Produkte wie Fitnessarmbänder, Smartwatches oder andere Wearables Daten über die Herzfrequenz, den Blutdruck, die zurückgelegten Schritte und die Gesamtaktivität des Trägers sowie Standortdaten gesammelt. Häufig geht die Nutzung von Wearables mit der Installation von Gesundheitsapps auf Smartphones oder Tablets einher, die den Nutzer zu mehr sportlicher Betätigung animieren sollen. Die technischen Möglichkeiten, sich im Zuge einer Selbstoptimierung und Motivation selbst zu überwachen und zu kontrollieren, sind vielfältig. Diese Daten stehen dabei nicht bloß dem Träger oder Nutzer der Geräte zum persönlichen Feedback zur Verfügung, sondern ermöglichen es auch, den Herstellern umfangreiche Nutzerprofile zu erstellen. Zudem haben einige (gesetzliche) Krankenkassen die Beliebtheit von digitalen Fitnessangeboten erkannt und bieten neben Apps, digitalen Ärzteführern und Onlinekursen auch Zuschüsse für den Erwerb von Pulsmessern, Selftrackern u. a. digitalen Fitnessgeräten an. So gewährt zum Beispiel die AOK-Nordost ihren Versicherten jedes zweite Jahr einen Zuschuss von fünfzig Prozent der Kosten oder bis zu 50 Euro beim Erwerb eines dieser Produkte. Sie bietet ihren Versicherten zudem seit dem 1. Januar 2015 ein AOK-Gesundheitskonto, in dem verschiedenste Gesundheitsleistungen im Jahr mit bis zu 270 Euro bezuschusst werden können (AOK 2015). Bislang setzen die Krankenkassen jedoch nur auf Bezuschussungen – eine Weiterleitung persönlicher Daten an die Krankenkasse findet zurzeit (noch) nicht statt (Bohsem 2015). Im System der gesetzlichen Krankenkassen ist das Bonussystem nicht neu und vielen durch die Bonushefte bekannt. Die neuen Anreizsysteme werden dabei in bereits bestehende andere Bonusprogramme integriert. Die Versicherten sollen dabei zu einer gesünderen Lebensweise animiert werden.

Am 17. Juli 2015 ist das Gesetz zur Stärkung der Gesundheitsförderung und Prävention in Kraft getreten.¹⁰ Nach § 65a PräVg sollen die Krankenversicherungen in ihren Satzungen ausdrücklich festlegen, unter welchen Bedingungen ihre Versicherten Anspruch auf einen Bonus haben. Durch die Bezu-

¹⁰ Gesetz zur Stärkung der Gesundheitsförderung und Prävention (Präventionsgesetz – PräVg), BGBl 1368/2015 I Nr. 31.

schussung von Wearables, Fitnessapps und digitalen Sportkursen kommt es nämlich zu einer indirekten Subvention für Bewegungstrainings. Gerade weil die durch die Verwendung dieser Geräte entstehenden Daten bislang noch nicht an die Versicherungen übermittelt werden, stellt sich die Frage, ob sich Bonuszahlungen und niedrigere Prämien auf Dauer rechtfertigen lassen, wenn eine gesündere Lebensweise der verwendenden Versicherten nicht überprüft wird. (Dams 2014) Derzeit ist es den gesetzlichen Krankenkassen jedoch nur unter den in § 284 Abs. 1 SGB V abschließend aufgeführten Fällen erlaubt, personenbezogene Daten ihrer Versicherten zu erheben. Dabei ist die Erhebung der Daten auch an das strenge Kriterium der Erforderlichkeit gebunden. Es muss ein bestimmbarer Zweck vorliegen, damit die Daten gesammelt werden dürfen. Ist dies nicht gegeben, ist das Sammeln der Daten unzulässig, sodass die Verarbeitung der gewonnenen Daten unzulässig wäre. Da die bereichsspezifischen Vorschriften des SGB V den allgemeinen Vorschriften des Bundesdatenschutzgesetzes (BDSG) vorgehen, ist eine Einwilligung von Patienten nicht möglich. (Peters 2015, Rn. 6,10)

Bei privaten Versicherungen können die Versicherten der Erhebung ihrer personenbezogenen Daten durch das Versicherungsunternehmen vertraglich zustimmen. Bei der DKV können Versicherte sich den Kauf eines Fitnessarmbands oder auch einer Smartwatch mit einem Beitrag von fünfzig Euro fördern lassen. Dieses Angebot bezieht sich allerdings nur auf bestimmte Tarife. (Berres und Weber 2015) Einen Schritt weiter geht die Generali: Für 2016 plant der Konzern die Einführung seiner Vitality-Produkte in Deutschland, Österreich und Frankreich. Neben Innovationen in der Krankenversicherung sind auch Produkte für die Lebens- und Berufsunfähigkeitsversicherung geplant. Dabei soll der Versicherte zu Beginn das Gesundheits- und Fitnessniveau ermitteln und sich dann Ziele setzen, bei deren Erreichung Punkte vergeben werden. Um Gutscheine und Rabatte zu bekommen, werden Punkte für ärztliche Vorsorgetermine, aber auch für Fitness, Bewegung und den Einkauf von gesunden Lebensmitteln vergeben. (Generali 2015) Da Generali Kooperationen mit Sportartikelherstellern und anderen Firmen plant, sind auch Rabatte für Wearables denkbar (Berres und Weber 2015).

Die Anwendbarkeit des BDSG auf die durch das „self-tracking“ erhobenen Daten ergibt sich aus § 1 Abs. 2, BDSG, der die Anwendung des Gesetzes auf die Erhebung, Verarbeitung und Nutzung von personenbezogenen Daten festlegt.

Durch das Gerät werden die Daten über den Puls, die Herzfrequenz oder andere Bewegungsdaten sowohl erhoben als auch verarbeitet – und zwar in Form der Speicherung und Aufbereitung für den Nutzer. Unstrittig ist, dass es sich bei den durch die Wearables erhobenen Daten um personenbezogene Daten handelt, da nach § 3 Abs. 1 BDSG personenbezogene Daten Einzelangaben über persönliche oder sachliche Verhältnisse einer bestimmten oder bestimmbaren Person sind. Einzelangaben über persönliche Verhältnisse sind jene, die der Identifizierung der Person dienen, worunter auch Angaben zum Gesundheitszustand fallen (Franzen 2016, Rn. 2). Daten über den Gesundheitszustand einer Person sind dabei besonders sensible Angaben über eine Person und fallen daher unter § 3 Abs. 9 BDSG.

Normadressat ist die verantwortliche Stelle. Nach § 3 Abs. 7 BDSG ist das jede Person oder Stelle, die personenbezogene Daten für sich selbst erhebt, verarbeitet oder nutzt oder dies durch andere im Auftrag vornehmen lässt. Wird eine Fitnessapp von einer gesetzlichen Krankenkasse oder einer Versicherung angeboten, so ist diese als verantwortliche Stelle anzusehen. Auch wenn die personenbezogenen Daten nicht von der Krankenkasse oder Versicherung selbst verarbeitet werden, sondern durch eine andere Stelle im Auftrag der Krankenkasse oder Versicherung, trägt diese die Verantwortung für den Umgang mit den personenbezogenen Daten und die Einhaltung der gesetzlichen Vorgaben. (Dammann 2014, Rn. 224 ff.) Die damit einhergehenden Kontroll- und Sorgfaltspflichten ergeben sich aus § 11 BDSG: Wird für den technischen Betrieb der App ein Clouddienst eingesetzt, so muss die Krankenkasse oder Versicherung darauf achten, dass die Datenverarbeitung nicht in den USA stattfindet, da das Safe Harbor Abkommen¹¹ durch das Urteil des Europäischen Gerichtshofs¹² für ungültig erklärt wurde, weil es keinen adäquaten Daten-

11 Das Safe Harbor Abkommen war eine Vereinbarung zwischen der EU und den USA in Bezug auf die Übermittlung personenbezogener Daten in die USA. Das Abkommen basierte auf einer Entscheidung der Europäischen Kommission aus dem Jahr 2000. Grundsätzlich verbietet die Europäische Datenschutzrichtlinie eine Datenübermittlung an Staaten mit einem geringeren Datenschutzniveau, zu welchen die USA zählen. Durch das Safe Harbor Abkommen wurde ein Verfahren entwickelt, welches den Unterzeichnern des Abkommens dennoch einen Datentransfer ermöglichte. Für mehr Informationen vgl. BDFI unter <http://bit.ly/1j5DdjR>.

12 EuGH, Urteil vom 6. Oktober 2015, C-362/14. Maximilian Schrems v. [Irish] Data Protection Commissioner, Fn.106. <http://curia.europa.eu/juris/document/document.jsf?docid=169195&doclang=DE> (Zugriff: 23. November 2015).

schutz für die Datenübertragung zwischen Europa und den USA sicherstellt. Im Februar 2016 haben sich die EU-Kommission und die Vereinigten Staaten auf ein neues Abkommen zur transatlantischen Übermittlung von Daten für kommerzielle Zwecke geeinigt (sog. EU-US Privacy Shield). Das neue Abkommen soll die Grundrechte europäischer Bürger schützen, indem es strengere Datenschutzauflagen für US-Unternehmen vorsieht, den Zugriff der US-Behörden auf personenbezogene Daten begrenzt und Beschwerdemöglichkeiten für EU-Bürger bereithält. (Europäische Kommission 2016).

Die Tatsache, dass Versicherungen wie die Generali international operieren, steht der Anwendung des deutschen BDSG nicht entgegen. Der Anknüpfungspunkt ist die deutsche Niederlassung der Versicherung.¹³

Für die Anwendbarkeit des BDSG ist es unerheblich, ob die Daten vom Betroffenen selbst oder einem Dritten stammen oder für welchen Zweck sie erhoben wurden (Dammann 2014, Rn. 4). Beim Datenschutzrecht handelt es sich um ein sogenanntes Verbot mit Erlaubnisvorbehalt. Das bedeutet, dass die Erhebung, Verarbeitung oder Nutzung personenbezogener Daten grundsätzlich verboten ist, sofern nicht die Einwilligung des Betroffenen vorliegt oder eine Rechtsvorschrift dies erlaubt (Scheja und Haag 2013, Rn. 74).

Durch die Einwilligung wird der Umgang mit den personenbezogenen Daten legitimiert. Sie muss vor Beginn der Datenverarbeitung erteilt worden sein. Eine nachträgliche Genehmigung stellt keine Einwilligung dar, wodurch die Verarbeitung der personenbezogenen Daten unzulässig bleibt (Simitis 2014, Rn. 29). Außerdem muss sie freiwillig erteilt werden und sich auf den konkreten Umgang mit den Daten beziehen, weshalb der Betroffene über den Zweck der Erhebung, Verarbeitung oder Nutzung der Daten sowie den geplanten Umfang der Datenerhebung in Kenntnis gesetzt werden muss. Ist der konkrete Umfang noch unklar, besteht die Pflicht, den Betroffenen über alle

13 Vgl. § 1 Abs. 5 BDSG, die Anwendbarkeit des deutschen Datenschutzrechts knüpft primär an den Sitz der verantwortlichen Stelle. Hier gilt insoweit das Recht des Ortes, wo die Daten erhoben, verarbeitet oder genutzt werden. Sofern die tätige Stelle im Inland eine Niederlassung besitzt, greift allerdings wieder das Territorialitätsprinzip, sodass das deutsche Datenschutzrecht anwendbar ist. Dies gilt auch im Falle von rechtlich selbstständigen Tochtergesellschaften ausländischer Unternehmen (vgl. von Lewinski 2014, Rn. 52).

in Betracht kommenden Möglichkeiten und die daraus resultierenden Folgen zu informieren. Dementsprechend umfangreich können die für eine wirksame Einwilligung notwendigen Informationen ausfallen. Da es sich bei den durch Wearables erhobenen Daten nicht selten um besonders sensible Daten nach § 3 Abs. 9 BDSG handelt, muss sich die Einwilligung ausdrücklich auf diese Daten beziehen. Aufgrund des im Datenschutzrecht geltenden Grundsatzes der Zweckbindung müssen die Daten gelöscht werden, sobald der festgelegte Zweck für die Datenerhebung erreicht wurde.

Die Einwilligung des Betroffenen bedarf nach § 4 Abs. 1 S. 3 BDSG der Schriftform und muss von ihm eigenhändig unterzeichnet werden. Das Schriftformerfordernis dient dem Schutz des Betroffenen vor übereilter und unbedachter Äußerung. Nach § 126a BGB ist eine elektronische Einwilligung möglich, sofern sie eine elektronische Signatur aufweist.¹⁴

Soll die Erhebung und Verarbeitung der Daten im Rahmen eines geplanten Anreizsystems wie jenem der Generali erfolgen, so muss dem Schriftformerfordernis Genüge getan werden und sich die Einwilligung explizit auf die Erhebung und Verarbeitung der durch die Fitnessarmbänder oder Apps erhobenen Gesundheitsdaten beziehen.¹⁵

Das BDSG ist gem. § 1 Abs. 3 subsidiär gegenüber bereichsspezifischen Regelungen, wie den datenschutzrechtlichen Vorschriften des Telemediengesetzes (TMG). Dieses findet stets Anwendung, wenn es sich bei dem Dienst um ein Telemedium handelt. Nach § 1 Abs. 1 TMG sind dies elektronische Informa-

14 Nach der Rechtsprechung des BGH ist eine Einwilligung auch im Rahmen von Allgemeinen Geschäftsbedingungen möglich, sofern sie besonders hervor- gehoben ist. Dadurch ist dann eine gesonderte Unterschrift nicht notwendig (vgl. Payback-Urteil und Happy-Digits-Urteil). Dies gilt jedoch nicht für AGBs im elektronischen Geschäftsverkehr, mangels Schriftlichkeit. BGH, Urteil vom 16. Juli 2008, Az. VIII ZR 348/06 („Payback-Urteil“). <http://juris.bundesgerichtshof.de/cgi-bin/rechtsprechung/document.py?Gericht=bgh&Art=en&Datum=Aktuell&n-r=45162&linked=urt&Blank=1&file=dokument.pdf> (Zugriff: 23. November 2015). BGH, Urteil vom 11. November 2009, Az. VIII ZR 12/08 („Happy Digits-Urteil“). https://www.jurion.de/Urteile/BGH/2009-11-11/VIII-ZR-12_08 (Zugriff: 23. November 2015).

15 Die Erhebung und Verarbeitung von personenbezogenen Daten durch Versicherun- gen ist nicht von der Privilegierung der Forschung nach § 4a Abs. 2 BDSG erfasst.

tions- und Kommunikationsdienste mit Ausnahme von Telekommunikation und Rundfunk. Während Telekommunikation auf die reine Übertragung von Signalen abzielt, kommt es bei Telemedien dagegen auf eine Inhaltsleistung an. Für die Anwendung muss zumindest eine Inhaltsleistung angeboten werden, wie dies bei den Wearables der Fall ist und es muss ein sogenanntes Anbieter-Nutzer-Verhältnis nach § 11 TMG bestehen. Stehen Berufs- oder dienstliche Zwecke für die Datennutzung im Vordergrund, ist das TMG nicht anwendbar. Bei den hier zu untersuchenden Diensten besteht gerade ein klassisches Anbieter-Nutzer-Verhältnis zwischen dem Verbraucher, der zum Beispiel die Trackingdienste nutzt, und dem Betreiber oder Hersteller, der die Dienste anbietet.

Neben den wichtigsten datenschutzrechtlichen Grundsätzen aus dem BDSG kennt das TMG spezielle Erlaubnistatbestände, in denen der Datenumgang ausnahmsweise erlaubt ist. Dabei wird zwischen Bestandsdaten (§ 14 TMG) und Nutzungsdaten (§ 15 TMG) unterschieden.

Bestandsdaten sind personenbezogene Daten des Nutzers, die während der gesamten Durchführung des Vertrags über die Nutzung eines Telemediums erforderlich sind, also insbesondere Kontakt- und Bankdaten. Bei Trackingdaten handelt es sich um Daten, die nach Vertragsschluss erst durch die Inanspruchnahme der Dienste erhoben werden, sodass es sich gerade nicht um Bestandsdaten handelt. Geht es jedoch um die Kopplung des Trackers mit einem Bonusprogramm wie Generali dies plant, dann ist die Erhebung von Kontaktdaten erforderlich, um eine Zurechnung der Daten zum Nutzer des Wearables zu ermöglichen.

„Nutzungsdaten“ sind erforderlich, um die Inanspruchnahme der Dienste zu ermöglichen und abzurechnen. Dabei werden auch solche Daten erfasst, die während oder durch die Nutzung entstehen (Spindler und Nink 2015, Rn. 2). Nutzungsdaten sind etwa Angaben über die vom Nutzer in Anspruch genommenen Dienste oder die Dauer der Benutzung. Sie müssen von den Inhaltsdaten abgegrenzt werden, auf die in Ermangelung spezieller Regelungen des TMG das BDSG anzuwenden ist. Inhaltsdaten sind im Gegensatz zu Nutzungsdaten gerade nicht zur Inanspruchnahme des Dienstes notwendig. Vielmehr sind sie Daten, die durch einen Telemediendienst übermittelt werden, um die Leistungs- und Rechtsverhältnisse zu erfüllen (Spindler und Nink 2015, Rn. 3).

Es muss somit festgestellt werden, ob die von den Wearables erhobenen Daten als Nutzungs- oder als Inhaltsdaten zu qualifizieren sind, um sie dementsprechend dem Anwendungsbereich eines datenschutzrechtlichen Gesetzes zuzuordnen zu können. Dabei muss zwischen den Trackingdaten und solchen, die notwendig sind, um die Trackingdaten an ein Bonusprogramm zu koppeln, unterschieden werden. Die von den Wearables erhobenen Trackingdaten betreffen je nach Gerät Gesundheitsdaten wie Puls- und Blutdruck oder messen die sportliche Aktivität mithilfe von Geodaten. Die Erhebung dieser Daten hat den Zweck, die vertraglich vereinbarte Leistung, namentlich die Erbringung der Trackingdienste, zu erfüllen. Somit handelt es sich um Inhaltsdaten, sodass die datenschutzrechtlichen Sonderbestimmungen der §§ 11–15a TMG keine Anwendung finden und auf die allgemeinen Regelungen des BDSG zurückgegriffen werden muss.¹⁶ Bei der Erhebung von Gesundheitsdaten im Rahmen von Bonusprogrammen müssen zusätzlich solche Daten erhoben werden, mithilfe derer der Nutzer identifiziert und seinen Trackingdaten zugeordnet werden kann. In diesem Fall würden Bestands-, Inhalts- und Nutzungsdaten erhoben werden, auf die zum einen das TMG als auch das BDSG anwendbar sind. Die Einwilligung kann nach § 13 Abs. 2 TMG auch in elektronischer Form erfolgen, sofern sichergestellt ist, dass der Betroffene die Einwilligung bewusst und eindeutig erteilt hat, dies protokolliert wurde, der Inhalt der Einwilligung jederzeit abrufbar ist und dem Betroffenen die jederzeitige Möglichkeit zum Widerruf der Einwilligung offen steht.

Die Einwilligung nach § 13 Abs. 2 TMG bezieht sich aber nur auf die Bestands- und Nutzerdaten. Da für die Verwendung von Wearables im Rahmen von Bonuspunkteprogrammen von Versicherungen auch gerade die Inhaltsdaten relevant sind, da sich aus ihnen der Nachweis der sportlichen Betätigung ergibt, ist das Schriftformerfordernis des § 4a Abs. 1 S. 3 BDSG einzuhalten. Wurde nur eine elektronische Einwilligung eingeholt, so ist diese zwar für die Bestands- und Nutzungsdaten wirksam, in Bezug auf die Inhaltsdaten aber liegt

16 In Ausnahmefällen sind Inhaltsdaten doch unter § 15 TMG zu fassen, vgl. hierzu Spindler/Nink, Rn. 7.

eine unwirksame Einwilligung vor¹⁷, sofern sie nicht mit einer qualifizierten elektronischen Signatur nach dem Signaturgesetz versehen ist.¹⁸

Durch die Verwendung von Fitnessapps und Wearables will der Nutzer sich zu mehr Bewegung motivieren. Werden die von den Geräten erhobenen Daten im Rahmen von Bonusprogrammen oder zur Senkung von Versicherungstarifen an Versicherer übertragen, trägt der Nutzer zur Schaffung seines Gesundheitsscores bei. Hier besteht die Gefahr von zukünftigen Versicherungstarifen nach dem Modell „pay-as-you-live“, wie sie bereits bei Autoversicherungen existieren (sogenannte Pay-as-you-drive-Tarife) (Fromme 2015; Kfz-Versicherungen 2015). Nicht umsonst hat die Bundesdatenschutzbeauftragte vor unbedachtem Umgang mit den Gesundheitsdaten zur Erzielung kurzfristiger finanzieller Vorteile gewarnt und die Frage aufgeworfen, ob der Gesetzgeber den Schutz, der gesetzlich Versicherten gewährt wird, auch Versicherten von privaten Kassen gewähren sollte (Voßhoff 2015).

5 Fazit

Beim Verkauf von smarten Produkten muss mehr Transparenz für den Verbraucher geschaffen werden. Der Verbraucher muss Klarheit über die Person seines Vertragspartners und die Laufzeit des internetbasierten Zusatzdienstes haben. Nur so kann er vor einem plötzlichen Wertverlust oder der völligen Unbrauchbarkeit des smarten Produktes geschützt werden.

Der Verbraucher muss klar über die Risiken aufgeklärt werden, bevor er sich dazu entschließt, seine durch Fitnessapps oder Wearables gesammelten Gesundheitsdaten an Krankenversicherungen weiterzuleiten. Gerade weil Algorithmen Korrelationen finden und Prognosen bilden, die auf den ersten Blick

17 Vgl. Simitis§ 4a Rn. 33 ff. Wird die Schriftform der Einwilligung nach § 4a Abs. 1 S. 3 BDSG nicht eingehalten, ist die Einwilligung wegen des Formmangels nichtig nach § 125 BGB.

18 Vgl. § 126a BGB.

nicht sichtbar sind, ist die Frage, inwieweit der Verbraucher die Folgen der Nutzung seiner Daten durch seine Versicherung abschätzen kann.

Der Verbraucher kann bei Vorliegen einer unzulässigen Erhebung, Verarbeitung und Nutzung seiner personenbezogenen Daten einen Schadensersatzanspruch nach § 7 BDSG geltend machen. Problematisch ist zum einen, dass der Betroffene zuerst einmal davon Kenntnis erlangen muss, was sich aufgrund der häufigen Intransparenz der Datenerhebungs- und Datenverwendungsvorgänge als schwierig erweisen dürfte. Zum anderen muss er den Nachweis eines konkreten Schadens erbringen.

Verstöße gegen Datenschutzbestimmungen dürfen für die Unternehmen nicht mehr Gewinn bringen, als an Bußgeld bezahlt werden muss. Eine Erhöhung der Geldstrafe würde dazu führen, dass auch marktbeherrschende Unternehmen spürbar getroffen werden und sich die Sanktionswirkung entfalten kann.

Literatur

- AOK-Nordost. 2015. *Aok*. <https://www.aok.de/nordost/leistungen-service/aok-gesundheitskonto-248715.php> (Zugriff: 20. November 2015).
- Berres, Irene und Nina Weber. 2015. Zuschuss für Wearables: Die Kasse trainiert mit. *Spiegel Online* (7. August). <http://www.spiegel.de/gesundheit/ernaehrung/apple-watch-und-co-was-soll-die-krankenkasse-bezuschussen-a-1046835.html> (Zugriff: 20. November 2015).
- Bohsem, Guido. 2015. Zuschuss für die Apple-Watch. *Sueddeutsche.de*. (6. August). <http://www.sueddeutsche.de/wirtschaft/aok-bonus-fuer-apple-watch-1.2596338> (Zugriff: 20. November 2015).
- Bräutigam, Peter und Thomas Klindt. 2015. Industrie 4.0, das Internet der Dinge und das Recht. *Neue Juristische Wochenschrift* 68, Nr. 16, 1137–1141.
- Busche, Jan. 2016. § 145, Rn. 11, 12. In: *Münchener Kommentar zum BGB*, hg. von Hans Jürgen Sacker und Roland Rixecker. 7. Auflage. München: Beck.
- Dammann, Ulrich. 2014. § 3 BDSG, Rn. 4, 224 ff. In: *Bundesdatenschutzgesetz*, hg. von Spiros Simitis. 8. Auflage. Baden-Baden: Nomos.
- Europäische Kommission. 2016. EU Commission and United States agree on new framework for transatlantic data flows: EU-US Privacy Shield. Europe-

- an Commission Press Release Database (2. Februar). http://europa.eu/rapid/press-release_IP-16-216_en.htm (Zugriff: 8. April 2016).
- Franzen, Martin. 2016. § 3 BDSG, Rn. 2. In: *Erfurter Kommentar zum Arbeitsrecht*, hg. von Rudi Müller-Glöße, Ulrich Preis und Ingrid Schmidt. 16. Auflage. 2016. München: Beck.
- Fromme, Herbert. 2015. Billigere Autoversicherung dank Blackbox. *Sueddeutsche.de* (20. Mai). <http://www.sueddeutsche.de/auto/telematik-tarife-bei-kfz-versicherungen-viel-ueberwachung-fuer-ein-bisschen-ersparnis-1.2486679> (Zugriff: 23. November 2015).
- Generali, Deutschland. Vitality. 2015. <http://www.generali-deutschland.de/online/portal/gdinternet/de/content/311198/1150478> (Zugriff: 20. November 2015).
- KFZ-Versicherungen. 2015. Pay as you drive (PAYD). *Kfz-Versicherungen*. <http://www.kfz-versicherungen.com/ratgeber/pay-as-you-drive/> (Zugriff: 23. November 2015).
- Lewinski, Kai. 2014. § 1 BDSG Rn. 52. In: *Auernhammer BDSG – Kommentar zum Bundesdatenschutzgesetz*, hg. von Martin Eßer und Philipp Kramer. 4. Auflage. München: Beck.
- Oetker, Hartmut. 2015. § 249, Rn. 18. In: *Münchener Kommentar zum BGB*, hg. von Hans Jürgen Sacker und Roland Rixecker. 7. Auflage. München: Beck.
- Peters, Karl. 2015. § 284, Rn. 6,10. In: *Kasseler Kommentar zum Sozialversicherungsrecht*, hg. von Stephan Leitherer. 86. Ergänzungslieferung – Stand 06/2015. München: Beck.
- Pilkington, Katie. 2013. Samsung's RF4289HARS smart fridge has room to grow. *Cnet.com*. 23. September. <http://www.cnet.com/products/samsung-rf4289hars-refrigerator-series/> (Zugriff: 20. November 2015).
- Scheja, Gregor und Christian Haag. 2013. Teil 5 Datenschutzrecht, Rn. 74. In: *Münchener Anwaltshandbuch IT-Recht*, hg. von Andreas Leupold und Silke Glossner. 3. Auflage. München: Beck.
- Simitis, Spiros. 2014. § 4a BDSG, Rn. 29, 33 ff. 2014. In: *Bundesdatenschutzgesetz*, hg. von Spiros Simitis. 8. Auflage. Baden-Baden: Nomos.
- Solmecke, Christian und Simon-Elias Vondrlík. 2013. Rechtliche Probleme bei Produkten mit serverbasierten Zusatzdiensten – Was passiert, „wenn der Kühlschrank keine Einkaufsliste mehr schreibt...“. *MultiMedia und Recht* 16, Nr. 12, 755–760.

- Spindler, Gerald und Judith Nink. 2015. § 15 TMG, Rn. 2, 3. In: *Kommentar zum Recht der elektronischen Medien*, hg. von Gerald Spindler und Fabian Schuster. 3. Auflage. München: Beck.
- Staudinger, Ansgar. 2014. § 823, Rn. 12. In: *BGB Handkommentar*, hg. von Reiner Schulze, 8. Auflage. Baden-Baden: Nomos.
- vzbv (Verbraucherzentrale Bundesverband). 2015. Big Data: Verbraucher befürchten Nachteile durch Profilbildung. Pressemitteilung 4. Mai. *vzbv.de*. <http://www.vzbv.de/pressemitteilung/big-data-verbraucher-befuerchten-nachteile-durch-profilbildung> (Zugriff: 30. Oktober 2015).
- Wagner, Gerhard. 2014. § 823, Rn. 180, 184. In: *BGB Handkommentar*, hg. von Reiner Schulze et al. 8. Auflage. Baden-Baden: Nomos.