FAKULTÄT
FÜR !NFORMATIK
Faculty of Informatics

Probleme und Risiken bei Erfassung medizinisch relevanter Daten in mobilen Anwendungen

Diplomarbeit

zur Erlangung des akademischen Grades

Diplom-Ingenieur

im Rahmen des Studiums

Medizinische Informatik

eingereicht von

Patric Strasser, BSc
Matrikelnummer 0728052

an der
Fakultät für Informatik der Technischen Universität Wien

Betreuung: Ao. Univ.-Prof. Mag. Dr. iur. Markus Haslinger

Wien, 9. Juni 2015

(Unterschrift Verfasser/In) (Unterschrift Betreuung)

FAKULTÄT
FÜR !NFORMATIK
Faculty of Informatics

Problems and risks of collection of medically relevant data in mobile apps and devices

Master's Thesis

submitted in partial fulfillment of the requirements for the degree of

Master of Science

in

Medical Informatics

by

Patric Strasser, BSc
Registration Number 0728052

to the Faculty of Informatics
at the Vienna University of Technology

Advisor: Ao. Univ.-Prof. Mag. Dr. iur. Markus Haslinger

Vienna, June 9, 2015

(Signature of Author) (Signature of Advisor)

Eidesstattliche Erklärung

Patric Strasser, BSc
Finsterergasse 6/2/20, 1220 Wien

Hiermit erkläre ich, dass ich diese Arbeit selbständig verfasst habe, dass ich die verwendeten Quellen und Hilfsmittel vollständig angegeben habe und dass ich die Stellen der Arbeit – einschließlich Tabellen, Karten und Abbildungen –, die anderen Werken oder dem Internet im Wortlaut oder dem Sinn nach entnommen sind, auf jeden Fall unter Angabe der Quelle als Entlehnung kenntlich gemacht habe.

Bei allen Bezeichnungen, die auf Personen bezogen sind, werden beide Geschlechter angesprochen, unabhängig von der in der Formulierung verwendeten konkreten geschlechtsspezifischen Bezeichnung.

(Ort, Datum) (Unterschrift Verfasser/In)

Danksagung

Hiermit möchte ich mich zu allererst bei meinen Eltern, Alexander und Silvia, für ihre jahrelange Unterstützung auf meinem gesamten Ausbildungsweg bedanken.

Ein besonderer Dank geht an meine Freundin und Partnerin Lea Singer, die mich speziell in den letzten Jahren und im Besonderen während der Erstellung dieser Arbeit tatkräftig in allen Situationen unterstützt hat.

Zusätzlich danke ich Mag. Eva Singer-Meczes und MMag. Dr. Walter Perné, LL.M. für das Korrekturlesen.

Ein großer Dank ergeht an meinen Studienkollegen und guten Freund Dipl.-Ing. Markus Putzenlechner für die jahrelange Freundschaft und die großartigen gemeinsamen Studienjahre, welche auch durch ihn wesentlich an Beschwerlichkeit verloren haben.

Ich bedanke mich darüber hinaus sehr herzlich bei meinem Betreuer Ao. Univ.-Prof. Mag. Dr. Markus Haslinger für die verständnisvolle Begleitung und im höchsten Maß professionelle Betreuung meiner Diplomarbeit.

Kurzfassung

Das Aufkommen des Internets und die vollständige Durchdringung aller Bereiche durch Netzwerktechnologie und -kommunikation ist bis heute eine schwer zu erfassende Tatsache. Einen guten Teil für den unglaublichen Erfolg liefern die mobilen Geräte, wobei dieser durch den Siegeszug der Smartphones zusätzlich beschleunigt wird. Das „Tandem“ aus Internet und Smartphone ist aus dem täglichen Leben kaum noch wegzudenken. Beinahe jede Information ist ortsunabhängig, zu jeder Tageszeit, für jede Person verfügbar. Durch diese Entwicklung entstanden auch neue Geschäftsmodelle. Das Sammeln von personenbezogenen Daten wurde über die Jahre zur Prämisse für alle modernen Unternehmen. Dadurch lassen sich noch genauere Personenprofile erstellen, um noch exaktere Werbung zu generieren. Dies ist ein großes Verkaufsargument, da zielgerichtete Werbung weniger Streuverlust bietet und somit effizienter ist. Doch auch abseits der Werbeindustrie sammeln die neuen Anbieter fleißig Daten; teilweise, um ihre eigenen Dienstleistungen anzubieten. Angefangen von immer verfügbaren Datenspeichern im virtuellen Raum, der sogenannten Cloud, bis hin zu Fitness und Healthcare Applikationen für unterwegs ist alles verfügbar. Dies bietet allerdings speziell im Bereich des Datenschutzes erhebliche Risiken, da weder der Gesetzgeber noch der Bürger auf solche Situationen in jeglicher Form vorbereitet war und noch immer nicht ausreichend ist. Aus diesem Grund ergeben sich selbst bei der Erhebung von sehr sensiblen Gesundheitsdaten Unwissen und Unschlüssigkeiten auf beiden Seiten. Nachteilig für die Privatperson wirkt sich zusätzlich die Tatsache aus, dass Unternehmen oft wesentlich schneller auf neue Situationen und Möglichkeiten reagieren als der Gesetzgeber. Obendrein ist die derzeitige inhomogene Rechtslage im Bereich des Datenschutzes innerhalb der Europäischen Union äußest nachteilig für rechtliche Klarheit. Datenexporte in unsichere Drittländer, zu welchen auch die Vereinigten Staaten von Amerika gezählt werden müssen, sind darüber hinaus ein sehr heikles und komplexes Thema und bieten daher zusätzlichen Zündstoff. Daher ist es Ziel dieser Diplomarbeit, die aktuelle Rechtslage zu analysieren und danach auf dieser Grundlage eine Testanordnung zu schaffen, welche exemplarisch mobile Fitness-Anwendungen auf Datenschutzrisiken untersucht. Die Ergebnisse können dann sowohl eine Hilfestellung für die Verbraucher als auch ein Leitfaden für Unternehmen darstellen.

Schlüsselwörter

Datenschutz, Personenbezogene Daten, Sensible Daten, Internet, BigData, Smartphone, Tablet, App, Wearable Devices, Smartwatch, Health App, Medical App, Fitness App

Abstract

The advent of the Internet and the comprehensive penetration of this medium into all areas of human endeavour is a profound reality whose dimensions and implications are as yet not fully achieved - nor readily comprehensible. It can be described as a revolutionary evolution – a geometric progression in hardware technology coupled with quantum leaps in human behavior and comprehension. A large measure of the incredible success of this phenomenon has generally been based on mobile devices - which success has been further accelerated by the spectacular impact of smart phones. The synergistic capability that the internet and the smart phone provide is so fundamental to daily life - as to be virtually inconceivable without it. This is true for every level of endeavour; from teenager and parent, to student and professors and from business managers to doctors and scientists. In this regard, virtually every person in every profession has come to expect the instant availability of information independent of location or qualification at any time of the day or night – usually at no cost – and with very little effort. Naturally, this development has spawned a wide and deep range of new business models and opportunities – many of which are still emerging – including the automatic collection, sorting and analysis of personal and business data. Consequently, it is now possible to create detailed personal profiles in retail sales for customer, client, patient and potential buyer profiles that enable more precise and specifically targeted advertising which results in less waste, lower costs, better productivity and much higher efficiency. Beyond the obvious benefits to the sale of durable and non-durable goods the benefits to the advertising industry in the full range of services are quite remarkable; ranging from data stores permanently available in virtual space (the so-called "cloud") – to fitness, healthcare, academic, research and travel applications - everything is readily available. In conjunction with the obvious benefits, these developments also continue to engender substantial risks in the field of data protection, law enforcement, health care, business liability and personal privacy - which neither the legislature nor the citizenry were prepared for across the full spectrum of possibilities. For this reason, the collection of very sensitive personal medical data is marked by ignorance and apprehension on both sides of the equation. An additional disadvantage is that business enterprises respond more quickly and with more flexibility than government bureaucracies or the legislature. Furthermore, the complex and variegated approach to data protection within the European Union is extremely detrimental to legal clarity and uniformity in best business practices. The export and import of data – to and from basically unsafe nations such as the United States of America and many dozens of others – is a very sensitive and complicated issue which offers more fuel for potential conflict and legal liability. Therefore, it is imperative to analyze the existing legal situation, compare the available options, develop a test

model and then compare and examine exemplary fitness applications to assess and quantify the inherent data protection risks. The results can serve as a guide for both business endeavours and consumers.

Keywords

Data Privacy, Personal Data, Sensitive Data, Internet, BigData, Smartphone, Tablet, App, Wearable Devices, Smartwatch, Health App, Medical App, Fitness App

Inhaltsverzeichnis

KAPITEL 1

Einleitung

Dieses Kapitel dient als Übersicht zur grundlegenden Frage- und Problemstellung dieser Arbeit sowie zur dahinter liegenden Motivation. Darüber hinaus wird die vorweg definierte Zielsetzung deklariert und der Aufbau der Arbeit grob skizziert.

1.1 Problemstellung

Der Schutz der eigenen Daten und Privatsphäre ist so populär wie nie zuvor. Dies resultiert nicht zuletzt aus der rasend schnellen Entwicklung und Verbreitung von Internetzugängen und mobilen Endgeräten. Zum Beispiel hatten in Österreich bereits im Jahr 2010 circa 99% der Bevölkerung die Möglichkeit, das Internet auch zu Hause zu nutzen. [1] Vor allem Smartphones sind speziell in Europa sehr verbreitet und ermöglichen somit fast jedem Bürger den einfachen und schnellen Zugriff auf das Internet. Dass gerade mobile Geräte eindeutig die Zukunft der nächsten EDV-Generation sind, war schon 2008 mehr als ersichtlich. [2] Dies wurde 2010 durch die Erkenntnis, dass damals bereits 5% allen HTTP-Verkehrs durch Geräte wie Smartphones entstanden ist, bestätigt. [3] Doch birgt gerade der vermehrte Einsatz von hoch personalisierten mobilen Geräten in Bezug auf den Datenschutz erhebliche Risiken.

Speziell für den Umgang mit sogenannten sensiblen Daten gibt es in Österreich sehr genaue Vorschriften. [4] Ebenfalls ist exakt geregelt, welche Informationen der (kommerzielle) Datenerheber dem Nutzer über sich selbst zur Verfügung stellen muss. [5] Des Weiteren hat die EU-Kommission in der Datenschutzrichtlinie (DSRL) 95/46/EG [6] unter anderem reguliert, welche

[1] Auer: Erschließung des ländlichen Raums durch Breitband-Internet [7] (S. 29)
[2] Dietl: Mobile Computing - Innovationen und Trends für Hardware und Software [27]
[3] Erman et al.: HTTP in the home: it is not just about PCs [32]
[4] Datenschutzgesetz [25]
[5] E-Commerce-Gesetz [29]
[6] Datenschutzrichtlinie 95/46/EG [104]

Daten unter welchen Sicherheitsvorkehrungen wie lange gespeichert werden dürfen. Zusätzlich ist die Übertragung von Daten in Drittstaaten reglementiert. [7] Darüber hinaus steht das Europäische Datenschutzrecht direkt vor einem Wandel, da an einer vollständigen Reformierung in Form der Datenschutz-Grundverordnung [8] gearbeitet wird.

Somit ist zu klären, welche Daten unter welche Kategorie der Schutzwürdigkeit fallen und ob diese gesetzlichen Regelungen in praxi auch wirklich eingehalten wurden. Dies ist speziell bei den mittlerweile weit verbreiteten Smartphone Apps im Bereich Fitness und Healthcare ein sehr komplexes Thema. Hier gilt es, genau zu klären, ob die jeweilige Applikation schutzwürdige Daten weiterleitet und an externe Server überträgt. Zusätzlich ist zu hinterfragen, ob diese Daten entsprechend sicher gespeichert werden und ob der Speicherort außerhalb der Europäischen Union liegt.

Wie die Vergangenheit zeigt, gibt es leider bereits ausreichend Beispiele, in denen sich speziell Smartphone-Apps als sehr „gesprächig“ erweisen; sehr oft auch ohne die Zustimmung des Nutzers, wie unter anderem WhatsApp [9] und Facebook [10] sehr gut demonstriert hatten. In diesen beiden Fällen wurden ungefragt oder zumindest mit absolut unzureichender Information für den Benutzer Daten aus den Adressbüchern an die jeweiligen Firmenserver übertragen. In diesen Fällen kommt noch hinzu, dass Daten übertragen wurden, die eigentlich nicht dem Benutzer per se „gehören“, da es sich um persönliche Informationen Dritter handelt. Dies sind aber lediglich Beispiele für personenbezogene und noch nicht sensible, sprich unter anderem gesundheits- und krankheitsrelevante, Daten. In diesem Bereich muss aufgrund strengerer Auflagen noch genauer geprüft werden. Als ein Beispiel für solche sensible Datenübermittlung kann Facebooks Open Graph genannt werden, welcher unter anderem die Übertragung und Veröffentlichung von Fitness Daten (z.B. von Lauf-Apps) ohne zusätzliche Benutzereingabe ermöglicht, wie Facebook selbst [11] angibt.

1.2 Motivation

Durch die immer stärkere Verbreitung und Nutzung mobiler Geräte wie Smartphones rückt auch das Wirtschaftsmodell des gezielten Datensammelns in den Fokus vieler moderner Unternehmen. Je mehr Daten über eine Person bekannt sind, umso gezielter kann Werbung ausgeliefert werden. Diese Idee ist nicht neu; allerdings erreicht sie mit Smartphones und deren Möglichkeit, immer und überall mit dem Internet verbunden zu sein, neue Dimensionen. Plötzlich ist es für Unternehmen möglich, ohne großen Aufwand sehr stark personalisierte Profile, ange-

[7] Datenschutzrichtlinie 95/46/EG [104]
[8] Datenschutz-Grundverordnung [126]
[9] Whittaker: WhatsApp privacy practices under scrutiny [133]
[10] Gilbert: iPhone App Privacy: Path, Facebook, Twitter And Apple Under Scrutiny For Address Book Controversy [41]
[11] Yao: Early Success Stories: Fitness and Open Graph [137]

fangen von persönlichen Vorlieben und Eigenschaften bis hin zur exakten Standorterfassung, anzufertigen. Eine noch relativ neuartige Entwicklung sind sogenannte „Wearable Devices“ wie Fitness-Armbänder. Diese werden durchgehend getragen und erfassen mittels eingebauter Sensoren jeden Schritt und jede Bewegung des Trägers. Manche verfügen sogar über eingebaute Pulsmesssensoren. Somit können zum Beispiel bei sportlichen Aktivitäten komplette Fitness-Profile sehr leicht aufgezeichnet und ausgewertet werden. In Kombination mit einem Smartphone und diversen Apps lassen sich diese Daten komfortabel betrachten und nachverfolgen. Dies klingt für jeden Sportbegeisterten in erster Linie sehr verlockend. Leider wird viel zu oft das erhebliche datenschutzrechtliche Risiko vergessen, welches sich hinter derartiger Datenverarbeitung verbirgt. Daher ist es wichtig, genau diese Risiken zu analysieren, aufzuzeigen und bei der Bevölkerung ein höheres Bewusstsein für Datenschutz zu erwirken.

1.3 Zielsetzung

Im ersten Schritt der Arbeit sollen die gesetzlichen Grundlagen Österreichs, der Europäischen Union und der Vereinigten Staaten von Amerika im Bereich des Datenschutzes analysiert und dargelegt werden. Anschließend sollen der aktuelle Stand der Technik eruiert und die potenziellen Risiken aufgezeigt werden. Anhand dieser Erkenntnisse kann exemplarisch eine Auswahl an Apps im Bereich Fitness und Healthcare einem vorher festgelegten Test unterzogen werden, welcher im Abschluss als Grundlage für eine Einschätzung der derzeitigen Lage dienen soll.

1.4 Aufbau der Arbeit

In Kapitel 2 wird die Rechtslage erörtert: Im konkreten Fall wird es sich um die Rechtssituation in Österreich, der Europäischen Union sowie den Vereinigten Staaten von Amerika handeln. Es sollen die Rechte und Pflichten der Parteien dargelegt werden und nachgeprüft werden, inwiefern die festgestellten Unterschiede sich gegenseitig beeinflussen beziehungsweise miteinander interagieren. Darüber hinaus soll in diesem Kapitel ein direkter Vergleich der Rechtsvorschriften erfolgen, in welchem die Vor- sowie Nachteile gegenübergestellt werden. Danach wird in Kapitel 3 der aktuelle Stand der Technik im Bereich der mobilen Endgeräte sowie Applikationen erläutert. Dies umfasst Smartphones, diverse Wearable Devices sowie mobile Anwendungen, die sogenannten Apps. Im Anschluss wird in Kapitel 4 eine Testanordnung festgelegt, welche dann auf ausgewählte Fitness-Apps angewendet werden soll. Anhand dieser festgelegten Testkriterien und Fragestellungen ergibt sich eine untereinander vergleichbare Ergebnismenge, welche in Kapitel 5 in einer Gegenüberstellung verarbeitet wird. Daraus lassen sich letzten Endes die finalen Erkenntnisse in Kapitel 6 ableiten.

KAPITEL 2
Grundlagen

In diesem Kapitel werden die allgemeinen rechtlichen Grundlagen im Bereich des Datenschutzes in Österreich, der Europäischen Union (EU) und den Vereinigten Staaten von Amerika (USA) zusammengefasst. Danach werden positive wie negative Aspekte der einzelnen Bestimmungen erläutert. Als Abschluss werden nach Möglichkeit die länderspezifischen Eigenheiten im Bereich des gesetzlichen Datenschutzes miteinander verglichen.

> „Die Anerkennung von Privatheit und Datenschutz als Grundrechte bedeutet, dass ihre praktische Umsetzung ganz oben auf der politischen Tagesordnung der EU stehen muss.“ [1]

2.1 Österreichische Rechtsvorschriften

Als primäre Grundlage für dieses Kapitel gilt das Datenschutzgesetz (DSG) 2000 in der Fassung vom 04.11.2014 [2] sowie das E-Commerce-Gesetz (ECG), ebenfalls in der Fassung vom 04.11.2014 [3].

> „Bei dem Grundrecht auf Datenschutz nach § 1 DSG 2000 handelt es sich um eine Verfassungsbestimmung im Sinne des österreichischen Rechtssystems.“ [4]

> „Zweck dieses Gesetzes ist es, den einzelnen davor zu schützen, dass er durch den Umgang mit seinen personenbezogenen Daten in seinem Persönlichkeitsrecht beeinträchtigt wird.“ [5]

[1] o.A.: Tätigkeitsvorausschau des EDSB für 2014: Datenschutz im Herzen der EU-Politik [92]
[2] Datenschutzgesetz [25]
[3] E-Commerce-Gesetz [29]
[4] Kellner: Europol - Das Spannungsverhältnis zwischen Sicherheit und Grundrechten [76] (S. 79)
[5] Moos: Datenschutzrecht; schnell erfasst [85] (S. 2)

Grundlegend hat, laut Datenschutzgesetz, jeder Bürger Anspruch auf Geheimhaltung seiner personenbezogenen Daten. Dies findet sich im Artikel 1, § 1, Absatz 1. Allerdings räumt der Gesetzgeber in Absatz 2 das Recht ein, bei Eingriffen einer staatlichen Behörde auch ohne lebenswichtiges Interesse und Zustimmung des Betroffenen die personenbezogenen Daten verwenden zu dürfen. Des Weiteren bestimmt der Absatz 3, dass der Betroffene ein Recht auf Richtigstellung, Löschung sowie Auskunft über die Daten hat, wobei im Speziellen die Auskunft exakt definiert ist: nämlich in den Rechten auf Auskunft, welche Daten erhoben wurden, wer diese Daten erhoben hat, wofür diese Daten verwendet und an wen sie übermittelt werden. [6] Selbst in Bezug auf Datenspeicherung bei Organisationen wie Europol hat der Betroffene das grundsätzliche Recht auf Richtigstellung sowie Löschung, wie Kellner beschreibt. [7] Dies bedeutet zum Beispiel, dass jeder Bürger die Möglichkeit hat, bei jedem Datenverarbeiter, sei es eine Supermarktkette oder ein Webportal, die ihn betreffenden, gespeicherten Daten zu erfragen und gegebenenfalls richtigstellen zu lassen. [8]

> „Das DSG schützt personenbezogene Daten von „jedermann“. Schutzobjekt ist der sog. Betroffene [...] oder aber auch eine Personengemeinschaft [...].“ [9]

Selbsterklärend ist das österreichische Datenschutzrecht auf Datenverwendung im Inland anzuwenden. Nicht ganz selbsterklärend hingegen ist die Gültigkeit des DSG für die Verwendung von Daten im Ausland, sofern es sich um einen Staat der Europäischen Union handelt und das Unternehmen einen Sitz in Österreich aufrecht erhält. [10] Das reine Durchführen von personenbezogenen Daten durch Österreich ist vom DSG hingegen nicht erfasst. [11] Dies bedeutet, dass ein reines Durchleiten von Daten in jeglicher Form, sei es digital oder analog, nicht dem österreichischen Datenschutzgesetz unterliegt und somit auch nicht von diversen besonderen Rechten und Pflichten beider Parteien betroffen ist.

> „Grundsätzlich ist das DSG auf jede Datenverwendung in Österreich anzuwenden. Eine Durchbrechung des Territorialitätsprinzips besteht aber zu Gunsten des Sitzstaatsprinzips innerhalb der EU.“ [12]

Das österreichische Datenschutzrecht kennt, in Artikel 2, § 4, Ziffer 1 und 2, zwei Arten von schutzwürdigen Daten: [13] einerseits die „einfachen“ personenbezogenen Daten, welche noch die Untergruppe der indirekt personenbezogenen Daten beinhalten. Direkt personenbezogene Daten sind Daten, welche den Rückschluss auf die Identität des Betroffenen ohne weitere Mittel

[6] Datenschutzgesetz [25] (S. 3)
[7] Kellner: Europol - Das Spannungsverhältnis zwischen Sicherheit und Grundrechten [76] (S. 98)
[8] Pollirer et al.: Datenschutzgesetz 2000 [95] (S. 124ff)
[9] Fercher et al.: Aktuelle Fragen des Datenschutzrechts [74] (S. 23)
[10] Datenschutzgesetz [25] (S. 4)
[11] Fercher et al.: Aktuelle Fragen des Datenschutzrechts [74] (S. 24)
[12] Staudegger et al.: Informatikrecht [73] (S. 163)
[13] Help.gv.at - Datenschutz [114]

zulassen. Indirekt personenbezogene Daten hingegen sind Daten, welche den Rückschluss auf die Identität mit rechtlich zulässigen Mitteln nicht zulassen. [14]
Andererseits die sensiblen Daten: Diese beziehen sich auf Informationen wie ethnische Herkunft, politische Meinung, religiöse Überzeugung, Gesundheit oder Sexualleben. Außer Frage steht, dass diese Kategorie der höchsten Schutzwürdigkeit unterliegen muss. [15]
Besonders hervorzuheben ist der Unterschied zwischen indirekt personenbezogenen und nicht personenbezogenen Daten. Oftmals werden die nicht personenbezogenen Daten auch als anonymisierte Daten bezeichnet. Bei dieser Gruppe handelt es sich um vollständig vom Betroffenen entkoppelte und nicht rückführbare Informationen. Der Unterschied liegt darin, dass sie, im Gegensatz zu indirekt personenbezogenen Daten, auch nicht mit rechtlich unzulässigen Mitteln Rückschlüsse zulassen. Derartige Daten werden oft zu rein statistischen Zwecken erhoben (zum Beispiel eine Umfrage, wie viele Frauen im Alter von 18 und 25 Jahren in Wien Raucherinnen sind). [16]

> „Sensible Daten sind Daten, die den höchstpersönlichen Lebensbereich jedes Menschen betreffen; sie werden durch das Datenschutzgesetz besonders geschützt.“ [17]

Des Weiteren definiert Artikel 2, § 4, Ziffer 8 und 9, dass zum einen jegliche Nutzung von Daten als Verwenden von Daten deklariert ist und zum anderen, dass jegliche datenbezogene Tätigkeit mit Ausnahme des Übermittelns zur Verarbeitung von Daten zählt. Zusätzlich klärt Ziffer 14, dass eine Zustimmung zur Datenverarbeitung seitens des Betroffenen immer freiwillig, eindeutig und ohne Zwang abgegeben werden muss. [18]

Der Verwendung von Daten ist im österreichischen Datenschutzgesetz der vollständige 2. Abschnitt gewidmet. So definiert Artikel 2, § 6, dass Daten nur nach Treu und Glauben sowie auf rechtmäßige Weise zur Verwendung kommen dürfen. Weiters müssen die Zwecke eindeutig und von Anfang an fixiert sein und die Verwendung darf über diese nicht hinausgehen. Auch ist festgelegt, dass die Daten immer aktuell gehalten werden müssen und diese keinesfalls länger als bis zum Erreichen der festgelegten Zwecke gespeichert werden dürfen. Verantwortlich für die Einhaltung dieser Regeln ist immer der Auftraggeber oder, bei ausländischem Auftraggeber, ein von ihm benannter inländischer Vertreter. [19]
Zusätzlich setzt der Gesetzgeber in § 7 eindeutig voraus, dass der Empfänger seine Befugnis zur Datenerhebung dem Übermittelnden glaubhaft gemacht und diesen ausreichend aufgeklärt hat. Außerdem erfordert dieser Paragraph die Einhaltung der gelindesten Mittel zur Erhebung und Verarbeitung von Daten. [20]
Allerdings sieht das DSG auch Ausnahmen von der Geheimhaltung vor. Zum einen sind die

[14] Mayer-Schönberger et al.: Datenschutzgesetz [82] (S. 25)
[15] Datenschutzgesetz [25] (S. 4)
[16] Help.gv.at - Datenschutz [114]
[17] Fercher et al.: Aktuelle Fragen des Datenschutzrechts [74] (S. 28)
[18] Datenschutzgesetz [25] (S. 4f.)
[19] Datenschutzgesetz [25] (S. 5f.)
[20] Datenschutzgesetz [25] (S. 6)

Geheimhaltungsinteressen bei nicht-sensiblen Daten unter anderem dann nicht verletzt, wenn der Betroffene der Verwendung seiner Daten zugestimmt hat, wobei diese Zustimmung jederzeit vollständig widerrufen werden kann. Zum anderen gelten diese Interessen nicht als verletzt, wenn die sensiblen Informationen vom Betroffenen selbst veröffentlicht wurden bzw. diese nur in indirekt personenbezogener Weise verwendet werden und somit keinerlei Rückschlüsse auf die Person möglich sind. Zusätzlich ist es zulässig, diese eigentlich sehr schutzwürdigen Daten zu verarbeiten, sofern sie zur medizinischen Behandlung oder Gesundheitsvorsorge des Patienten nötig sind, wobei eindeutig die Geheimhaltungspflicht des medizinischen Personals herauszustreichen ist. [21]

> „Unter die Schweigepflicht fallen alle Informationen und Tatsachen, die dem Arzt und seinen Hilfskräften im Rahmen der Behandlung von Patienten bekannt werden. Dazu gehört auch die Tatsache, dass eine Person z.B. eine Arztpraxis aufsucht.“ [22]

Da es nur logisch erscheint, dass nicht jedes Unternehmen alle (im Speziellen technische) Bereiche einer solchen Datenerhebung mit dem eigenen Personal abdecken kann und es wirtschaftlich auch nicht als sinnvoll erscheint, hat der Gesetzgeber auch für diesen Fall eine Möglichkeit geschaffen. Somit regelt Artikel 2, § 10, Absatz 1, dass ein Auftraggeber berechtigt ist, eine für ihn zulässige Datenerhebung und Verarbeitung an einen Dienstleister auszulagern, sofern dieser Dienstleister alle nötigen datenschutzrelevanten Auflagen und Richtlinien einhält. Es genügt hier aber nicht einfach eine glaubhaft gemachte Zusicherung seitens des Dienstleisters, denn zusätzlich ist der Auftraggeber dazu verpflichtet, die Einhaltung auch wirklich zu kontrollieren. [23]

Ein wenig strenger ist die Übermittlung von Daten ins Ausland, wie Artikel 2, § 12 sicherstellt. Lediglich die Übermittlung der Daten innerhalb des Europäischen Wirtschaftsraumes ist vollkommen genehmigungsfrei, mit Ausnahme des öffentlichen Bereichs in Bezug auf nicht dem EU-Recht unterliegende Belange. Zusätzlich sind Übermittlungen in Drittstaaten ausschließlich dann nicht explizit genehmigungspflichtig, wenn die Drittstaaten angemessene Datenschutzstandards umgesetzt haben, was vom Bundeskanzler zu beurteilen ist, oder wenn die Daten in Österreich zulässigerweise veröffentlicht wurden, die Daten für den jeweiligen Empfänger nur indirekt personenbezogen sind, der Inhaber einer solchen Übermittlung zweifellos zugestimmt hat oder ein Vertrag nur durch das Übermitteln in einen Drittstaat erfüllbar ist. Beinahe jeglicher anderer Datenverkehr ist vor der Übermittlung bei der Datenschutzbehörde genehmigen zu lassen. [24] [25]

Die gesetzlich vorgegebenen Maßnahmen im Bereich des Datenschutzes erstrecken sich allerdings keinesfalls lediglich auf die Erhebung und Verarbeitung von Daten. Auch über den Zeit-

[21] Datenschutzgesetz [25] (S. 7f.)
[22] Höpken et al.: Datenschutz in der Arztpraxis [55] (S. 19)
[23] Datenschutzgesetz [25] (S. 8)
[24] Datenschutzgesetz [25] (S. 8f.)
[25] Knyrim: Datenschutzrecht [77] (S. 113ff)

punkt der Erhebung hinaus ist es notwendig, die Daten sicher und geschützt zu verwahren sowie vor unbefugten Zugriffen zu schützen. Sowohl interne als auch externe Risikoquellen sind dabei zu berücksichtigen. So sieht Artikel 2, § 14, Absatz 2 unter anderem die Regelung von Zutrittsberechtigungen für Räumlichkeiten sowie betreffend die Zugriffsberechtigung auf Datenbestände vor. Weiters ist ein Protokoll über jeden Zutritt und Zugriff zu führen und eine Dokumentation über alle erfolgten Sicherheitsmaßnahmen zu erstellen. Darüber hinaus ist es notwendig, die technischen Maßnahmen immer auf dem aktuellen Stand zu halten, um das Angriffspotential zu minimieren. [26]
Nach Fercher [27] umfasst der Begriff Datensicherheit in der Informatik drei Bereiche: die Vertraulichkeit, welche für die autorisierte Zugriffsberechtigung steht; die Integrität, welche die Richtigkeit, Vollständigkeit und Aktualität der Daten garantiert, sowie die Verfügbarkeit, welche die allgemeine Zugänglichkeit und Erreichbarkeit aller Daten für die autorisierten Personen sicherstellt. [28]
Zusätzlich ist es notwendig, jeden Mitarbeiter zur Geheimhaltung zu verpflichten und eindeutig festzustellen, dass ohne Weisung des Dienstgebers kein Mitarbeiter Daten übermitteln darf. [29]

> „Jeder Mitarbeiter ist über seine nach dem DSG und nach innerorganisatorischen Datenschutzvorschriften einschließlich der Datensicherheitsvorschriften bestehenden Pflichten zu belehren. [...] Mögliche Maßnahmen, mit denen der Belehrungspflicht entsprochen wird, sind innerbetriebliche Schulungen, eine geregelte Einarbeitung neuer Mitarbeiter, eine Herausgabe von Richtlinien oder der Besuch von DSG-Seminaren.“ [30]

Datenerhebende haben selbstverständlich nicht nur Pflichten der Geheimhaltung und des Schutzes. Sie unterliegen auch diversen Informationspflichten. Wie Artikel 2, § 24 feststellt, hat der Auftraggeber über den Zweck der Erhebung zu informieren sowie seinen Namen und eine Kontaktadresse leicht auffindbar und frei zugänglich zu machen. Außerdem ist er verpflichtet, im Falle eines Datendiebstahls oder Verlustes sonstiger Art den Betroffenen zu informieren. [31] Beispielsweise musste die Wirtschaftskammer Österreich nach einem Hacker-Angriff auf ihre Server im Jahr 2011 alle möglicherweise betroffenen Personen über diesen Vorfall informieren. [32]

Zusätzlich zu allen Pflichten auf Seiten der Auftraggeber sieht das österreichische Datenschutzgesetz eine Reihe von Rechten für die Betroffenen vor. Diese werden gesammelt im 5. Abschnitt festgehalten. Jede Person hat das Recht auf Auskunft im Bezug auf die über sie erhobenen, verarbeiteten und gespeicherten Daten bei dem jeweiligen Datenerheber. Die Auskunft muss innerhalb von acht Wochen ergehen. Sofern die Auskunft nicht oder nur teilweise möglich ist,

[26] Datenschutzgesetz [25] (S. 10)
[27] Fercher et al.: Aktuelle Fragen des Datenschutzrechts [74]
[28] Fercher et al.: Aktuelle Fragen des Datenschutzrechts [74] (S. 81)
[29] Datenschutzgesetz [25] (S. 11)
[30] Fercher et al.: Aktuelle Fragen des Datenschutzrechts [74] (S. 86)
[31] Datenschutzgesetz [25] (S. 15)
[32] Futurezone: Anonymous veröffentlicht tausende WKO-Daten [36]

muss eine schriftliche Begründung innerhalb der gleichen Frist erfolgen. Die Regelung zum Auskunftsrecht findet sich in Artikel 2, § 26. [33] Weiters hat jeder Betroffene das Recht auf Aktualisierung seiner Daten beim Auftraggeber. Darüber hinaus muss der Erheber sogar selbst eine Aktualisierung anstreben, sobald er von der Fehlerhaftigkeit seiner Daten erfährt. Außerdem legt Artikel 2, § 28 ein nahezu vollumfängliches Widerspruchsrecht seitens des Inhabers fest. Somit ist der Dateninhaber jederzeit ermächtigt, der Verwendung und Verarbeitung seiner Daten zu widersprechen, sofern diese nicht gesetzlich vorgesehen ist. [34]

Für Internetdienstanbieter, sogenannte „Internet Service Provider (ISP)“, gilt rein rechtlich das Telekommunikationsgesetz (TKG) [35]. Jedoch legt § 92, Absatz 1 des TKG fest, dass bei nicht von diesem Gesetz geregelten Sachverhalten das DSG zur Anwendung kommt und somit ein subsidiäres Recht zum TKG darstellt. [36]

> „Soweit dieses Bundesgesetz nicht anderes bestimmt, sind auf die in diesem Bundesgesetz geregelten Sachverhalte die Bestimmungen des Datenschutzgesetzes 2000, BGBl. I Nr. 165/1999, anzuwenden.“ [37]

In § 93 wird das Kommunikationsgeheimnis genauer deklariert und unter anderem ein nicht bewilligtes Mithören, Abhören, Aufzeichnen oder Abfangen jeglicher Nachrichten sowie Verkehrs- und Standortdaten untersagt. [38] Weiters verpflichtet § 95a, Absatz 1 den Diensteanbieter bei einer Datenschutzverletzung umgehend die Datenschutzbehörde sowie die betroffene Person darüber in Kenntnis zu setzen. [39] Die Ermittlung und Verarbeitung von Stammdaten, Verkehrsdaten, Standortdaten und Inhaltsdaten darf nach § 96, Absatz 1 lediglich für die Durchführung und Aufrechterhaltung der Kommunikationsdienste vollzogen werden. [40] Darüber hinaus müssen nach § 99, Absatz 1 Verkehrsdaten nach Beendigung der Verbindung unverzüglich gelöscht oder anonymisiert werden. Der Gesetzgeber räumt sich allerdings einige Ausnahmen in Absatz 5 ein, welche die weitere Verwendung und Speicherung von Verkehrsdaten unter bestimmten Umständen und Rahmenbedingungen gestattet. [41]

[33] Datenschutzgesetz [25] (S. 16f.)
[34] Datenschutzgesetz [25] (S. 17)
[35] Telekommunikationsgesetz [116]
[36] Telekommunikationsgesetz [116] (S. 50)
[37] Telekommunikationsgesetz [116] (S. 50)
[38] Telekommunikationsgesetz [116] (S. 52)
[39] Telekommunikationsgesetz [116] (S. 53)
[40] Telekommunikationsgesetz [116] (S. 54)
[41] Telekommunikationsgesetz [116] (S. 55f)

2.2 Europäische Rechtsvorschriften

Der europäische Datenschutz ist in vielen Bereichen des europäischen Rechts verankert. Sowohl die EU-Grundrechtecharta, in Artikel 7, [42] als auch die Europäische Menschenrechtskonvention (EMRK), in Artikel 8, [43] sichern den Schutz des Privatlebens und der Kommunikation. [44] Außerdem schützt die EU-Grundrechtecharta in Artikel 8 [45] die Verarbeitung von personenbezogenen Daten in besonderem Maß. Diese grundrechtlichen Verankerungen des Datenschutzes sind selbstverständlich notwendig, aber in ihrer doch sehr simplen, undifferenzierten und detailarmen Ausgestaltung keinesfalls hinreichend. Dies hat die Europäische Union bereits vor der Jahrtausendwende erkannt und dementsprechend die Datenschutzrichtlinie (DSRL) 95/46/EG [46] erlassen. Diese Richtlinie dient sowohl dem Schutz vor der Datenverarbeitung als auch der Ermöglichung des freien Verkehrs von personenbezogenen Daten. Sie hat somit zwei Gegensätze und folglich ein starkes Spannungsfeld zu bewältigen. [47] Zusätzlich ist klar hervorzuheben, dass die Datenschutzrichtlinie 95/46/EG [48] die Grundlage für das nationale Datenschutzrecht der einzelnen Mitgliedsstaaten bildet. Lange Zeit war es umstritten, ob die Richtlinie lediglich eine echte Grundlage und somit einen Mindeststandard vorgibt, was den Mitgliedsländern einen sehr breiten Spielraum zur strengeren Rechtssetzung ermöglicht hätte, oder ob sie die Erlaubnistatbestände zwingend und unumstößlich festsetzt. Dieser Streitfrage erteilte der Europäische Gerichtshof mit einer Entscheidung am 24.11.2011 [49] eine klare Antwort, welche den Mitgliedern eindeutig untersagt, strengere Anforderungen an die Datenverarbeitung zu legen, als die Richtlinie sie vorgibt. [50]

> „Es gilt darüber nachzudenken, wie dort stärker reguliert werden kann, wo größere Gefahren für die Persönlichkeitsrechte zu befürchten sind als bei einer eigentlich „belanglosen Datenverarbeitung“, etwa beim Führen einer Telefonliste, der Nutzung von E-Mail-Diensten oder einem Fax-Gerät. Nutzer von Facebook oder anderen sozialen Netzwerken sollten nicht den gleichen Informations- und Dokumentationspflichten sowie den gleichen Kontroll- und Sanktionsmechanismen unterliegen wie Facebook selbst. [...] Mit der jetzigen Systematik droht die Kapitulation des Datenschutzrechts vor der Komplexität des Internets.“ [51]

Durchaus positiv kann die aktuelle Entwicklung innerhalb der Europäischen Kommission gedeutet werden. Schon 2012 hat man einen ersten Entwurf zu einer Datenschutz-Grundverordnung

[42] EU-Grundrechtecharta [22] (S. C 364/10)
[43] Die Europäische Menschenrechtskonvention [26] (S. 10f)
[44] Tinnefeld et al.: Einführung in das Datenschutzrecht [122] (S. 102f)
[45] EU-Grundrechtecharta [22] (S. C 364/10)
[46] Datenschutzrichtlinie 95/46/EG [104]
[47] Kort: Datenschutzrecht in der Europäischen Union: de lege lata und de lege ferenda [78] (S. 3)
[48] Datenschutzrichtlinie 95/46/EG [104]
[49] Urteil des Gerichtshofs (Dritte Kammer), 24. November 2011 [125]
[50] Kort: Datenschutzrecht in der Europäischen Union: de lege lata und de lege ferenda [78] (S. 4)
[51] o.A.: Ein neues Datenschutzrecht für Europa [88] (S. 3)

[52] vorgelegt, welche die bisherige Datenschutzrichtlinie 95/46/EG [53] ersetzen soll. Sie soll vollständig statt der Datenschutzrichtlinie eingesetzt werden. Darüber hinaus ist, im Gegensatz zur Richtlinie, die Verordnung direkt geltendes Recht und wird somit auch die nationalen Gesetze überlagern. Damit soll eine europaweite Vereinheitlichung des Datenschutzes erzielt und Rechtssicherheit für Verbraucher sowie Anbieter geschaffen werden. [54]

> „Die Verordnung gelte unmittelbar. Man müsse künftig also die betreffende EU-Vorschrift und nicht eine nationale Vorschrift anwenden. Unternehmen würden nicht mehr mit einer Vielzahl von Datenschutzbehörden konfrontiert sein, auch wenn sie in mehreren Ländern aktiv seien.“ [55]

Dies ist ein sehr wünschenswertes Szenario; allerdings werden bereits Stimmen laut, dass durchaus einige Punkte des Entwurfs keinesfalls optimal gelöst sind und dringend einer Überarbeitung unterzogen gehören. [56]

2.2.1 Aktuell geltendes Recht

Aufgrund der bereits angesprochenen Datenschutzrichtlinie 95/46/EG [57] ist es natürlich nicht verwunderlich beziehungsweise sogar zwingend, dass das österreichische Datenschutzrecht den Inhalten der DSRL in vielen Punkten sehr ähnelt.
So sind die Definitionen betreffend „personenbezogene Daten“, „Verarbeitung personenbezogener Daten“, „Verantwortliche“, „Auftragsverarbeiter“, „Empfänger“, sowie die „Einwilligung der betroffenen Person“ in Artikel 2 nahezu ident mit jenen im österreichischen Datenschutzgesetz. [58] Weiters klärt Artikel 3, Absatz 1, dass die Richtlinie sowohl ganz als auch teilweise automatisiert verarbeitete Daten umfasst. [59]
Die DSRL, so wie das österreichische Datenschutzgesetz, sieht in Artikel 6 vor, dass Daten ausschließlich nach Treu und Glauben erhoben, zweckbestimmt eingesetzt, korrekt und aktuell gehalten und nicht länger als notwendig aufbewahrt werden müssen. [60] Darüber hinaus müssen entweder die Einwilligung der betroffenen Person, das Erfordernis der Verarbeitung für eine Vertragserfüllung oder lebenswichtiger Interessen vorliegen. Dies schreibt Artikel 7 fest. [61]
Besonders hervorzuheben ist das in Artikel 8, Absatz 1 festgeschriebene Generalverbot der Verarbeitung jeglicher personenbezogener Daten, aus denen rassische oder ethnische Herkunft, politische Meinung, religiöse Überzeugung sowie gesundheitliche Daten oder Informationen über

[52] Datenschutz-Grundverordnung [126]
[53] Datenschutzrichtlinie 95/46/EG [104]
[54] Kort: Datenschutzrecht in der Europäischen Union: de lege lata und de lege ferenda [78] (S. 4)
[55] Kramer: Licht und Schatten im künftigen EU-Datenschutzrecht [79] (S. 1)
[56] Kort: Datenschutzrecht in der Europäischen Union: de lege lata und de lege ferenda [78] (S. 6)
[57] Datenschutzrichtlinie 95/46/EG [104]
[58] Datenschutzrichtlinie 95/46/EG [104] (S. Nr. L 281/38f)
[59] Datenschutzrichtlinie 95/46/EG [104] (S. Nr. L 281/39)
[60] Datenschutzrichtlinie 95/46/EG [104] (S. Nr. L 281/40)
[61] Datenschutzrichtlinie 95/46/EG [104] (S. Nr. L 281/40)

das Sexualleben hervorgehen. Diese Daten werden in der österreichischen Rechtsprechung kurz „sensible Daten“ genannt. Ausnahmen von diesem Generalverbot werden nachfolgend in Absatz 2 festgelegt. Dazu zählt unter anderem die Möglichkeit der Verarbeitung, wenn der Betroffene eindeutig, freiwillig und unmissverständlich dieser zugestimmt hat oder diese zur Wahrung lebenswichtiger Interessen nötig ist. Eine weitere Ausnahme bildet Absatz 3, welcher die Verarbeitung gestattet, sofern sie der Gesundheitsvorsorge dient und die verarbeitenden Personen ohnehin durch eine entsprechende Geheimhaltungspflicht gebunden sind. [62]
Die DSRL sieht in Artikel 10 vor, dass der Datenerhebende dem Betroffenen gewisse Informationen über sich selbst zur Verfügung stellen muss. Dazu zählt unter anderem seine Identität und der Zweck der Erhebung. [63] Ebenfalls zählt das Auskunftsrecht des Betroffenen dazu sowie das Recht auf Aktualisierung bzw. Löschung der Daten, sofern sie nicht der Richtlinie entsprechend verarbeitet wurden. [64] In Artikel 14 ist weiter das Widerspruchsrecht der betroffenen Person geregelt. Gleichwohl wie im österreichischen Datenschutzrecht, ist in der DSRL verankert, dass jeder Betroffene das Recht auf Widerspruch zur initialen bzw. weiteren Verarbeitung seiner Daten hat. [65]
Der Schutz der Vertraulichkeit der Daten in Bezug auf Angestellte, welche für den Verarbeiter tätig sind, findet sich in Artikel 16 wieder. Dieser besagt, dass diese Personen nur auf Weisung des Verantwortlichen tätig werden dürfen. [66]

Die Übermittlung von Daten an bzw. in ein Drittland ist in Artikel 25, Absatz 1 prinzipiell untersagt. Eine Ausnahme ermöglicht ein angemessenes Schutzniveau im Drittland. Nur unter dem Gesichtspunkt der Angemessenheit, welcher sich nach Absatz 2 aus mehreren Faktoren, aber wohl primär aus der Rechtslage des Drittlandes, zusammensetzt, ist es erlaubt, personenbezogene Daten in dieses Land zu transferieren. [67] Die Ausnahmeregelung zu diesem Verbot, in ein nach dieser Richtlinie als unsicher geltendes Land, personenbezogene Daten übermitteln zu dürfen, stellt Artikel 26 mit mehreren Punkten dar. Unter anderem ist es erlaubt, in ein solches Land Daten zu exportieren, sofern der Betroffene freiwillig und ohne jeden Zweifel die Einwilligung dazu erteilt hat. [68]

Eine weitere wichtige Stütze des europäischen Datenschutzrechts ist die Richtlinie 2002/58/EG [69], oftmals als „E-Datenschutzrichtlinie“ bezeichnet, welche sich primär mit der Vertraulichkeit der Daten bei der Erhebung, Übermittlung und Verarbeitung befasst. Sie ist zukunftsorientiert und technikneutral ausgestaltet und hat somit den Vorteil, bei fortschreitender Technologie nicht innerhalb kürzester Zeit durch den neuen Stand der Technik und die damit verbundenen neuen Anforderungen als veraltet angesehen werden zu müssen. Außerdem wird damit die Richtlinie

[62] Datenschutzrichtlinie 95/46/EG [104] (S. Nr. L 281/40f)
[63] Datenschutzrichtlinie 95/46/EG [104] (S. Nr. L 281/41)
[64] Datenschutzrichtlinie 95/46/EG [104] (S. Nr. L 281/42)
[65] Datenschutzrichtlinie 95/46/EG [104] (S. Nr. L 281/42f)
[66] Datenschutzrichtlinie 95/46/EG [104] (S. Nr. L 281/43)
[67] Datenschutzrichtlinie 95/46/EG [104] (S. Nr. L 281/45f)
[68] Datenschutzrichtlinie 95/46/EG [104] (S. Nr. L 281/46)
[69] E-Datenschutzrichtlinie 2002/58/EG [103]

97/66/EG [70] ersetzt. [71]
Als Beispiel kann die Definition der Begrifflichkeit „Verkehrsdaten“ angegeben werden. Die Richtlinie legt zum einen in Artikel 2 [72] fest, welche Daten als Verkehrsdaten gelten, und zum anderen definiert sie in Artikel 6 [73], zu welchem Zweck diese verwendet werden dürfen und welche Pflichten, darunter eine Informationspflicht an den Betroffenen, der Datenverarbeiter hat.
Wie Kort explizit herausstreicht, reglementiert die Richtlinie die Verwendung der Daten sehr streng, da die erlaubte Verwendung der Daten keinesfalls über die typischen Anwendungen für Telekommunikationsdienste hinausgehen darf. Jegliche andere Verwendung erfordert eine explizite Einwilligung des Betroffenen. [74]

Besonders und gesondert hervorzuheben ist die Stellungnahme der Artikel 29-Gruppe im Jahr 2011 zum Thema der Geolocation-Services. Man hat festgestellt, dass die E-Datenschutzrichtlinie keine Anwendung findet, sofern die Anbieter der Dienste nicht gleichzeitig auch Netzbetreiber sind. In vielen Fällen wird dies aber nicht der Fall sein. Weiter hat die Gruppe klargestellt, dass sich Anbieter solcher Geo-Services keinesfalls im rechtsfreien Raum befinden, sondern vielmehr der Datenschutzrichtlinie unterliegen. [75]

> „Es sei einem Anbieter von Geolocation-Diensten und -Anwendungen möglich, die genaue Lage eines WiFi-Zugangspunktes basierend auf der entsprechenden Signalstärke herauszufinden. [...] Beispielsweise könne der Besitzer einer Wohnung oder eines Hauses, wo sich ein bestimmter WiFi-Zugangspunkt befindet, indirekt identifiziert werden.“ [76]

2.2.2 Ausblick auf das neue europäische Datenschutzrecht

Auch der Europäischen Kommission ist schon seit einigen Jahren klar, dass die aktuelle Rechtslage im Bereich des Datenschutzes suboptimal ist. Einerseits sind die vorhandenen Vorschriften nicht mehr zeitgemäß und erfassen die aktuellen Anforderungen und Bedürfnisse der Bürger sowie der Wirtschaft nicht ausreichend, was zu einer Verringerung des Datenschutzes und Steigerung der Rechtsunsicherheit führt; andererseits ist es für alle Parteien ungünstig, im europäischen Raum keine einheitlichen Regeln vorzufinden. Gerade in der heutigen Zeit mit der immer noch weiter zunehmenden Bedeutung von Internet, Smartphones und dem damit verbundenen Datenaustausch, welcher spielend über Landesgrenzen hinweg geht, ist eine Vereinheitlichung

[70] Richtlinie 97/66/EG [105]
[71] Reimer et al.: Handbuch Datenschutzrecht [10] (S. 59)
[72] E-Datenschutzrichtlinie 2002/58/EG [103] (S. L 201/43)
[73] E-Datenschutzrichtlinie 2002/58/EG [103] (S. L 201/44)
[74] Kort: Datenschutzrecht in der Europäischen Union: de lege lata und de lege ferenda [78] (S. 4)
[75] Hladjk: EU-Datenschutzrecht und Geolocation-Services [53] (S. 1)
[76] Hladjk: EU-Datenschutzrecht und Geolocation-Services [53] (S. 1)

zumindest innerhalb des Europäischen Wirtschaftsraumes notwendig. Bei entsprechender Umsetzung ist sogar von einem Standortvorteil die Rede. [77]

> „Mit einer solch rechtssicheren aber technikneutralen Verordnung und einem starken Datenschutz für die ganze EU könnte sich Europa einen Standortvorteil im globalen Markt erarbeiten.“ [78]

Somit hat die Europäische Kommission im Jänner 2012 einen Vorschlag zur Reform des europäischen Datenschutzrechts gemacht. Dieser Vorschlag sieht die Ablöse der Datenschutzrichtlinie 95/46/EG [79] durch eine direkt in allen Mitgliedsstaaten geltende Datenschutz-Grundverordnung [80] vor. Diese Grundverordnung soll sowohl den länderübergreifenden Austausch und die Verarbeitung von personenbezogenen Daten regeln und somit die Wirtschaftszweige stärken, die ihre Geschäftsmodelle auf diesen Bereichen aufbauen, als auch den Betroffenen mehr Schutz und Rechtssicherheit vor allfälligen Gesetzesübertretungen und Datenmissbrauch bieten. Klares designiertes Ziel ist es, die Privatsphäre der Bürger stärker und besser zu schützen und nicht weiterhin eine starke Zersplitterung des Datenschutzes durch die einzelnen landesspezifischen Umsetzungen innerhalb der Europäischen Union zuzulassen. [81]

Durchaus lässt auch der starke politische Rückhalt und Nachdruck der maßgeblichen amtierenden Politiker, wie unter anderem der deutschen Bundeskanzlerin Angela Merkel, auf einen positiven und raschen Ausgang der Entwurfsarbeiten hoffen. [82]

Schon wie die Datenschutzrichtlinie aus dem Jahr 1995 zielt auch der Entwurf der Datenschutz-Grundverordnung nicht auf zu detaillierte und ausdefinierte Regelungen ab, sondern ist bemüht, einen Rahmen für die Anwendungen und technischen Gegebenheiten zu schaffen. [83]

> „Wir regeln bewusst nicht Google Street View oder den Datenschutz bei Apps, sondern konzentrieren uns auf Grundprinzipien und allgemeine Vorgaben des Datenschutzes.“ [84]

Ein sehr interessanter Ansatz in diesem Bereich, welcher bereits im Jahr 2007, folglich fünf Jahre vor dem ersten Entwurf der Verordnung, in einer Mitteilung der Kommission an das Europäische Parlament und den Rat [85] angedacht wird, ist die Einstellung „Datenschutz durch

[77] Albrecht: Starker EU-Datenschutz wäre Standortvorteil [2]
[78] Albrecht: Starker EU-Datenschutz wäre Standortvorteil [2] (S. 657)
[79] Datenschutzrichtlinie 95/46/EG [104]
[80] Datenschutz-Grundverordnung [126]
[81] Kort: Datenschutzrecht in der Europäischen Union: de lege lata und de lege ferenda [78] (S. 4)
[82] Reimer: Merkel: Acht-Punkte-Programm für einen europäischen und internationalen Datenschutz [100] (S. 675)
[83] Friedrich: International: EU-Datenschutzrecht soll vereinheitlicht werden [35] (S. 2)
[84] Friedrich: International: EU-Datenschutzrecht soll vereinheitlicht werden [35] (S. 2)
[85] Mitteilung der Kommission an das Europäische Parlament und den Rat [84] (S. 3f)

Technik“ bzw. „privacy by design“. Damit verfolgt man den Gedanken, dass eine vom Technologiestand unabhängige Einstellung der Menschen bzw. Wirtschaftstreibenden vorangetrieben wird, welche den Datenschutz bereits bei der Entwicklung der Produkte als fixe Größe und wichtigen Punkt mit einplant. Dies bedeutet, dass sich Entwickler und Designer bereits bei der Erstellung ihrer Produkte, getrieben durch die Datenschutz-Grundverordnung, darüber Gedanken machen müssen, welche Daten sie zu welchem Zeitpunkt wirklich benötigen und keinesfalls mehr als diese erheben bzw. verarbeiten. Bei Social-Media-Plattformen etwa wäre das möglich, indem man ohne die eindeutige und ausdrückliche Zustimmung des Betroffenen keinerlei Daten öffentlich anzeigt. [86] Als Beispiel kann man die Aktion von Facebook nennen, welche die Standard-Einstellung für das Veröffentlichen neuer Status-Nachrichten von „Öffentlich“ auf „Freunde“ Anfang 2014 umgestellt hat. [87] Allerdings ist hier zu betonen, dass, auch wenn dieses Vorgehen lobenswert ist, es keinesfalls den kompletten Gedanken von „Datenschutz durch Technik“ ausreichend und vollständig erfüllt.

Der Entwurf sieht weiter vor, dass das Auskunftsrecht der Betroffenen deutlich gestärkt wird und pro Land eine zentrale nationale Datenschutzbehörde als alleiniger Ansprechpartner gelten soll. Dies läuft unter dem Begriff „one-stop-shop“-System. Diese Behörden sollen außerdem eine völlige Unabhängigkeit vom Staat erhalten und zusätzlich neue und stärkere Mittel bekommen, um gesetzliche Rahmenbedingungen bei Verstößen durchzusetzen. So sieht beispielsweise die Verordnung vor, dass ein Rechtsverstoß mit bis zu einer Million Euro oder zwei Prozent des Jahresumsatzes des Unternehmens bestraft werden kann. [88]

Ebenfalls beschäftigt sich der Entwurf mit der Tatsache, dass einmal eingegebene Daten, speziell in sozialen Netzwerken, nie wieder aus den Datenbanken der Betreiber verschwinden und der Verbraucher aktuell kaum die Möglichkeit hat, eine Löschung durchzusetzen. Dies soll sich, nach Wünschen der Europäischen Kommission, mit dem „Recht auf Vergessenwerden“ ändern. Dies sieht eine Rechtsgrundlage des Betroffenen zur vollständigen Löschung seiner bisher erhobenen Daten bei einem Dienst vor. Prinzipiell ein sehr guter Ansatz, speziell, wenn man diverse durchaus freiwillige Veröffentlichungen der Bürger in jungen Jahren auf Social-Media-Plattformen bedenkt, welche diesen im Erwachsenenalter wohl weitaus weniger attraktiv erscheinen werden. Leider ist die Durchsetzung einer solchen vollständigen Löschung von Daten praktisch sehr schwer bis kaum zu realisieren. Man bedenke, dass in einem sozialen Netzwerk nicht nur der Benutzer selbst Daten, wie Fotos, von sich selbst einstellt, sondern auch andere Benutzer Daten von diesem einstellen können. Somit wäre ein echtes „Vergessen“ dieser Person zwangsläufig auch eine Sperrung bzw. Löschung von Inhalten, die andere Benutzer erstellt haben bzw. deren Rechte sie besitzen - sofern man davon ausgeht, dass eine Software intelligent genug entwickelt ist, überhaupt alle Inhalte, diese Person betreffend, zu finden.[89]

[86] Kort: Datenschutzrecht in der Europäischen Union: de lege lata und de lege ferenda [78] (S. 4)
[87] The Next Web: Facebook changes default privacy setting of new users' posts from Public to Friends [130]
[88] Kort: Datenschutzrecht in der Europäischen Union: de lege lata und de lege ferenda [78] (S. 4f)
[89] Kort: Datenschutzrecht in der Europäischen Union: de lege lata und de lege ferenda [78] (S. 5)

Die Verordnung soll auch die Problematik entschärfen, welche sich aktuell stellt, wenn ein Unternehmen aus einem Drittland, sprich außerhalb der Europäischen Union, Daten innerhalb der EU erhebt. So soll sich zukünftig ein betroffener Bürger der EU an heimische Datenschutzbehörden wenden können, wenn er einen Verstoß gegen das europäische Datenschutzrecht melden will. Derzeit muss sich der Dateninhaber an die zuständige Behörde des Sitzstaates des Unternehmens wenden und sich den dort geltenden Rechtsvorschriften und -gepflogenheiten unterwerfen. Dies ist für eine einzelne Privatperson nahezu unmöglich. [90]

Es gibt allerdings auch deutliche Kritikpunkte an dem Entwurf in seiner ursprünglichen Form. So kritisiert unter anderem Kort, dass, speziell in Deutschland, die Position der betrieblichen Datenschutzbeauftragten massiv geschwächt wird. Derzeit muss ein solcher Beauftragter nach deutschem Recht ab einer Anzahl von neun Mitarbeitern, welche sich überwiegend mit Datenverarbeitung beschäftigen, bestellt werden. In dem Entwurf der Datenschutz-Grundverordnung ist dieser erst ab einer Mitarbeiteranzahl von 250 vorgesehen. [91]
Zusätzlich wird, ebenfalls speziell in Deutschland, der Wegfall der nationalen Gesetze scharf kritisiert. Da ein Inkrafttreten der Grundverordnung die nationalen Gesetze überlagern würde und diese somit nicht mehr zu Anwendung kämen, würden auch viele kleine, aber nicht weniger wichtige Spezialgesetze im Bereich des Datenschutzes und der informationellen Selbstbestimmung wegfallen. Weiters ist noch völlig unklar, inwieweit die nationalen Gesetzgeber nach einem Inkrafttreten der Grundverordnung überhaupt noch Spielräume hätten. [92] [93] [94]
Konkret kann man als Beispiel das sehr ausdifferenzierte und strenge Beschäftigungsdatenschutzrecht anführen, bei welchem nach Inkrafttreten der Datenschutz-Grundverordnung vollkommen fraglich ist, in welchem Ausmaß es noch Gültigkeit hätte. Darunter fallen unter anderem die Vorgaben zur Videoüberwachung oder der Kündigungsschutz von Datenschutzbeauftragten. [95] Auch wird befürchtet, dass das ohnehin angespannte Verhältnis zwischen den USA und Europa im Bereich des Datenschutzes noch weiter aufgebrochen wird, da die beiden Parteien bereits heute sehr unterschiedliche Ansichten in diesem Bereich vertreten. Dies könnte mit einer Verschärfung der Gesetzgebung in diesem Bereich noch weiteren Diskussionsstoff bieten. [96]

Ein relativ versteckter, wenn auch nicht unwesentlicher Problemfall eröffnet sich, wenn man die Anwendbarkeit des Verordnung auf unentgeltliche Dienstleistungen betrachtet. Auf europarechtlicher Ebene gilt eine Dienstleistung nur als solche, sofern sie gegen Entgelt erbracht wird. Sofort stellt sich hier die Frage, wie mit grundsätzlich unentgeltlichen Angeboten zu verfahren

[90] Kort: Datenschutzrecht in der Europäischen Union: de lege lata und de lege ferenda [78] (S. 6)
[91] Kort: Datenschutzrecht in der Europäischen Union: de lege lata und de lege ferenda [78] (S. 6)
[92] Kort: Datenschutzrecht in der Europäischen Union: de lege lata und de lege ferenda [78] (S. 6)
[93] Härting: Datenschutzreform in Europa: Einigung im EU-Parlament: Kritische Anmerkungen; Computer und Recht [56] (S. 716)
[94] Schneider et al.: Datenschutz in Europa – Plädoyer für einen Neubeginn: Zehn „Navigationsempfehlungen“, damit das EU-Datenschutzrecht internettauglich und effektiv wird [111] (S. 307)
[95] Schüßler et al.: EU-Datenschutz-Grundverordnung und Beschäftigtendatenschutz [110] (S. 643)
[96] Kort: Datenschutzrecht in der Europäischen Union: de lege lata und de lege ferenda [78] (S. 6)

ist. Selbstverständlich liegt auch hinter diesen ein Geschäftsmodell, und die Einnahmen gestalten sich oftmals durch Werbung und Verwertung der erhobenen personenbezogenen Daten, aber ob dies den Aspekt der Entgeltlichkeit erfüllt, ist nicht klar definiert. [97]
Nicht zu unterschätzen ist weiters die Problematik des generalisierten Verbotsprinzip. Der Entwurf der Verordnung stützt seine Grundsätze, ebenso wie viele nationale Rechtssetzungen sowie die bisher geltende europäische Datenschutzrichtlinie, auf das Prinzip des Generalverbots zur Verarbeitung von personenbezogenen Daten und räumt in weiterer Folge lediglich einzelne Ausnahmen ein. Dieses Vorgehen allerdings muss laut mancher Expertenmeinung als verfassungswidrig angesehen werden, da die grundsätzlich freie Verarbeitung von Daten genauso als Teil der Menschenwürde und Entfaltungsfreiheit verstanden werden muss. [98]

2.3 Amerikanische Rechtsvorschriften

Die amerikanische Rechtslage ist insofern ungleich schwieriger zu beurteilen, als sich die Rechtsprechung in den Vereinigten Staaten von der europäischen grundlegend unterscheidet. Unter anderem beruht die Entscheidungsfindung der Richter neben den Gesetzestexten auch wesentlich auf den Entscheidungen anderer Richter in ähnlichen vorangegangenen Fällen. Somit kommt sogenannten Präzedenzfällen viel größere Bedeutung zu als in anderen Ländern. Man spricht daher auch von einem „Case Law“. Zusätzlich muss erwähnt werden, dass es wenig Bundesgesetze gibt, sondern vielmehr - auch in juristischer Sicht - auf Selbstverwaltung der einzelnen Bundesstaaten gesetzt wird. [99]

> „In den USA existiert nur ein schwach ausgeprägter verfassungsrechtlicher Datenschutz, der sich primär gegen staatliche Stellen wendet. Anders ist die Situation in den einzelnen Bundesstaaten.“ [100]

Dies spiegelt sich natürlich auch im Bereich des Schutzes von personenbezogenen Daten wieder. Es gibt bereichsspezifische Schutzvorschriften, auf welche in den folgenden Kapiteln noch genauer eingegangen wird. Im Wesentlichen wird der Datenschutz aber eher der Eigenverantwortung der Bürger und Wirtschaft übergeben. Man pflegt den Gedanken, dass ein Unternehmen, welches einen unerwünschten Umgang mit Daten gegen den Willen der Bürger durchführt, ohnehin nicht lange überleben kann. Somit sollte es im Eigeninteresse jedes Unternehmens sein, sich den Wünschen der Bürger anzupassen. Problematisch wird es lediglich, wenn die Materie so komplex oder neuartig ist, dass der Bürger die Gefahr nicht erkennen oder beurteilen kann. [101]

[97] Wieczorek: Der räumliche Anwendungsbereich der EU-Datenschutz Grundverordnung [134] (S. 647)
[98] Giesen: Für ein verfassungsgemäßes Datenschutzrecht in Europa: Wann beginnt die EU, sich auf ihre freiheitlichen Prinzipien zu besinnen? [40] (S. 551f)
[99] Wagner: Das Safe-Harbor Modell; Datenschutzbestimmungen in der Relation EU-USA [128] (S. 27)
[100] Tinnefeld: Rechtliche und technische Rettungsanker für Privatheit und Datenschutz [121] (S. 582)
[101] Wagner: Das Safe-Harbor Modell; Datenschutzbestimmungen in der Relation EU-USA [128] (S. 32f)

2.3.1 U.S. Constitution

Vorweg kann klargestellt werden, dass die Verfassung, im Original „Constitution“ [102] genannt, der United States of America (USA) kein Recht vorsieht, um personenbezogene Daten zu schützen. [103] Lediglich in der „Bill of Rights“ [104], genauer gesagt im vierten Zusatzartikel der Verfassung, findet sich das Recht auf Schutz der Bürger und deren Eigentum. Dies könnte als Grundstein für einen etwaigen persönlichen Datenschutz gesehen werden; wobei eindeutig festzuhalten ist, dass aufgrund der Formulierung des Artikels dieser wohl eher auf den Schutz der Bürger vor überbordenden Maßnahmen der Staatsgewalt, wie zum Beispiel Hausdurchsuchungen, bezogen ist, als auf den Schutz der Bürger untereinander. [105]

Problematisch ist allerdings die extreme Weite der Rede- und Meinungsfreiheit, welche durch den ersten Verfassungszusatz garantiert wird. Dieser gibt laut amerikanischen Gerichten den Bürgern - und somit auch der Wirtschaft - das sehr umfassende Recht, personenbezogene Daten zu erheben beziehungsweise zu sammeln und zu verwenden. Man erkennt hier leicht das große Konfliktpotenzial, welches sich durch eine stärkere Reglementierung des Datenschutzes ergeben kann. [106]

2.3.2 The Privacy Act of 1974

Im Jahr 1974 haben die USA ein Gesetz zum Schutz der Bürger vor unerlaubter Datensammlung durch Bundesbehörden erlassen, den sogenannten „Privacy Act of 1974“ [107]. Es soll dem Bürger mehr Rechte und Möglichkeiten der Kontrolle bei der Datenerhebung einer Bundesbehörde geben. Damit ist unter anderem ein Recht auf Einsicht und, falls notwendig, Korrektur eingeschlossen. Bemerkenswert an diesem Gesetz sind aber besonders zwei Dinge: Zum einen umfasst das Gesetz lediglich Bundesbehörden und keine Behörden der einzelnen Bundesstaaten, zum anderen wird der verwendete Begriff „Routinegebrauch“ nicht näher definiert, woraus sich ein sehr unscharfes Bild der Abgrenzung ergibt. Daher liegt die Vermutung nahe, dass durch das Gesetz nahezu kein Schutz erwirkt wird. [108]

2.3.3 The Privacy Protection Act of 1980

Der Schutz von Journalisten, Autoren und Nachrichtenagenturen bezüglich ihrer Arbeit und ihren Quellen beziehungsweise Informanten ist durch den „Privacy Protection Act of 1980“ [109]

[102] Constitution of the United States [24]
[103] Hardenberg: Individualisierte Medizin in den USA [49] (S. 620)
[104] Bill of Rights [11]
[105] Wagner: Das Safe-Harbor Modell; Datenschutzbestimmungen in der Relation EU-USA [128] (S. 27)
[106] Wagner: Das Safe-Harbor Modell; Datenschutzbestimmungen in der Relation EU-USA [128] (S. 28)
[107] Privacy Act of 1974 [97]
[108] Wagner: Das Safe-Harbor Modell; Datenschutzbestimmungen in der Relation EU-USA [128] (S. 28f)
[109] Privacy Protection Act of 1980 [98]

gewährleistet. In diesem Gesetz wird festgehalten, dass eine Einsichtnahme sowie Beschlagnahme einschlägiger Materialien durch Behörden ausschließlich bei strafrechtlicher Verfolgung oder Gefahr für die nationale Sicherheit zulässig ist. [110] [111]

2.3.4 The Right of Financial Privacy Act of 1978

Der „Right of Financial Privacy Act of 1978“ [112] wurde nach einer Entscheidung des „U.S. Supreme Court“ im Jahr 1976 eingeführt, dass Kontoinhaber keinerlei Recht auf Privatheit und Datenschutz hätten. Dieses Gesetz schützt zwar nicht vollständig vor Zugriffen der Behörden, jedoch erlegt es den Behörden die Pflicht auf, jeden Kontoinhaber vor dem Zugriff ausreichend darüber zu informieren und gibt diesem das Recht, Einspruch zu erheben. [113] [114]

2.3.5 The Fair Credit Reporting Act of 1970

Der „Fair Credit Reporting Act of 1970“ [115] stellt eine der größten Einschränkungen im Bereich des amerikanischen Datenschutzes dar. Zwar erstrecken sich die Reglementierungen lediglich auf den Gebrauch und keinesfalls auf die Qualität und Quantität der Daten, dennoch ist dies ein großer Schritt für den Datenschutz in diesem Land. Somit sind alle Unternehmen oder Unternehmensteile, welche sich die Bonitätsprüfung [116] von Bürgern als Geschäftsziel erkoren haben, zumindest zu einer Zweckbindung der erhobenen Daten verpflichtet. Zusätzlich garantiert das Gesetz dem Überprüften ein Recht auf Einsicht und Korrektur der über ihn gesammelten Daten - sofern dieser überhaupt Kenntnis über die Sammlung und Speicherung der Daten erlangt, da eine Informationspflicht des Betroffenen nicht existiert. [117] [118]

2.3.6 The Drivers Privacy Protection Act of 1994

Vor dem Jahr 1994 war das Melderegister für Kraftfahrzeuge samt allen Informationen öffentlich einsehbar. Dies ermöglichte einem Fan, sein Idol aufzuspüren und auch zu ermorden. Durch den „Drivers Privacy Protection Act of 1994“ [119] ist es seitdem grundsätzlich verboten, Daten aus

[110] Wagner: Das Safe-Harbor Modell; Datenschutzbestimmungen in der Relation EU-USA [128] (S. 29)
[111] Electronic Privacy Information Center: The Privacy Protection Act of 1980 [20]
[112] Right to Financial Privacy Act of 1978 [106]
[113] Wagner: Das Safe-Harbor Modell; Datenschutzbestimmungen in der Relation EU-USA [128] (S. 29)
[114] Electronic Privacy Information Center: The Right to Financial Privacy Act [21]
[115] Fair Credit Reporting Act of 1970 [33]
[116] Brunst: Anonymität im Internet - rechtliche und tatsächliche Rahmenbedingungen [15] (S. 33)
[117] Wagner: Das Safe-Harbor Modell; Datenschutzbestimmungen in der Relation EU-USA [128] (S. 29f)
[118] Electronic Privacy Information Center: The Fair Credit Reporting Act (FCRA) and the Privacy of Your Credit Report [19]
[119] Drivers Privacy Protection Act of 1994 [28]

diesem Register öffentlich zu machen oder an Dritte weiterzugeben. Dies gilt für Behörden, Polizeibeamte sowie Dienstleister gleichermaßen. [120] [121]

2.3.7 The Telephone Consumer Protection Act of 1991

Die USA sind ein Paradies der Werbeindustrie. Dies ist allgemein und hinlänglich bekannt. [122] Man ist nicht einmal am Telefon sicher vor Werbung. Es geht sogar so weit, dass Werbeagenten die vermeintlichen Kunden anrufen dürfen, um ein Produkt zu bewerben. Jedoch führte der „Telephone Consumer Protection Act of 1991“ [123] einige sehr begrüßenswerte Untersagungen ein. Seitdem ist es unter anderem nicht mehr erlaubt, automatische Wählanlagen zu verwenden. Diese gab es in mehreren Ausführungen. Einerseits haben diese Geräte automatisch Telefonnummern angerufen und ein Tonband abgespielt, sobald der Anruf entgegengenommen wurde. Andererseits wurden viele Nummern von der Anlage zeitgleich angerufen, die erste Person, die abgehoben hatte, wurde zu einem Werbeagenten durchgestellt, die anderen bekamen keine Verbindung. Dies hat natürlich zur Folge, dass bei den Kunden, die keine Verbindung bekommen haben, zu einem späteren Zeitpunkt erneut versucht wurde, anzurufen. Demzufolge war es möglich, dass bei ein und der selben Nummer sehr oft das Telefon geläutet hat, ohne dass jemals ein Agent am Hörer war. Die Frustration und Verärgerung der Nummerninhaber liegt auf der Hand. [124] Zusätzlich wurden sogenannte „do-not-call“ Listen eingeführt, welche von den Marketingfirmen verpflichtend zu berücksichtigen sind. Der erwünschte Erfolg blieb bisher leider aus. [125] Daher ist es auch nicht weiter verwunderlich, dass Telekommunikationskonzerne beide Seiten bedienen. Sie stellen sowohl den Telefonmarketingfirmen Geräte, Informationen sowie Schulungen zur Verfügung, um deren Marketing besser durchführen zu können. Gleichzeitig bietet der gleiche Konzern für die Nummerninhaber auch kostenpflichtige Angebote zum Schutz vor derartigem Marketing an. [126]

2.3.8 The Children's Online Privacy Protection Act of 1998

Ein für amerikanische Datenschutzverhältnisse sehr außergewöhnliches Recht findet man in dem „Children's Online Privacy Protection Act of 1998“ [127]. Die Besonderheit liegt in diesem Fall nicht an dem eingeführten speziellen Datenschutz für Kinder - definiert als Bürger unter 13 Lebensjahren - sondern vielmehr darin, dass es erstmalig nicht auf die Art der erhobenen Daten

[120] Wagner: Das Safe-Harbor Modell; Datenschutzbestimmungen in der Relation EU-USA [128] (S. 30)
[121] Electronic Privacy Information Center: The Drivers Privacy Protection Act (DPPA) and the Privacy of Your State Motor Vehicle Record [18]
[122] Temath: Kulturelle Parameter in der Werbung: Deutsche und US-amerikanische Automobilanzeigen im Vergleich [118] (S. 32ff)
[123] Telephone Consumer Protection Act of 1991 [117]
[124] Electronic Privacy Information Center: Telemarketing and the Telephone Consumer Protection Act (TCPA) [17]
[125] Wagner: Das Safe-Harbor Modell; Datenschutzbestimmungen in der Relation EU-USA [128] (S. 30)
[126] Electronic Privacy Information Center: Telemarketing and the Telephone Consumer Protection Act (TCPA) [17]
[127] Children's Online Privacy Protection Act of 1998 [23]

beschränkt ist, sondern vollumfänglichen Datenschutz für diese Personengruppe gewährleisten soll. [128] Im Speziellen ergeben sich durch diesen Rechtsakt einige Pflichten für den Datensammler sowie Rechte für den Betroffenen. In erster Linie ist hervorzuheben, dass Kinder nicht alleine entscheidungsfähig sein können, und dementsprechend wird ein großer Wert auf die Information und das Einverständnis der Eltern gelegt. Somit sieht das Gesetz die eindeutige vorherige Einwilligung der Eltern zu einer möglichen Datensammlung vor. Zusätzlich müssen alle gesammelten Daten der Kinder für die Eltern offengelegt werden und einsehbar sein. Des Weiteren verpflichtet sich der Datenerhebende zu besonderer Sorgfalt, Verschwiegenheit und Schutz der Daten in Bezug auf Zugriffe befugter wie unbefugter Dritter. Außergewöhnlich und damit besonders erwähnenswert ist auch das Recht der Eltern auf Beendigung der Datenerhebung sowie auf die vollständige Löschung aller bisher erhobenen Daten. [129]

2.3.9 The Health Insurance Portability and Accountability Act of 1996

Um den Austausch von Gesundheitsdaten innerhalb der gesamten Vereinigten Staaten von Amerika zwischen Krankenhäusern und Versicherungsanstalten zu ermöglichen, wurde 1996 der „Health Insurance Portability and Accountability Act of 1996“ [130] erlassen. Dieser Act betrifft sowohl die Daten zur Patientenidentifizierung als auch deren bisherige Krankengeschichte sowie aktuelle Behandlungen. Selbst genetische Informationen zählen dazu. Das Gesetz regelt somit sowohl die Ermöglichung des Datenaustauschs als auch den Schutz dieser Daten vor unbefugten Zugriffen. Dies wird gewährleistet durch das Prinzip der Datensparsamkeit und der Datenhoheit des Patienten. Das bedeutet, dass der Patient der alleinige Verfüger seiner Daten ist. Er alleine kann und muss vor jeglicher Einsicht entscheiden, wer Einsicht nehmen darf und welche Daten eingesehen werden dürfen. Ebenfalls ist der Patient ermächtigt, seine eigenen Daten einzusehen und gegebenenfalls eine Korrektur oder Änderung zu erwirken. [131]

2.3.10 The Genetic Information Nondiscrimination Act of 2008

Der „Genetic Information Nondiscrimination Act of 2008“ [132] regelt, wie der Name bereits vermuten lässt, den Umgang mit genetischen Informationen von Bürgern. Er verbietet sowohl Arbeitgebern als auch Versicherungsanstalten die Nachfrage oder die Anforderung eines Gentests. Weiters wird Versicherungen jegliche Art der Profilerstellung aufgrund solcher Informationen untersagt. Daraus ergibt sich das Verbot von Anpassungen des Versicherungsschutzes oder der Versicherungsbeiträge auf Grundlage von Gendaten. Der Schutz erstreckt sich außerdem auch auf die ableitbaren Geninformationen der Familiengeschichte. Somit ist es, wenn auch medizinisch durchaus relevant, nicht zulässig, für die betroffenen Gruppen ein erhöhtes Brust-

[128] Wagner: Das Safe-Harbor Modell; Datenschutzbestimmungen in der Relation EU-USA [128] (S. 30f)
[129] Electronic Privacy Information Center: Children’s Online Privacy Protection Act (COPPA) [16]
[130] Health Insurance Portability and Accountability Act of 1996 [51]
[131] Hardenberg: Individualisierte Medizin in den USA [49] (S. 620f)
[132] Genetic Information Nondiscrimination Act of 2008 [39]

krebsrisiko des Patienten aus deren Familienkrankengeschichte abzuleiten. Nicht geschützt sind allerdings Geninformationen, welche das Geschlecht oder das Alter betreffen. Klar festzuhalten ist, dass dieses Gesetz explizit nicht für Lebens-, Berufsunfähigkeits- und Pflegeversicherungen gilt. Zusätzlich ist noch hervorzuheben, dass die einzelnen Bundesstaaten in den letzten Jahren einige Gesetze im Bereich des Datenschutzes für Geninformationen erlassen haben. Somit ergibt sich eine äußerst inhomogene Schutzlage für derartig sensible Daten innerhalb der gesamten USA. [133]

> „Das Schutzniveau variiert in den einzelnen Bundesstaaten jedoch erheblich. Außerdem weicht das Verständnis schutzwürdiger genetischer Informationen voneinander ab, denn der eine Bundesstaat schützt nur DNA und RNA, ein anderer erstreckt den Schutz auf Daten aus der Familiengeschichte und auf andere medizinische Informationen mit genetischer Relevanz. Nur etwa die Hälfte der Bundesstaaten gewährt Schutz gegen heimliche kommerzielle Gentests. Es existiert in den USA demnach ein Flickenteppich an gesetzlichen Schutzvorgaben zum Umgang mit genetischen Gesundheitsdaten.“ [134]

2.3.11 Kalifornien als Vorreiter

Kalifornien, speziell der Landstrich „Silicon Valley“, gelegen im südlichen Teil der „San Francisco Bay Area“, gilt als einer der bedeutensten Orte der Software- und Technologieindustrie. Hier sind Firmen wie Apple, Intel, Google, Facebook, Amazon, Oracle und viele mehr angesiedelt. Die Aufzählung liest sich ganz klar wie das „who-is-who“ dieser Branche. [135] [136] [137] Ausgerechnet dieser Bundesstaat übernimmt seit vielen Jahren die unangefochtene Vorreiterrolle im Bereich des rechtlich geregelten Datenschutzes. [138]

The Breach Notification Law

Bereits im Jahr 2003 führte Kalifornien das „Breach Notification Law“ [139] ein. Dieses Gesetz sieht seitdem vor, dass bei unerlaubter Veröffentlichung oder Diebstahl von personenbezogenen Kundendaten alle Betroffenen unverzüglich über diesen Vorfall zu informieren sind. Mittlerweile haben fast alle Bundesstaaten in diesem Bereich nachgezogen und ähnliche Gesetze erlassen. Zusätzlich gibt es bereits Bemühungen für ein entsprechendes Bundesgesetz. Eine Reform des „Breach Notification Law“ im Jahr 2014 hat das Gesetz zusätzlich dahingehend verschärft,

[133] Hardenberg: Individualisierte Medizin in den USA [49] (S. 621f)
[134] Hardenberg: Individualisierte Medizin in den USA [49] (S. 621f)
[135] Turner: Exhibition: Shots of Silicon Valley [123]
[136] Adams: Growing where you are planted: Exogenous firms and the seeding of Silicon Valley [1]
[137] Wonglimpiyarat: The dynamic economic engine at Silicon Valley and US Government programmes in financing innovations [135]
[138] Orthwein et al.: Kann Europa von Kalifornien Datenschutz lernen? [93] (S. 613)
[139] Breach Notification Law [14]

dass die Klarnamenpflicht als Erfüllungszweck gefallen ist. Demnach ist die Informationspflicht bereits dann gegeben, wenn lediglich ein gewähltes Pseudonym des Benutzers veröffentlicht wurde. Somit gelten auch rein virtuelle Identitäten als vollständig schutzbedürftig. [140] [141]

The Shine the Light Law

Ebenfalls im Jahr 2003 wurde das „Shine the Light Law“ [142] erlassen, welches 2005 in Kraft getreten ist. Seitdem ist es für alle Unternehmen, welche in Kalifornien Daten erheben, verpflichtend, bei der Erhebung und Weitergabe von Daten zu Werbezwecken den Benutzer ausreichend über diesen Umstand zu informieren. [143] Es muss aus der gewährten Information eindeutig hervorgehen, welche Daten zu welchen Zwecken erhoben und weitergegeben werden. Hervorzuheben ist, dass das Unternehmen selbst nicht in Kalifornien ansässig sein muss; es reicht aus, wenn Daten von Einwohnern Kaliforniens erhoben werden. Das Gesetz hat weiters 27 Datenkategorien festgestellt, welche unter die Definition der „personal information“ fallen; darunter klassische Kategorien wie „Name und Adresse“ oder die „Email Adresse“, aber auch ausgefallenere, wie etwa die „Kreditwürdigkeit des Kunden“. [144]

2.4 Analyse und Vergleich der Rechtsvorschriften

In diesem Kapitel sollen sowohl die Thematik des Datentransfers aus Europa in Drittstaaten behandelt - am Beispiel Österreich in die Vereinigten Staaten von Amerika - als auch die Vor- sowie Nachteile der divergenten Rechtslage im Bereich des Datenschutzes beleuchtet werden. Als letzter Punkt wird eine direkte Gegenüberstellung der wichtigsten Regelungen von Europa und den USA angestrebt.

2.4.1 Datentransfer in Drittstaaten

Wie bereits in Kapitel 2.1 festgestellt, ist die Übermittlung von personenbezogenen Daten aus Österreich in ein Land der Europäischen Union beziehungsweise des Europäischen Wirtschaftsraumes grundsätzlich genehmigungsfrei. Dies stellt Artikel 2, § 12 des österreichischen Datenschutzgesetz klar. Weiters ist in eben diesem Paragraphen die Erlaubnis zur Übermittlung erteilt, sofern das Zielland über einen angemessenen Datenschutz verfügt. [145] Die Grundlage dafür bildet Artikel 25, Absatz 1 der Datenschutzrichtlinie 95/46/EG [146] Dies wurde bereits in Kapitel 2.2.1 ausgiebig behandelt.

[140] Orthwein et al.: Kann Europa von Kalifornien Datenschutz lernen? [93] (S. 613f)
[141] Wagner: Das Safe-Harbor Modell; Datenschutzbestimmungen in der Relation EU-USA [128] (S. 31)
[142] Shine the Light Law [112]
[143] Orthwein et al.: Kann Europa von Kalifornien Datenschutz lernen? [93] (S. 613f)
[144] Shine the Light Law [112]
[145] Datenschutzgesetz [25] (S. 8f.)
[146] Datenschutzrichtlinie 95/46/EG [104] (S. Nr. L 281/45f)

Nachdem in den Vereinigten Staaten von Amerika aus europäischer Sicht, wie in Kapitel 2.3 dargelegt, kein angemessenes Datenschutzniveau vorhanden ist, müsste es konsequenterweise nicht erlaubt sein, in die USA personenbezogene Daten zu übermitteln. [147] Dies ist aber aufgrund des „Safe Harbor“ Abkommens doch möglich. Dieses Abkommen gewährleistet dem Betroffenen diverse Rechte. Jeder Betroffene muss über die Datenerhebung und den Zweck informiert werden; ferner, wer der Empfänger der Daten sein soll. Weiters hat jeder Betroffene das Recht auf Einsicht und Berichtigung der ihn betreffenden Daten. Zusätzlich wird ein Beschwerderecht bei der Federal Trade Commission (FTC) zugestanden. [148]

Es gibt allerdings einige sehr schwere Kritikpunkte an der „Safe Harbor“ Methodik. Es findet sich unter anderem eine Passage, welche suggeriert, dass zweckentfremdete Verwendung der erhobenen Daten den Regelfall darstellt und sich der Betroffene aktiv und selbstständig dafür einsetzen muss, diesem Umstand zu widersprechen. Ein viel größeres Problem stellt die vollständig fehlende Kontrolle seitens der FTC dar. Es sind bereits Fälle publik geworden, in denen sich Unternehmen mit dem „Safe Harbor“ Zertifikat geschmückt haben, welche sich selbst niemals zertifiziert haben. Aber selbst bei den offiziell angesuchten und zertifizierten Teilnehmern ist keinesfalls von einem garantierten Datenschutz auszugehen. Da „Safe Harbor“ auf einer Absichtserklärung und reiner Selbstkontrolle basiert und niemals von den Behörden weiter überprüft wird, kann eindeutig nicht von einem flächendeckend angemessenen Datenschutzniveau ausgegangen werden. Dementsprechend ist ein Transfer von personenbezogenen Daten in die USA eher sehr kritisch zu betrachten und tendenziell abzulehnen. [149]

> „Von dem Datenexport in die USA können sie trotz eines mit dem US-Außenministerium ausgehandelten „Safe-Harbor-Paket“ nur abraten.“ [150]

Eine mögliche Änderung dieser Situation wäre das Inkrafttreten der in Kapitel 2.2.2 behandelten Datenschutz-Grundverordnung [151]. Diese würde das Datenschutzrecht nicht nur für alle Staaten der Europäischen Union vereinheitlichen, sondern auch auf Unternehmen ausdehnen, welche keinen Sitz in der EU unterhalten, sofern die Datenerhebung bei einem Bürger der Union durchgeführt wird. Dies hätte eine deutliche Stärkung der Datenschutzrechte jedes EU-Bürgers zur Folge. Jedoch muss auch hier auf eine entsprechende Durchsetzbarkeit geachtet werden, damit dies nicht erneut zu einem zahnlosen Instrument verkommt. [152]

[147] Roßnagel et al.: Die Zulässigkeit der Übertragung personenbezogener Daten in die USA im Kontext der NSA-überwachung [107] (S. 547)
[148] Hammersen et al.: Datenübermittlung in Nicht-EU-Staaten: rechtliche Probleme [124] (S. 1)
[149] Hammersen et al.: Datenübermittlung in Nicht-EU-Staaten: rechtliche Probleme [124] (S. 2)
[150] Hammersen et al.: Datenübermittlung in Nicht-EU-Staaten: rechtliche Probleme [124] (S. 1)
[151] Datenschutz-Grundverordnung [126]
[152] Hammersen et al.: Datenübermittlung in Nicht-EU-Staaten: rechtliche Probleme [124] (S. 4)

> „Sollte die Datenschutz-Grundverordnung in Kraft treten, wäre damit insbesondere auch das mit den USA ausgehandelte Safe-Harbor-Abkommen obsolet. [...] Allerdings hilft auch das beste Gesetz nichts, wenn es nicht beachtet wird.“ [153]

2.4.2 Vorteile und Schwachstellen

In diesem Kapitel sollen die Vor- und Nachteile von strengem und schwachem Datenschutz beleuchtet und gegenübergestellt werden. Es zeigt sich nämlich, dass weder ein möglichst strenger noch ein möglichst schwacher Datenschutz das Ziel sein kann, da beide Extremata deutliche Nachteile aufweisen.

Ein nicht zu unterschätzender Problempunkt bei sehr starken Datenschutzregelungen ist die Einschränkung der Menschenwürde im Sinne der Beschneidung der Rede-, Meinungs- und Entfaltungsfreiheit. Sowohl im europäischen [154] [155] als auch im amerikanischen [156] [157] Rechtsverständnis ist man eben dieser Auffassung. Somit ist dies ein wichtiger und sehr ernst zu nehmender Balanceakt.

Der Vorteil und die teilweise Notwendigkeit eines strengen Datenschutzes für den einzelnen Bürger mag in erster Linie klar auf der Hand liegen [158] [159], leider wird oftmals die damit einhergehende Benachteiligung für die Wirtschaft vergessen. In weiterer Folge sollte man nicht außer Acht lassen, dass jeder einzelne Bürger doch in irgendeiner Weise auf die Wirtschaft angewiesen ist und somit eine schwer nachteilige Lage für Unternehmen doch wieder den Bürgern schadet. Dies soll keinesfalls bedeuten, dass ein Ausverkauf der persönlichen Daten jedes einzelnen stattfinden darf. Es soll lediglich unterstrichen werden, dass auch hier Ausgeglichenheit gefordert ist, die keine der beiden Seiten zu stark einschränkt oder benachteiligt. Man darf nämlich nicht unterschätzen, wie handels- und dienstleistungsschädlich ein zu strenger Datenschutz durchaus auch sein kann. [160] Bedenkt man zum Beispiel die Unmöglichkeit für Unternehmen, interne Informationen über ihre eigenen Mitarbeiter, sei es nur ein Adressbuch, über Landesgrenzen hinweg auszutauschen: Hier ist klar zu unterscheiden, in welche Länder diese Daten übertragen werden. Gelten diese nämlich als nicht sichere Drittländer außerhalb der EU, ist die Übermittlung - wenn überhaupt - nur unter sehr strengen Auflagen erlaubt, selbst dann, wenn die Daten den Konzern niemals verlassen. [161] Ähnliche Probleme ergeben sich bei - im Besonderen kommerzieller - Verwendung von „Cloud-Services“. Das Speichern von Daten in einem „Cloud-

[153] Hammersen et al.: Datenübermittlung in Nicht-EU-Staaten: rechtliche Probleme [124] (S. 4)
[154] siehe Kapitel 2.2.2
[155] Giesen: Für ein verfassungsgemäßes Datenschutzrecht in Europa: Wann beginnt die EU, sich auf ihre freiheitlichen Prinzipien zu besinnen? [40] (S. 551)
[156] siehe Kapitel 2.3.1
[157] Spies et al.: Microsoft als Initialzünder für mehr Datenschutz in den USA? [113] (S. 171)
[158] siehe Kapitel 2.3.1
[159] Spies et al.: Microsoft als Initialzünder für mehr Datenschutz in den USA? [113] (S. 171)
[160] Weichert: Freihandelsabkommen contra Datenschutz? [132] (S. 850)
[161] Götz: Grenzüberschreitende Datenübermittlung im Konzern [47] (S. 631ff)

Service“ bringt für Unternehmen sehr viele - speziell finanzielle - Vorteile mit sich. Allerdings sind die damit verbundenen Datenschutzrisiken erheblich. [162]

Ein uneinheitlicher Datenschutz ist sowohl für Bürger als auch für Unternehmen ein Hindernis. Sowohl innerhalb Europas als auch im internationalen Aspekt besteht derzeit noch kein allgemein gültiges Datenschutzrecht.
Wie in Kapitel 2.2 erfasst, besteht das Datenschutzrecht in Europa derzeit aus pro Land eigenständigen nationalen Gesetzen, welche als Grundlage die Datenschutzrichtlinie 95/46/EG [163] haben. Dies hat den Effekt, dass sich die Datenschutzrechte und -pflichten sowohl für Bürger als auch die Wirtschaft in ihren Ausprägungen pro Land durchaus unterscheiden können. Dies ergibt für beide Seiten eine gewisse Rechtsunsicherheit, mit der nur sehr schwer umgegangen werden kann.
Ein noch deutlich verschärfteres Bild stellt sich in den Vereinigten Staaten von Amerika dar. Wie in Kapitel 2.3 beschrieben, existieren in den USA kaum bundesweite Gesetze, sondern großteils bundesstaatliche Einzelgesetzgebungen. Zusätzlich herrscht in den Vereinigten Staaten die Ansicht, dass Datenschutz der Selbstkontrolle und Eigenständigkeit der Bevölkerung zu überantworten ist.
Daher ist es auch nicht weiter verwunderlich, dass sich die Datenschutzanforderungen der EU und USA nur schwer auf einen Nenner bringen lassen. Dies ist ganz klar ein wirtschaftliches Hindernis für beide Seiten. [164]

> „Generell muss festgestellt werden, dass das Datenschutzniveau in den USA nicht ansatzweise den deutschen und europäischen verfassungsrechtlichen Anforderungen genügt und daher ein berechtigtes Handelshemmnis darstellen kann.“ [165]

Eine undifferenzierte Überregulierung ist ebenfalls ein Problem, welches dem Bürger vermutlich erst bei persönlicher Betroffenheit bewusst werden dürfte. Wie in Kapitel 2.2 beschrieben, ist die derzeitige europäische Situation weitgehend undifferenziert. Somit hat zum Beispiel ein KFZ-Mechaniker, welcher eine digitale Kundenkartei führt, die exakt gleichen Rechte und Pflichten in Bezug auf den Datenschutz wie beispielsweise Facebook, ein multinationaler Konzern, welcher das wirtschaftliche Ziel hat, so viele persönliche Daten wie möglich zu sammeln, um ein maximal genaues Profil jeder Person zu erstellen und dieses effektiv für spezialisierte Werbung zu verwenden. Eine bessere Differenzierung und mehr Fingerspitzengefühl in der Ausgestaltung der Datenschutzgesetze wäre hier vermutlich von Vorteil. [166]

Die Verwendung von BigData, also die statistische Auswertung von einer sehr großen Menge an Daten, bringt nicht nur im Bereich des Straßenverkehrs wesentliche Vorteile. Auch in der

[162] Geis: Datenschutzrecht in der internationalen Netzgesellschaft [38] (S. 3)
[163] Datenschutzrichtlinie 95/46/EG [104]
[164] Weichert: Freihandelsabkommen contra Datenschutz? [132] (S. 850f)
[165] Weichert: Freihandelsabkommen contra Datenschutz? [132] (S. 851)
[166] o.A.: Ein neues Datenschutzrecht für Europa [88] (S. 3)

Medizin und Gesundheitsvorsorge können massive Wissenszuwächse und Erkenntnisse erwartet werden. Da aber medizinische Daten rein prinzipiell als sensible Daten der höchsten Schutzwürdigkeitsstufe angehören, ist dies ein überaus heikles Thema. [167] Hinzu kommt noch, dass eine Vielzahl der Daten aufgrund ihrer Individualität überwiegend auf die Einzelperson rückführbar sind. Im Speziellen sind Gendaten in der Regel immer auf das Individuum zurückführbar, aber ausgerechnet diese Daten haben aus wissenschaftlicher Sicht den größten Nutzen und versprechen den höchsten Erkenntnisgrad. Aussagen, die für ganze ethnische Gruppen gelten können, sind durchaus vorstellbar. [168]

> „Es geht um die Optimierung des Einsatzes von Personal, Krankenhausbetten und sonstigen Behandlungsressourcen, um Patientenflusssteuerung und Qualitätssicherung, um die Vermeidung von Nebenwirkungen bei Arzneimitteln, um individuelle und kollektive Risikoscreenings, um die Behandlungsunterstützung in den unterschiedlichsten Ausgestaltungen bis hin zur personalisierten Medizin durch auf die individuelle Disposition des Patienten angepasste Präventions- oder Behandlungsmethoden.“ [169]

Ein wesentliches Risiko von BigData ist allerdings die Datenschutzkonformität bei Verwendung dieser Daten, da oftmals eine einfache Pseudonymisierung keinesfalls ausreicht, um eine Reidentifizierbarkeit ernsthaft zu unterbinden. [170]

> „Eine Pseudonymisierung von einzelnen Personen zuordenbaren Datensätzen genügt für den Ausschluss einer Reidentifizierung regelmäßig nicht, insbesondere wenn die Pseudonyme längerfristig zur Zuordnung von Individualdatensätzen genutzt werden. [...] Eine Reidentifizierbarkeit entsteht schon dadurch, dass die ursprünglichen Stammdaten gemäß dem Pseudonymisierungsverfahren verändert werden und die pseudonymisierten Daten mit den angeblich anonymisierten Daten abgeglichen werden können. Derart ergibt sich eine direkte Zuordnung dieser Daten zu den Stammdaten. [...] Je detaillierter und umfangreicher ein Datensatz ist, umso leichter kann er mit Zusatzwissen wieder Individuen zugeordnet werden.“ [171]

2.4.3 Direkte Gegenüberstellung

Dieses Kapitel wird eine direkte Gegenüberstellung der Rechtslage der Europäischen Union und der Vereinigten Staaten von Amerika in Form einer Tabelle beinhalten, um eine schnelle Übersicht der primären Unterschiede zu bieten.

[167] Weichert: Big Data, Gesundheit und der Datenschutz [131] (S. 831f)
[168] Weichert: Big Data, Gesundheit und der Datenschutz [131] (S. 832)
[169] Weichert: Big Data, Gesundheit und der Datenschutz [131] (S. 834)
[170] Weichert: Big Data, Gesundheit und der Datenschutz [131] (S. 836)
[171] Weichert: Big Data, Gesundheit und der Datenschutz [131] (S. 836)

Tabelle 2.1: Direkte Gegenüberstellung der Rechtslage

	Europa	**USA**
Einheitliche Grundlage	JA Durch die Datenschutzrichtlinie 95/46/EG [172] ist in Europa eine einheitliche Grundlage vorhanden. [173]	NEIN Allgemein keine einheitliche Grundlage. Einzige Ausnahme ist der „Children's Online Privacy Protection Act of 1998" [174], welcher allerdings nur für Kinder unter 13 Jahren gilt. [175] [176]
Einzelne Ausprägung pro Land	JA Jedes Land der EU hat eigene Art der Umsetzung der DSRL und ebenso eigene „Spezialgesetze". [177]	JA Jeder Bundesstaat hat nach amerikanischem Denken eine große Eigenverantwortung in der Gesetzgebung und somit auch bei dem Thema Datenschutz. [178]
Aussicht auf Vereinheitlichung	JA Durch die Datenschutz-Grundverordnung [179] kann in absehbarer Zeit eine einheitliche Rechtslage für die gesamte EU entstehen. [180]	JA/NEIN Konkret gibt es keine bundesweiten offiziellen Bemühungen einer Vereinheitlichung, aber Kalifornien spielt als Vorreiter eine große Rolle. [181] Auch aus der Wirtschaft wird der Druck für einheitlichen Datenschutz größer. [182] [183]

Tabelle 2.1 - *Fortsetzung auf der nächsten Seite*

[172] Datenschutzrichtlinie 95/46/EG [104]
[173] siehe Kapitel 2.2.1
[174] Children's Online Privacy Protection Act of 1998 [23]
[175] siehe Kapitel 2.3.8
[176] siehe Kapitel 2.3
[177] siehe Kapitel 2.2.2
[178] siehe Kapitel 2.3
[179] Datenschutz-Grundverordnung [126]
[180] siehe Kapitel 2.2.2
[181] siehe Kapitel 2.3.11
[182] Spies et al.: Microsoft als Initialzünder für mehr Datenschutz in den USA? [113] (S. 171)
[183] siehe Kapitel 2.3

Tabelle 2.1 - *Fortsetzung der vorherigen Seite*

	Europa	**USA**
Datenschutzniveau	MITTEL/HOCH Bereits jetzt herrscht ein hoher Grad der Regelung durch die DSRL [184] und die einzelnen nationalen Gesetze. Diese nationalen Gesetze ergeben natürlich zwangsläufig eine leichte Diskrepanz zwischen den Datenschutzniveaus. [185] [186]	NIEDRIG/MITTEL Durch die Eigenverantwortung und die grundsätzlich abweichende Einstellung zum Thema Datenschutz herrscht in den USA aktuell überwiegend ein relativ geringer Datenschutz. [187]
Behinderung der Wirtschaft	MITTEL/HOCH Die starke und ausgeprägte Regulierung ist sowohl für inländische als auch Unternehmen aus Drittländern ein Hindernis für deren Entfaltung. Speziell die Undifferenziertheit kann kleinere Betriebe vor erhebliche Schwierigkeiten stellen. [188]	NIEDRIG Die moderaten Datenschutzbestimmungen, welche sich primär auf einzelne Bundesstaaten und/oder scharf begrenzte Teilbereiche beschränken, führen zu einer schwachen Behinderung der Wirtschaft. [189]

Tabelle 2.1 - *Fortsetzung auf der nächsten Seite*

[184] Datenschutzrichtlinie 95/46/EG [104]
[185] siehe Kapitel 2.1
[186] siehe Kapitel 2.2
[187] siehe Kapitel 2.3
[188] siehe Kapitel 2.4.2
[189] siehe Kapitel 2.3

Tabelle 2.1 - *Fortsetzung der vorherigen Seite*

	Europa	**USA**
Selbstbestimmung der Bürger	HOCH Die Selbstbestimmungsmöglichkeiten der Bürger innerhalb der EU sind im Bereich des Datenschutzes als relativ hoch anzusehen, da die Gesetze durch das generelle Verbot mit Erlaubnisvorbehalt ein relativ hohes Maß an Schutz für die Daten der Bürger festlegt und somit die Selbstbestimmungsmöglichkeiten stärkt. Der Ausrichtungsschwerpunkt liegt klar beim Schutz der Daten von Bürger. [190]	NIEDRIG Das gesamte amerikanische Recht ist auf dem Gedanken der Selbstbestimmung und Selbstregulierung aufgebaut. So auch im Bereich des Datenschutzes. Dementsprechend kommt auch der Wirtschaft ein hohes Maß an Selbstbestimmung zu, welches die Möglichkeiten der Bürger allerdings beschneidet. Der Schwerpunkt der Gesetzgebung liegt in diesem Fall auf der freien Marktwirtschaft und einer Stärkung dieser indem Unternehmen ein hohes Maß an Freiheiten eingeräumt wird. [191]
Risiko durch Fehleinschätzung der Bürger	NIEDRIG Da strenge Regelungen vorhanden sind, wird die Gefahr eines ungewollten Daten- bzw. Kontrollverlustes zumindest in der Theorie relativ gering gehalten. Selbst bei Unkenntnis der Materie oder Fehleinschätzung des Risikos ist das Gefahrenpotenzial per se eher gering einzuschätzen, wobei allerdings die internationale Vernetzung und die Wirtschaftspraxis sowie die zunehmend aggressivere Onlinekriminalität dies konterkarieren. [192]	HOCH Durch die schwachen beziehungsweise geringen Reglementierungen und das hohe Maß an Eigenverantwortung der Bürger in Kombination mit der sehr komplexen und undurchsichtigen Materie der Datenverarbeitung und Informationstechnologie ist das Risiko eines ungewollten Datenverlustes hoch. Erschwerend kommt die unbeschwerte Einstellung der amerikanischen Bevölkerung zur Verarbeitung persönlicher Daten hinzu. [193]

Tabelle 2.1 - *Fortsetzung auf der nächsten Seite*

[190] siehe Kapitel 2.2
[191] siehe Kapitel 2.3
[192] siehe Kapitel 2.2
[193] siehe Kapitel 2.3

Tabelle 2.1 - *Fortsetzung der vorherigen Seite*

	Europa	**USA**
Attraktivität für Unternehmen aus Drittländern	NIEDRIG/MITTEL Die nicht vollständig einheitliche Rechtslage innerhalb der EU und die relativ strengen Datenschutzauflagen machen den Standort Europa zunehmend unattraktiv für Unternehmen aus Drittländern. Einerseits müssen Unternehmen aus den USA deutlich höhere Anforderungen erfüllen als in ihrem Heimatland, andererseits müssen sie sich pro Land neuen Gesetzen und juristischen Feinheiten unterwerfen. Zumindest teilweise könnte sich diese Lage in absehbarer Zukunft mit der einheitlichen Datenschutz-Grundverordnung [194] verbessern. [195] [196]	MITTEL/HOCH Schwache Vorschriften machen die USA zwar für Unternehmen aus Drittländern sicherlich attraktiv, allerdings ist durch die juristische Eigenverantwortung der Bundesstaaten kein einheitliches rechtliches Feld innerhalb der Vereinigten Staaten gegeben. Dies ist für die kommerzielle Optimierung von Geschäftsprozessen keinesfalls förderlich. Durch aktuelle rechtliche Bestrebungen des Bundesstaates Kalifornien [197] und auch einzelner großer Konzerne [198] könnte sich diese Lage aber in einigen Jahren bessern. [199] [200]

2.4.4 Leitfaden für Unternehmen

Für Unternehmen ist die Erhebung und Verarbeitung von personenbezogenen Daten kein triviales Thema. Dies bedeutet aber nicht, dass es eine rechtliche Unmöglichkeit darstellen muss. In diesem Kapitel sollen ein paar Leitlinien und Eckpunkte sowie Tipps zur sicheren Verarbeitung von datenschutzrelevanten Inhalten erörtert werden.

Die Übermittlung der Daten innerhalb der EU ist rechtlich unproblematisch, ebenso wie die Übermittlung in von der EU festgestellte „sichere“ Länder, deren Datenschutzvorschriften den europäischen ausreichend gleichkommen. [201] Sofern die Übermittlung in Drittländer also nicht

[194] Datenschutz-Grundverordnung [126]
[195] siehe Kapitel 2.2
[196] siehe Kapitel 2.4.2
[197] siehe Kapitel 2.3.11
[198] Spies et al.: Microsoft als Initialzünder für mehr Datenschutz in den USA? [113]
[199] siehe Kapitel 2.3
[200] siehe Kapitel 2.4.2
[201] siehe Kapitel 2.4.1

notwendig ist, stellt sich für das Unternehmen keine weitere zusätzliche Herausforderung, als die innerhalb der EU geltenden Vorschriften zu beachten. Sofern ein Datentransfer in ein Drittland unumgänglich ist, dazu zählen auch Datentransfers in Drittstaaten innerhalb eines Konzerns [202], sind spezielle Vorkehrungen zu treffen.

Zwei brauchbare Lösungen scheinen einerseits die „EU-Standardvertragsklauseln“ und andererseits die „Binding Corporate Rules (BCR)“. [203]
Die Standardvertragsklauseln sind ein festgesetztes Regelwerk der EU-Kommission, welchem sich ein Datenexporteur sowie ein Datenimporteur unterwerfen kann. Diese Klauseln liegen in drei Varianten vor und unterscheiden sich teilweise maßgeblich in der Haftungsfrage bei Verstößen. [204] Somit gewährleistet eine Aufnahme, Durchführung und Einhaltung dieser Klauseln in geschäftliche Verträge sowohl die Datenschutzkonformität für den Verbraucher als auch die Rechtssicherheit für die Unternehmen, unabhängig von deren Herkunftsländern und den dort gültigen Datenschutzgesetzen. [205]
Die BCR sind verbindliche Unternehmensrichtlinien, welche einen sicheren Umgang mit personenbezogenen Daten garantieren sollen, selbst wenn die staatlichen Rechtsvorschriften des Konzerns einen derartigen nicht erfordern würden. Mit den BCR erlegt sich ein Konzern, auch landesgrenzenübergreifend, selbst die Verpflichtung eines ausreichenden Datenschutzes auf. Dieser muss natürlich dem Datenschutzniveau der Datenschutzrichtlinie 95/46/EG [206] entsprechen. [207]

Die Nutzung von „Cloud-Services“ zum Speichern, Teilen und Verteilen von Daten ist nicht nur für Privatpersonen verlockend. Das durchgehende Verfügbarmachen von E-Mails, Kalendern, Adressbüchern, Dokumenten und mehr - unabhängig vom Standort und Endgerät - und die gleichzeitige vollständige Sicherheit, keine Daten zu verlieren, da die Speicherzentren gegen nahezu jegliche Art von Datenverlust mehrfach abgesichert sind, klingt auch für Unternehmen sehr vielversprechend. Allerdings können sich gerade kleinere und mittlere Betriebe die Anschaffung und Instandhaltung einer solchen Cloud kaum leisten. Abhilfe versprechen hier Unternehmen, welche auf genau diesen Zweck ausgerichtet sind. Dies soll eine Einsparung von bis zu 20 Prozent ermöglichen. [208]
Problematisch wird die Situation dann, wenn die Anbieter die Daten nicht ausschließlich innerhalb der EU speichern. Laut europäischen Vorschriften muss der Auftraggeber, in diesem Fall der Kunde des Cloud-Anbieters, dafür sorgen, dass die Daten nach geltendem EU-Recht gesichert sind. Dies ist ihm natürlich schon allein aufgrund der Komplexität der Datenspeicherung

[202] Götz: Grenzüberschreitende Datenübermittlung im Konzern [47] (S. 634ff)
[203] Grapentin: Haftung und anwendbares Recht im internationalen Datenverkehr: EU-Standardvertragsklauseln und Binding Corporate Rules [45] (S. 102)
[204] Grapentin: Haftung und anwendbares Recht im internationalen Datenverkehr: EU-Standardvertragsklauseln und Binding Corporate Rules [45] (S. 102ff)
[205] Graf: Datenschutzrecht im Überblick [44] (S. 22f)
[206] Datenschutzrichtlinie 95/46/EG [104]
[207] Voskamp et al.: Grenzüberschreitende Datenschutzregulierung im Pazifik-Raum [127] (S. 455)
[208] o.A.: Datenschutzrecht: Neue Leitlinien für EU-Unternehmen bei der Nutzung der Cloud [87]

nicht möglich, und es droht ein Kontrollverlust bezüglich der Daten. [209] [210] Ein nicht zu unterschätzendes Problem ist bei Nutzung amerikanischer Cloud-Anbieter die Herausgabepflicht der Daten gegenüber den dortigen Behörden. Dies widerspricht dem in Europa geltenden Datenschutzrecht teilweise erheblich. [211] [212]
Die EU-Kommission war in diesem Bereich aber keineswegs untätig. So hat sie bereits Leitlinien für Unternehmen erstellt, welche die Benutzung von Cloud-Services unterstützen und auch reglementieren sollen. Diese Leitlinien stellen unter anderem erste Versuche von standardisierten Leistungsvereinbarungen seitens der Anbieter dar. Somit soll eine einfachere und sicherere Verwendung von Cloud-Services ermöglicht werden. [213]
Auch im Bereich der Angriffsabwehr bei Cloud-Services gibt es Vorteile. So liegt das Ziel der Angriffsabwehr nach außen klar auf der Hand, betreffend Angriffe innerhalb der Unternehmensstrukturen jedoch nicht. Bei vielen Anbietern werden Daten im Klartext auf den Servern gespeichert; somit könnte jeder Mitarbeiter mit ausreichender Zugriffsberechtigung die Daten jedes Kunden mitlesen. Das Fraunhofer AISEC in München hat hier den Entwurf einer „Sealed Cloud“ erarbeitet. In dieser Form der Cloud soll es auch internen Mitarbeitern nicht mehr möglich sein, jedwede Daten auszulesen, zu editieren oder zu löschen. [214] Mit genau diesem Gedanken an verbesserte Datensicherheit drängen bereits die ersten Unternehmen auf den Markt, welche eine Ende-zu-Ende-Verschlüsselung in der Cloud anbieten. [215]
Bei der Nutzung von Cloud-Services ist also zu erhöhter Vorsicht und Achtsamkeit geraten, insbesondere bei Unternehmen, welche eine nicht europäische Herkunft vermuten lassen. [216]

> „In der Cloud von US-Anbietern verschärfen sich diese Probleme. Mit dem Cloud-Anbieter muss vereinbart werden, ein dem europäischen Datenschutz vergleichbares Schutzniveau zu gewährleisten. Ein entscheidendes Rechtsproblem entzieht sich vertraglichen Regeln: der Zugriff der US-Sicherheitsbehörden auf die in der Cloud archivierten Dokumente.“ [217]

Für die Entwicklung von Smartphone-Apps sind ebenfalls einige Regeln einzuhalten. Einerseits sollten die Datenschutzbestimmungen, welche klar verständlich aufklären müssen, welche Daten zu welchem Zweck erhoben werden und was mit diesen in weiterer Folge passiert, für jeden Kunden leicht auffindbar sein. [218] Andererseits muss sich die App in weiterer Folge auch an diese Bestimmungen „halten“. Dies kann selbst für die Entwickler manchmal nicht ganz leicht zu erkennen sein. Beispielsweise können Werbeeinblendungen von Drittanbietern, welche in der

[209] o.A.: Ein neues Datenschutzrecht für Europa [88] (S. 4)
[210] Geis: Datenschutzrecht in der internationalen Netzgesellschaft [38] (S. 1f)
[211] Geis: Datenschutzrecht in der internationalen Netzgesellschaft [38] (S. 2)
[212] Hansen: Datenschutz nach dem Summer of Snowden [48] (S. 439f)
[213] o.A.: Datenschutzrecht: Neue Leitlinien für EU-Unternehmen bei der Nutzung der Cloud [87]
[214] o.A.: Sealed Cloud schließt IT-Sicherheitslücke „Mensch“ [91]
[215] Wyllie: Tresorit – Cloud Storage mit Ende-zu-Ende-Verschlüsselung [136]
[216] Geis: Datenschutzrecht in der internationalen Netzgesellschaft [38] (S. 3)
[217] Geis: Datenschutzrecht in der internationalen Netzgesellschaft [38] (S. 3)
[218] Bodden et al.: Schutzmaßnahmen gegen datenschutz-unfreundliche Smartphone-Apps [12] (S. 723f)

Regel zur Finanzierung einer App dienen, selbst Daten erheben und somit einen Verstoß gegen die Datenschutzbestimmungen verursachen. [219] [220] [221] [222] Auch ist es wichtig, dass der Anbieter einer Smartphone-App die Möglichkeit des Widerrufs der Nutzung der personenbezogenen Daten ausreichend berücksichtigt. Die reine Deinstallation der App durch den Kunden reicht hier keinesfalls aus, da das europäische Datenschutzrecht auch den Widerruf der Verwendung bereits erhobener Daten vorsieht. Für diesen Fall muss der Entwickler entsprechend Vorkehrungen treffen, um darauf rechtlich ausreichend reagieren zu können. [223] Interessant wird die Lage, wenn die Daten nicht direkt auf dem Endgerät des Benutzers erhoben werden, sondern auf einem Server, dessen Standort außerhalb Europas liegt, gespeichert werden. Demnach wären nämlich die Datenschutzbestimmungen des Server-Standort-Landes gültig, da keine Datenerhebung im Inland stattfindet. [224]

> „Das Verhalten von Apps kann gegen datenschutzrechtliche Vorgaben verstoßen. Die Rechtfertigung durch Einräumung von Berechtigungen wird in der Regel unwirksam sein, da meist gegen die Regeln der datenschutzrechtlichen Einwilligung verstoßen wird.“ [225]

[219] Bodden et al.: Schutzmaßnahmen gegen datenschutz-unfreundliche Smartphone-Apps [12] (S. 720)
[220] Heider: Die Gretchenfrage: Wie halten Sie’s mit der App-Sicherheit? [52] (S. 16)
[221] o.A.: Leitfaden für mehr App-Sicherheit im Geschäftsumfeld [89]
[222] o.A.: LG Frankfurt: Unzulässigkeit von App-Store-AGB [90]
[223] Bodden et al.: Schutzmaßnahmen gegen datenschutz-unfreundliche Smartphone-Apps [12] (S. 724)
[224] Bodden et al.: Schutzmaßnahmen gegen datenschutz-unfreundliche Smartphone-Apps [12] (S. 725)
[225] Bodden et al.: Schutzmaßnahmen gegen datenschutz-unfreundliche Smartphone-Apps [12] (S. 725)

KAPITEL 3

Technologische Entwicklung

In diesem Kapitel soll der aktuelle technologische Fortschritt kurz beleuchtet werden. Dies umfasst das Aufkommen der Smartphones und Tablets sowie der mobilen Anwendungen, welche „Apps“ genannt werden. Als Letztes werden noch die sogenannten „Wearable Devices“ besprochen. Dies sind Geräte, welche - im besten Fall unbemerkt - am Körper getragen werden können und den Träger mit Informationen über sich und/oder seine Umwelt versorgen.

3.1 Smartphones und Tablets

Smartphones, wörtlich „intelligente Telefone“, stellen eine Kombination aus einem mobilen Telefon, einem digitalen Assistenten, einem Media Player und einem Navigationsgerät dar. Sie verbinden somit viele Geräte in einem und bieten eine Fülle an Funktionen. Endgeräte mit mehr oder weniger diesen Charakteristika gab es schon im Jahr 1992, hergestellt von IBM. Es versuchten sich viele Firmen daran, diese Branche für sich zu erobern - großteils mit mäßigem Erfolg. [1] [2] Lediglich Research In Motion Limited (RIM), heute unter dem Namen BlackBerry Limited bekannt, konnte einige Zeit - wenn auch nur im Geschäftskundenkreis - einige Erfolge erzielen. [3]

Firma Apple Inc. ist es letzten Endes im Jahr 2007 gelungen, ein Gerät zu fertigen, welches die Massen begeisterte. [4] Es hatte bereits in seiner ersten Version ein 18-bit LCD Multi-Touch-Display, einen drei Achsen Beschleunigungssensor, Annäherungssensor, Umgebungslichtsensor und natürlich Bluetooth, USB sowie WLAN. Abgerundet wurde das Gerät mit seinem ganz auf Berührung optimierten Betriebssystem und dem integrierten App Store. Dies war dahingehend eine Neuheit, da der Großteil der bisher entwickelten Smartphones auf die Eingabe mit speziellen Stiften ausgelegt waren. Der App Store hatte zusätzlich den Vorteil, dass einerseits das Gerät

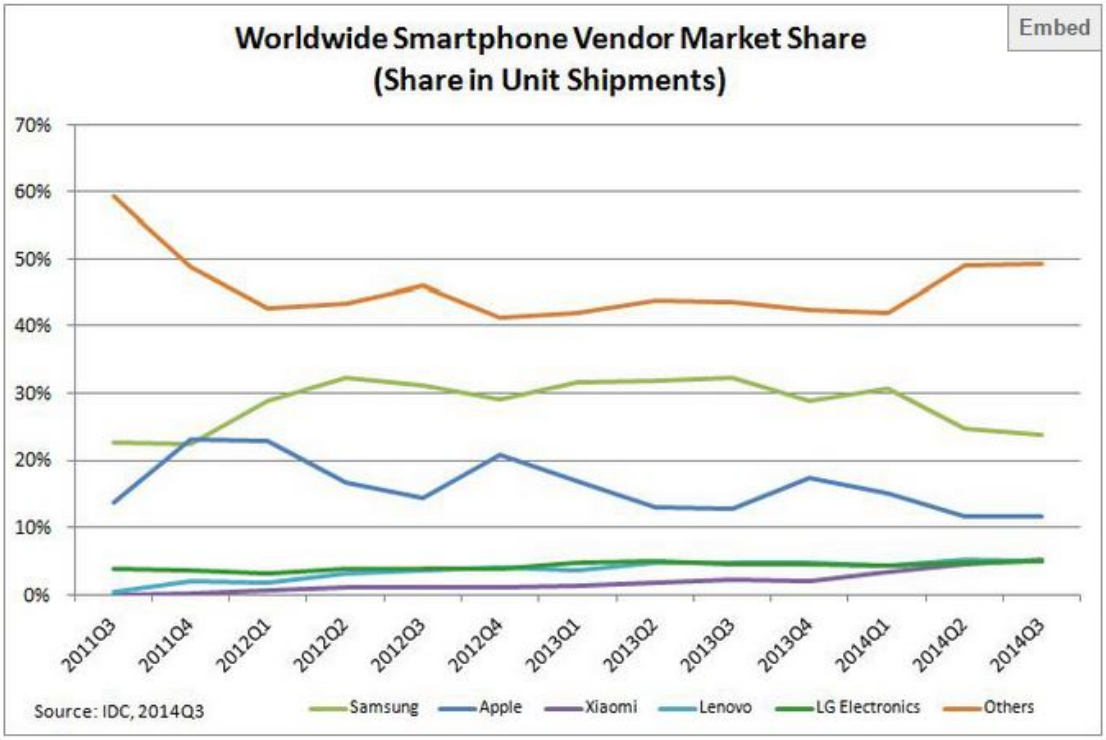
[1] ITWissen: Smartphone [69]
[2] Martin: The evolution of the smartphone [81]
[3] ITWissen: BlackBerry [60]
[4] Martin: The evolution of the smartphone [81]

jederzeit um beinahe beliebige Funktionen erweitert werden konnte und zusätzlich plötzlich jeder Entwickler weltweit die Möglichkeit hatte, ein Programm für sich selbst oder die ganze Welt für das Smartphone zu entwickeln. [5] [6]

Kurz darauf starteten auch alle anderen - erfahrenen sowie unerfahrenen - Hersteller die Produktion ähnlicher Geräte. Da das Betriebssystems des iPhones, welches iOS [7] genannt wird, durch seine einfache Bedienbarkeit [8] ein zwingendes Verkaufsargument darstellt und Apple dieses aber nicht zum Kauf oder Lizenzierung anbot, musste die Konkurrenz reagieren. Die Entscheidung fiel auf das ursprünglich von Andy Rubin, Rich Miner, Nick Sears und Chris White entwickelte System Android, und nur ein Jahr nach Vorstellung des iPhone war das erste Gerät mit Android erhältlich. Bereits im Jahr 2005 wurde Android Inc. von Google Inc. gekauft und in den Konzern integriert. [9] [10] [11] Den großen Unterschied bilden hier die beiden Herangehensweisen der Firmen. Apple betreibt sowohl die Entwicklung des Betriebssystems als auch des Gerätes selbst, wohingegen bei der Konkurrenz die Geräte von Hardware-Herstellern stammen, welche das Betriebssystem Android frei installieren dürfen, da es unter einer Open Source Lizenz veröffentlicht wird. [12]

Der erfolgreichste Gerätehersteller ist, gemessen an den Verkaufszahlen, eindeutig Samsung Electronics Co. Ltd. [13] [14] mit knapp 24 Prozent Marktanteil im dritten Quartal 2014. Dies entspricht beinahe dem Doppelten des zweitplatzierten Apple, welcher auf knapp 12 Prozent Marktanteil kommt. [15] Im Bereich der mobilen Betriebssysteme dominiert seit 2010 Android den Markt maßgeblich. Im dritten Quartal 2014 konnte Android einen Marktanteil von unglaublichen 84,4 Prozent verbuchen, wobei Apples iOS lediglich 11,7 Prozent schafft. [16] Dies ist allerdings auch auf den Erfolg von Samsung, welches beinahe ausschließlich Android als Betriebssystem verwendet, zurückzuführen. [17]

[5] ITWissen: iPhone [66]
[6] GSMArena: iPhone [46]
[7] ITWissen: iOS [64]
[8] Martin: The evolution of the smartphone [81]
[9] ITWissen: Android [59]
[10] Amadeo: The history of Android [3]
[11] Elgin: Google Buys Android for Its Mobile Arsenal [30]
[12] Martin: The evolution of the smartphone [81]
[13] Samsung Electronics Co. Ltd. [109]
[14] Reuters: Samsung Electronics Co. Ltd. [102]
[15] siehe Abbildung 3.1
[16] siehe Abbildung 3.3
[17] IDC: Smartphone Market Share [57]0



Period	Samsung	Apple	Xiaomi	Lenovo	LG	Others
Q3 2014	23.7%	11.7%	5.2%	5.1%	5.0%	49.3%
Q3 2013	32.2%	12.8%	2.1%	4.7%	4.6%	43.6%
Q3 2012	31.2%	14.4%	1.0%	3.7%	3.7%	46.0%
Q3 2011	22.7%	13.8%	-	0.4%	3.7%	59.4%

Source: IDC, 2014 Q3

Abbildung 3.1: Smartphone Marktanteile nach Herstellern
IDC: Smartphone Market Share [57]

Top Five Tablet Vendors, Shipments, and Market Share, Second Quarter 2014 (Preliminary Results, Shipments in millions)

Vendor	2Q14 Unit Shipments	2Q14 Market Share	2Q13 Unit Shipments	2Q13 Market Share	Year-over-Year Growth
1. Apple	13.3	26.9%	14.6	33.0%	-9.3%
2. Samsung	8.5	17.2%	8.4	18.8%	1.6%
3. Lenovo	2.4	4.9%	1.5	3.3%	64.7%
4. ASUS	2.3	4.6%	2.0	4.5%	13.1%
5. Acer Group	1.0	2.0%	1.5	3.4%	-36.3%
Others	21.9	44.4%	16.4	37.0%	33.4%
Total	**49.3**	**100.0%**	**44.4**	**100.0%**	**11.0%**

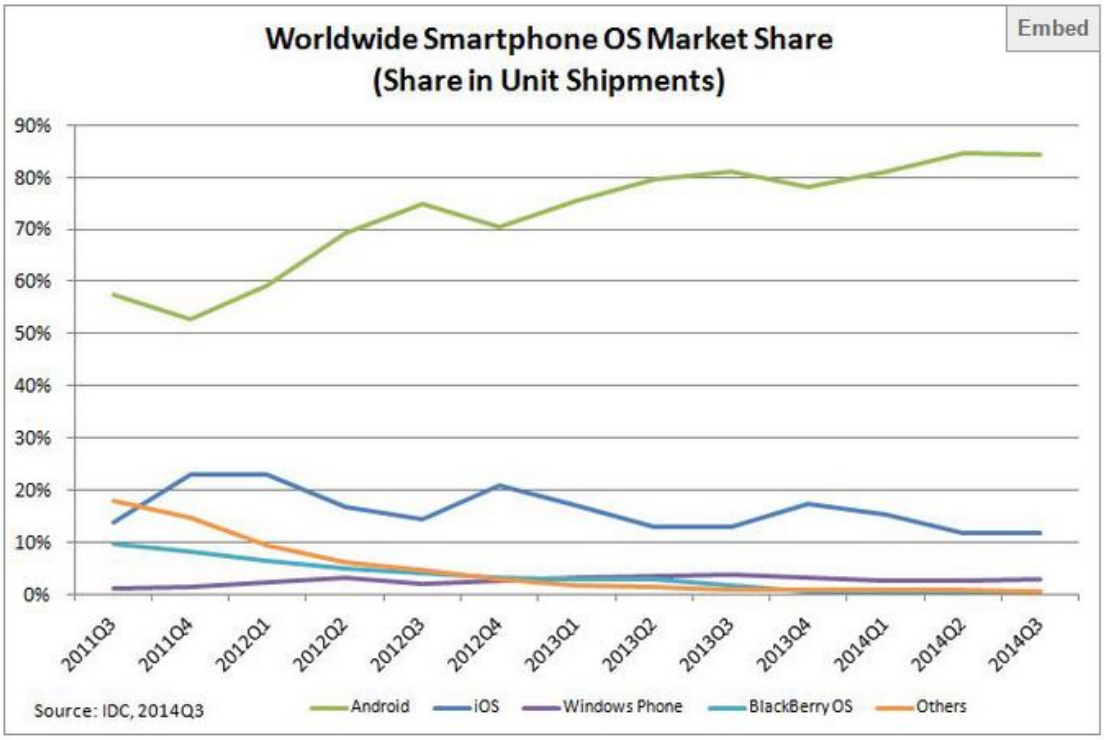
Abbildung 3.2: Tablet Marktanteile nach Herstellern
IDC: Tablet Market Share [58]

Neben den beiden bereits erwähnten gibt es noch einige weitere mobile Betriebssysteme, wie zum Beispiel Windows Phone [18] von Microsoft Corp. [19] [20]. Diese haben allerdings einen relativ geringen Verbreitungsgrad. [21]

Auch den zweiten großen technologischen Massenmarkt der letzten Jahre hat erneut Apple mit seinem iPad im Jahr 2010 eröffnet. [22] Ähnlich wie bei der Geschichte des Smartphones gab es auch vor dem Produkt von Apple bereits sogenannte Tablet Computer, kurz Tablets; allerdings schafften diese nie den richtigen Durchbruch im Massenverkauf. Dies ist auch darauf zurückzuführen, dass die Geräte davor eher auf Spezialisten mit sehr eigenen Bedürfnissen zugeschnitten waren. Zusätzlich war die Bedienung teilweise kaum intuitiv und oftmals umständlich. Nach der Veröffentlichung des iPads entwickelten abermals andere Hersteller in kürzester Zeit Konkurrenzprodukte und griffen erneut auf das Betriebssystem Android zurück. Im Wesentlichen kann gesagt werden, dass die Betriebssysteme der Tablets in weiten Teilen denen der Smartphones gleichen. Lediglich die Bildschirmauflösung wurde den größeren Anzeigen angepasst und die Telefoniefunktionen wurden entfernt. [23] [24]

Bei der Verteilung der Marktanteile liegt wiederum Android mit 72 Prozent vor iOS, welches lediglich auf 22,3 Prozent kommt. [25] Bemerkenswert ist der massive Zuwachs von Android in-

[18] ITWissen: Windows Phone [72]
[19] Microsoft Corp. [83]
[20] Reuters: Microsoft Corp. [101]
[21] siehe Abbildung 3.3
[22] ITWissen: iPad [65]
[23] ITWissen: Tablet [71]
[24] Bort: The History Of The Tablet, An Idea Steve Jobs Stole And Turned Into A Game-Changer [13]
[25] The Economic Times: Apple rules global tablet market with 22.3% share [119]



Period	Android	iOS	Windows Phone	BlackBerry OS	Others
Q3 2014	84.4%	11.7%	2.9%	0.5%	0.6%
Q3 2013	81.2%	12.8%	3.6%	1.7%	0.6%
Q3 2012	74.9%	14.4%	2.0%	4.1%	4.5%
Q3 2011	57.4%	13.8%	1.2%	9.6%	18.0%

Source: IDC, 2014 Q3

Abbildung 3.3: Smartphone Marktanteile nach Betriebssystem
IDC: Smartphone Market Share [57]

nerhalb von nur 3 Jahren. Im Jahr 2011 lag nämlich der Marktanteil von Tablets mit Apples Betriebssystem noch bei 72 Prozent. [26]

3.2 Mobile Apps

Der unglaubliche Erfolg der Smartphones sowie Tablets mit ihrer enormen Akzeptanz in der breiten Bevölkerung geht nicht zuletzt auch auf Apps zurück. [27] Apps sind kleine Programme, die von jeder Person mit ein wenig Programmiererfahrung erstellt werden können. [28] Die Verbreitung und Verfügbarmachung findet dann über die App-Plattformen der einzelnen Hersteller statt - bei Apple über den sogenannten „App Store“ und bei Google über den „Google Play Store“. [29]

> „Die hohe Beliebtheit von Smartphones ist zum größten Teil auf die Vielfalt der Apps in den Stores und das einfache Prinzip der Installation zurückzuführen. Es gibt für fast alle Vorlieben der Nutzer Apps im App-Store, wie z. B. Nachrichtenprogramme, Musik-Player, Spiele, Online-Banking oder Social Media.“ [30]

Die reinen numerischen Fakten sprechen eine klare Sprache und lassen keinen Zweifel an der Akzeptanz in der Bevölkerung. So hat der Google Play Store von 2300 Apps im März 2009 [31] auf 1,43 Millionen Apps im Dezember 2014 [32] sein Angebot um einen Faktor 621 erweitern können. Bereits im Juli 2013 feierte Google die „50 Milliarden App Downloads“-Marke. [33] Bemerkenswert ist auch die Gegenüberstellung der Downloadzahlen mit den Erträgen der jeweiligen Plattformen. So ist auffällig, dass die Anzahl der Downloads bei Google stetig höher ist als bei Apple, hingegen der Ertrag der Apps bei Apple teilweise signifikant über dem von Googles Plattform liegt. Siehe dazu auch Abbildungen 3.9 und 3.10. [34] [35]

Die Apps selbst können verschiedenste Anwendungsziele haben und es sind der Kreativität der Entwickler nahezu keine Grenzen gesetzt. Somit ist es nicht verwunderlich, dass sich auch ein nicht unwesentlicher Teil der Apps den Gesundheitsbereich als Ziel auserkoren hat. Hier muss zwischen „Health Apps“ und „Medical Apps“ unterschieden werden. Die Medical Apps sind ein Teilbereich der Health Apps, da sie einen klaren medizinischen Nutzen haben sollen und das

[26] The Economic Times: Google’s Android eating Apple’s market share [120]
[27] Bodden et al.: Schutzmaßnahmen gegen datenschutz-unfreundliche Smartphone-Apps [12] (S. 720)
[28] Gehring et al.: Zukunftstrend „Medical Apps“ [37] (S. 1402)
[29] Bodden et al.: Schutzmaßnahmen gegen datenschutz-unfreundliche Smartphone-Apps [12] (S. 720)
[30] Bodden et al.: Schutzmaßnahmen gegen datenschutz-unfreundliche Smartphone-Apps [12] (S. 720)
[31] Lawson: Android Market Needs More Filters, T-Mobile Says [80]
[32] appfigures: App Stores Growth Accelerates in 2014 [6]
[33] Warren: Google Play Hits 1 Million Apps [129]
[34] App Annie: App Annie Index – Market Q2 2013 [5]
[35] App Annie: App Annie Index – Market Q1 2014 [4]

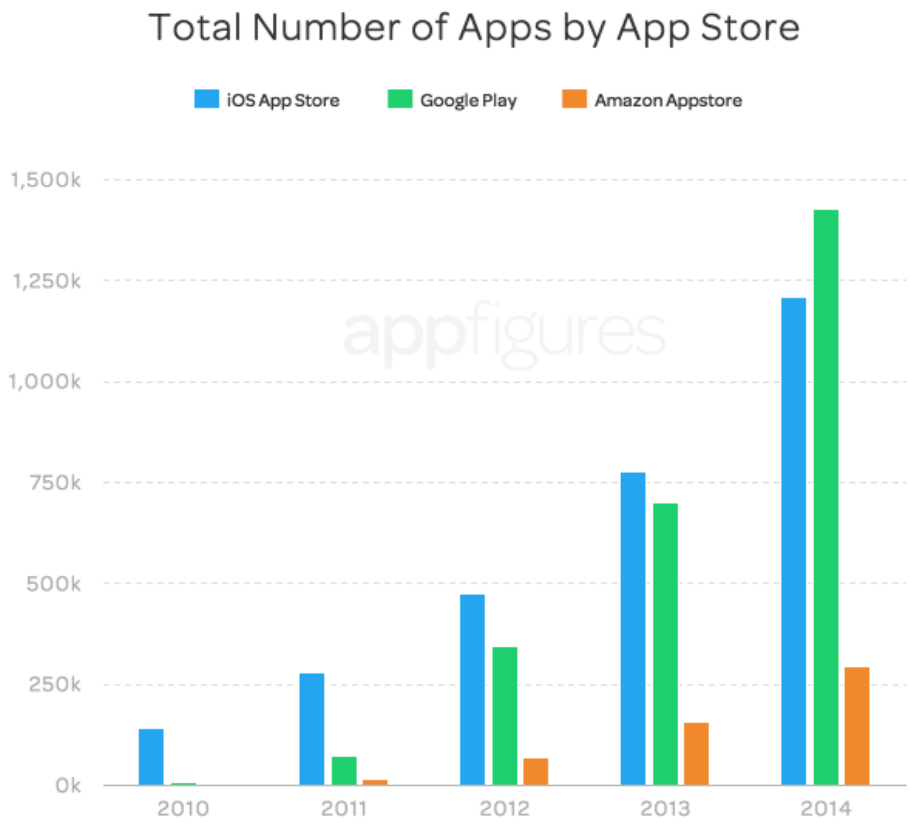


Abbildung 3.4: Anzahl der Apps nach App-Store im Vergleich
appfigures: App Stores Growth Accelerates in 2014 [6]

Ziel der medizinischen Verbesserung der aktuellen Situation unterstützen sollen. Health Apps allgemein können auch Anwendungen wie Fitness Planer oder digitale mobile Yoga Kurse sein. Siehe dazu auch die Abgrenzung in Abbildung 3.11. [36]

> „Führend im Angebot von Apps sind der Play Store von Google mit ca. 1,2 Mio. Apps (Stand Mai 2014) und der von Apple geführte App Store mit 1,14 Mio. Apps (Stand Mai 2014). [...] Der Gesamtmarkt für Apps wird im Jahr 2014 mit 8,3 Mrd. US-Dollar beziffert. Auch Apps für die Bereiche „Medizin“ und „Healthcare & Fitness“ bergen ein enormes finanzielles Potenzial: Beispielsweise liegt (Stand Mai

[36] Gehring et al.: Zukunftstrend „Medical Apps“ [37] (S. 1402f)

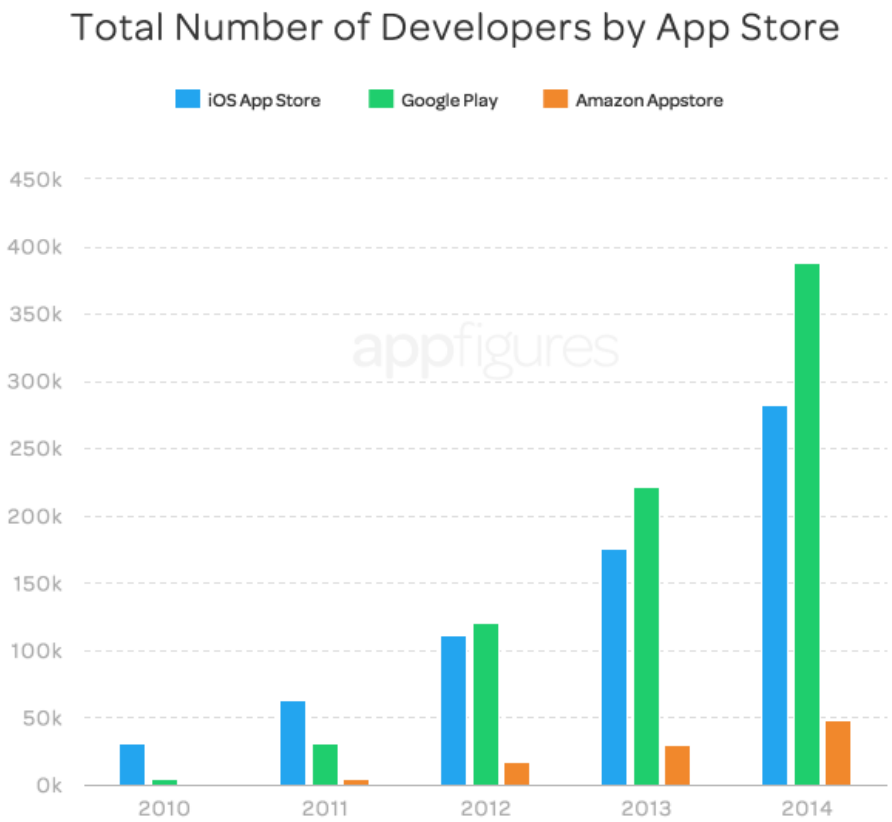


Abbildung 3.5: Anzahl der Entwickler nach App-Store im Vergleich
appfigures: App Stores Growth Accelerates in 2014 [6]

> 2014) die Zahl für „Healthcare & Fitness“ Apps für iOS bei 31.538 (2,76 %) und für Medical Apps bei 24.731 (2,17 %).“ [37]

Das enorme Potenzial des Marktes für Health Apps wurde auch von der Wirtschaft längst erkannt und die Entwicklungen laufen auf Hochtouren, was auch die Zahlen der Veröffentlichungen neuer Apps sowie die Anzahl der Downloads bestätigen. [38] Genau diese Zahlen und die Möglichkeit eines finanziellen Vorteils scheinen bei den ersten Versicherungsanstalten das Interesse an Health Apps geweckt haben. [39]

[37] Gehring et al.: Zukunftstrend „Medical Apps“ [37] (S. 1403)
[38] Gehring et al.: Zukunftstrend „Medical Apps“ [37] (S. 1402)
[39] Die Presse: Generali: App soll Gesundheit der Kunden überwachen [96]

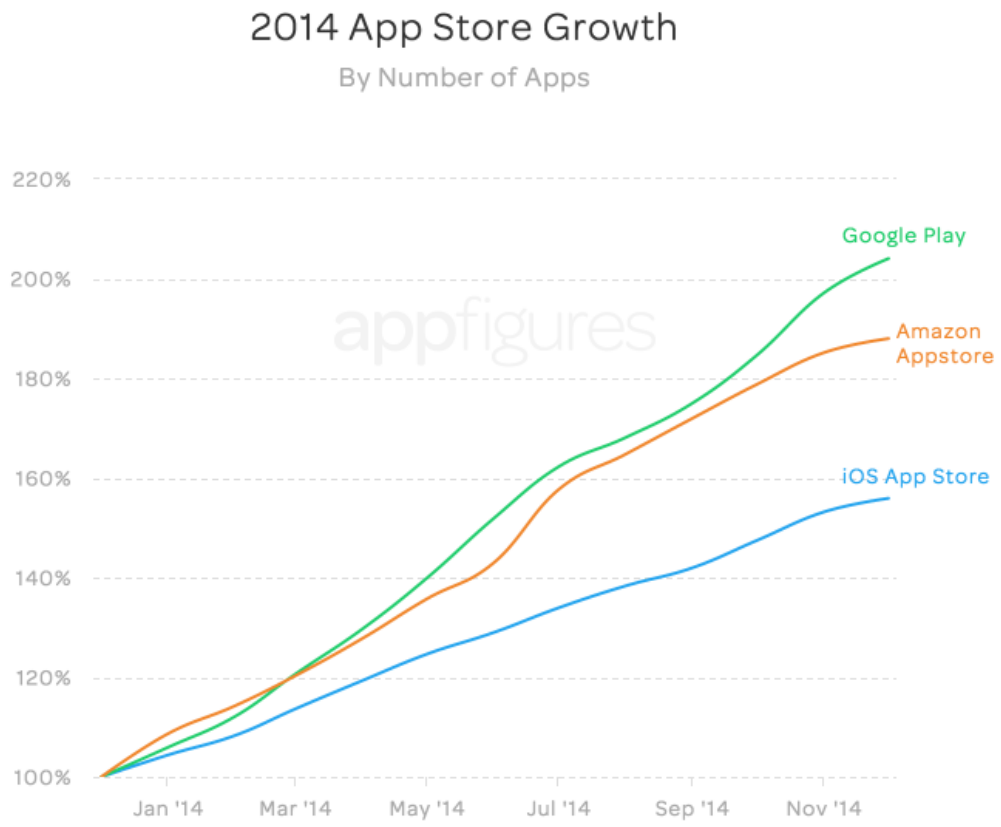


Abbildung 3.6: Zuwachs an Apps nach App-Store im Jahr 2014
appfigures: App Stores Growth Accelerates in 2014 [6]

Eine ähnliche Situation findet sich in den Krankenhäusern der USA. Hier wird offenbar mit dem Blick auf die mögliche Kostensenkung immer öfter anstelle des Einsatzes hochprofessioneller Geräte auf Überwachungslösungen von Smartphone-Herstellern gesetzt. [40]

3.3 Wearable Devices

Die Produktgruppe der Wearable Devices, welche auch Wearable Technology genannt wird, hatte bereits in den 1980er Jahren ihre Anfänge mit kleinen Taschenrechnern als Armbanduhren. [41] Allgemein kann man Wearable Devices als tragbare Computer beschreiben, welche in ihren

[40] Hoffmann: Apple HealthKit in US-Krankenhäuser immer öfter eingesetzt [54]
[41] Baguley: The Gadget We Miss: The Calculator Watch [9]

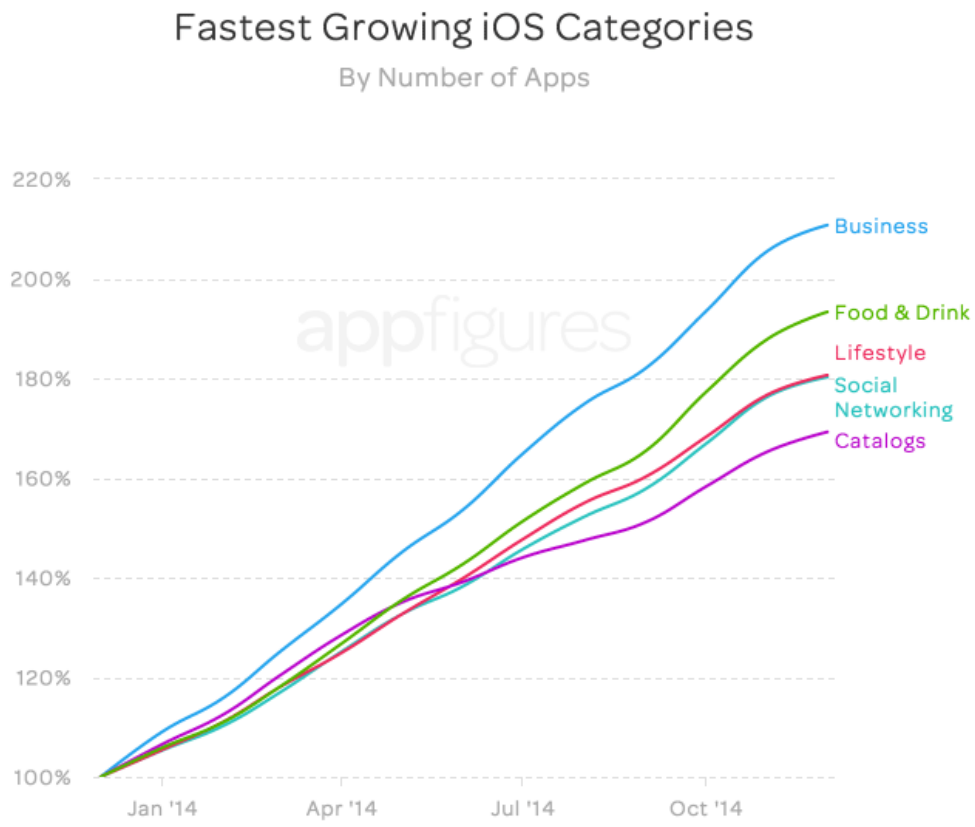


Abbildung 3.7: Am schnellsten wachsende iOS-App-Kategorien im Jahr 2014
appfigures: App Stores Growth Accelerates in 2014 [6]

Anfängen - geschuldet dem damaligen Stand der Technik - ohne Kommunikation mit anderen Geräten und heute als Zusatzprodukt - oftmals zu einem Smartphone - zu sehen sind. Der wirkliche Durchbruch für die Massenakzeptanz gelang mit den ersten Activity Trackern [42] und Smartwatches [43]. [44]

Activity Tracker sind tragbare Geräte, welche die Aktivitäten des Trägers messen und aufzeichnen können. Die Masse entspricht damit einem Band für das Handgelenk, welches Bewegung, Puls, geographische Position und ähnliche Daten aufzeichnen und an ein Smartphone übertragen kann. Diese Geräte zeichnen sich durch sehr einfache Bedienung, Tragekomfort, lange Akku-

[42] ITWissen: Fitness-Tracker [61]
[43] ITWissen: Smartwatch [70]
[44] ITWissen: Smart Wearables [68]

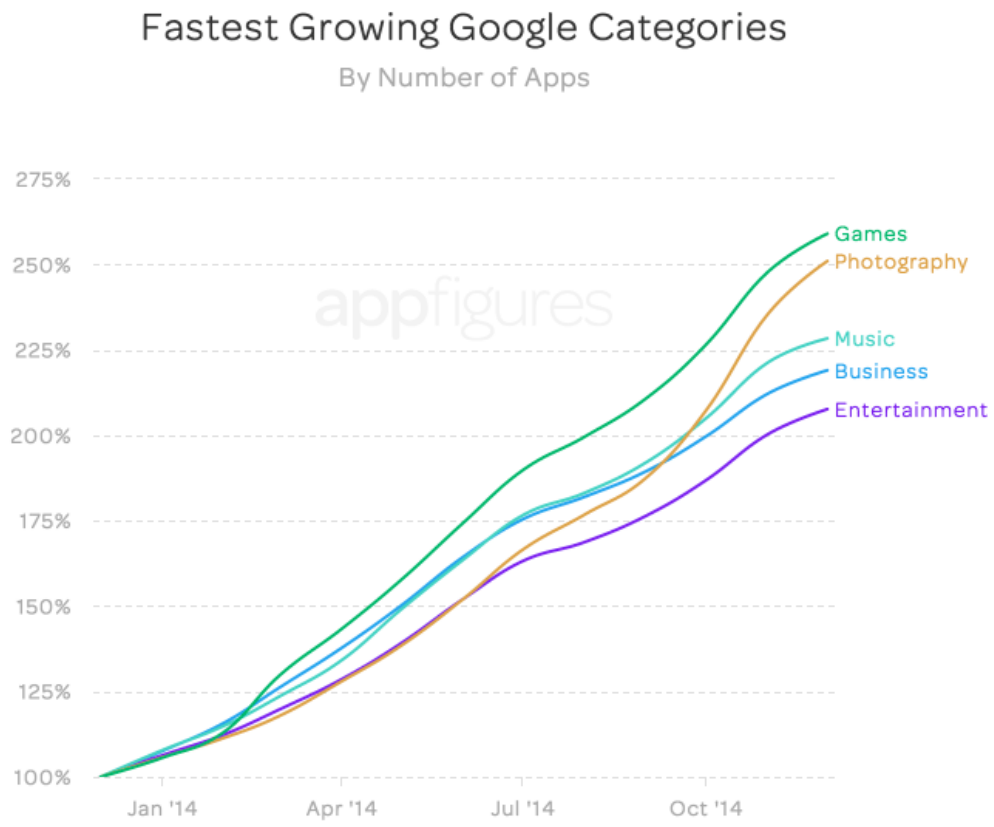


Abbildung 3.8: Am schnellsten wachsende Google-App-Kategorien im Jahr 2014
appfigures: App Stores Growth Accelerates in 2014 [6]

laufzeiten und hohe Resistenzen gegen Wasser, Schläge und Staub aus. Daher werden sie auch oft als Fitness Tracker bezeichnet. [45] [46] [47]

Smartwatches hingegen können nicht nur Informationen, gleich viele oder sogar mehr wie Activity Tracker, aufzeichnen, sie bieten dem Nutzer auch die Anzeige von Informationen. Sie sind sozusagen eine erweiterte, leichter erreichbare Anzeige des gekoppelten Smartphones. Somit ist es unter anderem möglich, eine ankommende Textnachricht direkt auf der Uhr zu lesen und sogar zu beantworten, ohne das Handy in die Hand nehmen zu müssen. [48]

[45] ITWissen: Fitness-Tracker [61]
[46] ITWissen: Intelligentes Armband [63]
[47] PCMag: Fitness Tracker [94]
[48] ITWissen: Smartwatch [70]

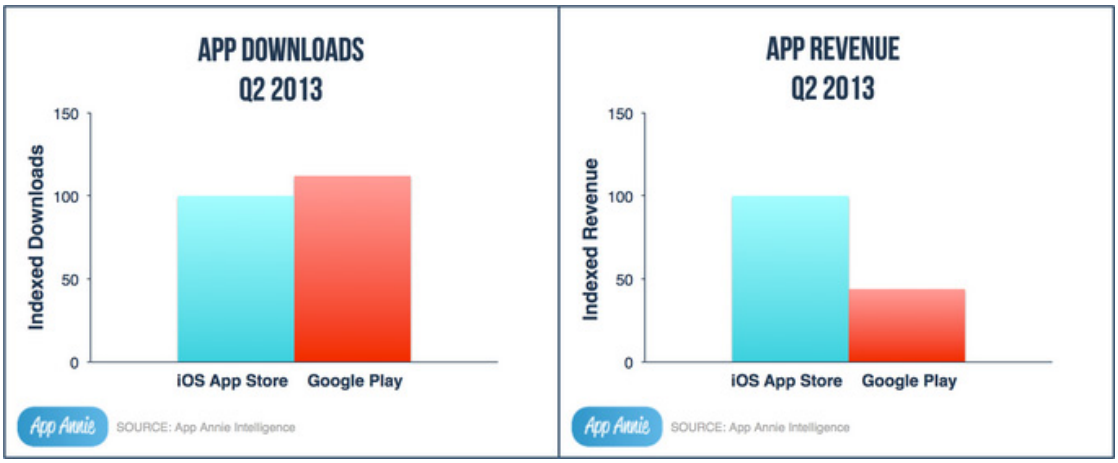


Abbildung 3.9: Downloads und Ertrag der App-Stores im Vergleich im Q2 2013
App Annie: App Annie Index – Market Q2 2013 [5]

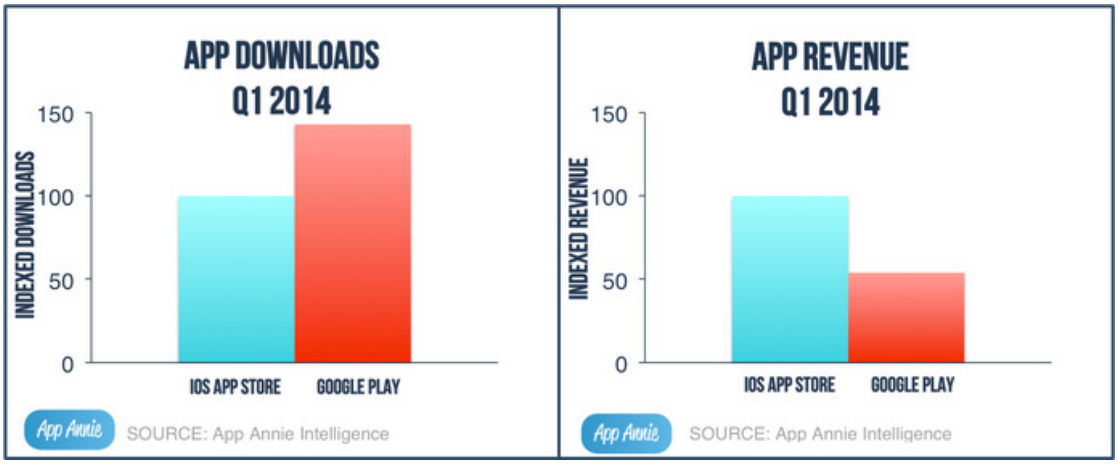


Abbildung 3.10: Downloads und Ertrag der App-Stores im Vergleich im Q1 2014
App Annie: App Annie Index – Market Q1 2014 [4]

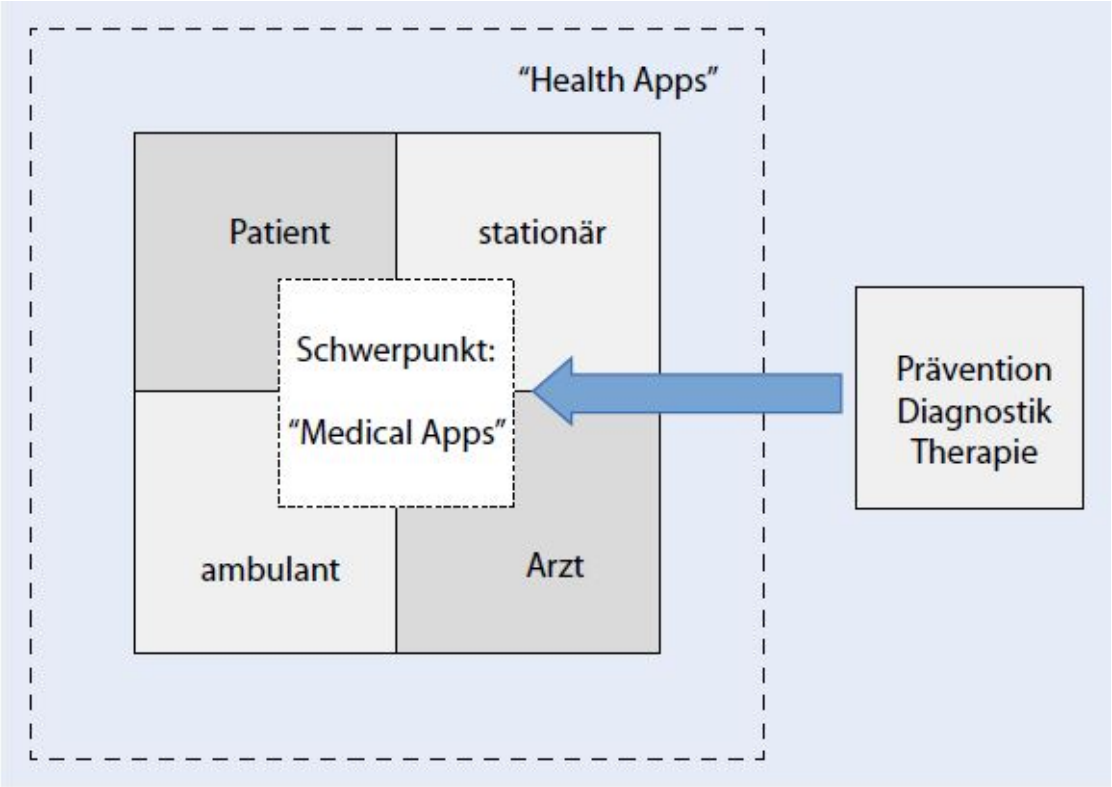


Abbildung 3.11: Abgrenzung von Health Apps und Medical Apps
Gehring et al.: Zukunftstrend „Medical Apps“ [37] (S. 1403)

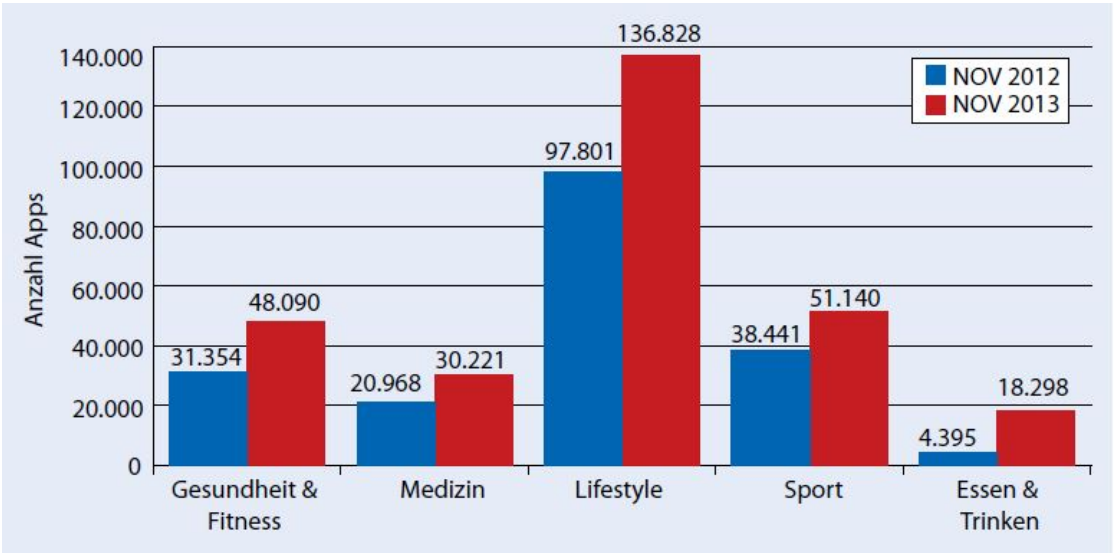


Abbildung 3.12: Verteilung von Health Apps von 2012 und 2013
Gehring et al.: Zukunftstrend „Medical Apps“ [37] (S. 1403)

Abbildung 3.13: Beispiele von Activity Trackern
Smartwach News: Top 5 Activity Trackers Of 2014 [86]

Abbildung 3.14: Beispiele von Smartwatches
Swide: Wearable tech and the top 5 smart watches at IFA 2014 [115]

Abbildung 3.15: Google Glass als Beispiel für Smartglasses
Hartung: The Reason Why Google Glass, Amazon Fire Phone and Segway All Failed [50]

Eine andere, aber bisher noch nicht sehr verbreitete Gruppe der Wearable Devices sind die E-Textiles. Darunter versteht man komplette Kleidungsstücke, die mit Sensoren ausgestattet sein können, um diverse Parameter wie zum Beispiel den Puls des Trägers zu messen und an ein Gerät, wie beispielsweise ein Smartphone, zu übertragen. [49]

Ebenfalls noch nicht massentauglich, aber durchaus vielversprechend sind die Smartglasses. Deren Aufgabe ähnelt der der Smartwatches. Sie sollen ein erweitertes Display des Smartphones darstellen und einfache Kommandos ohne direkte Interaktion mit dem Telefon ermöglichen. Dies wird einerseits durch eine holografische Einblendung direkt im Sichtfeld des Trägers erreicht, andererseits durch Sprachsteuerung. [50]

Die letzten beiden erwähnten Produktgruppen sind aufgrund ihres derzeitigen technologischen Entwicklungsstandes für die Massenproduktion noch nicht geeignet und ihr Verbreitungsgrad ist dementsprechend sehr gering.

Einen durchaus vielversprechenden Ausblick geben die neuesten Entwicklungen im professionellen medizinischen Einsatz. Dort könnten intelligente Klebestreifen zur Aufbringung auf die

[49] ITWissen: Intelligente Kleidung [62]
[50] ITWissen: Smart Glasses [67]

Haut, welche den Blutzucker des Trägers messen sollen, das Leben von Diabetikern maßgeblich erleichtern und verbessern. [51]

[51] Ramsey: Stick-On Tattoo Measures Blood Sugar Without Needles [99]

KAPITEL 4

Analyse des Marktes

Die Anzahl der Smartphone-Apps im Bereich Fitness und Healthcare nimmt stetig zu, da auch die Wirtschaft diesen Zweig und den Bedarf ganz klar erkannt hat. Derzeit geht man in Summe von knapp 100.000 Apps auf allen Plattformen aus. [1] Aus diesem Grund werden in diesem Kapitel als Stichprobe fünf Fitness Apps zu einem vollständigen Test herangezogen, um deren Datenschutzkonformität zu prüfen.

4.1 Vorgehensweise und Testumgebung

Aufgrund der deutlich stärkeren Verbreitung des Betriebssystems Android gegenüber allen anderen Plattformen [2] sowie der höheren Angebotszahl im Google Play Store gegenüber dem Apple App Store [3] wird sich die Auswahl der Testobjekte auf androidbasierte Apps beschränken.

Als Testgerät diente ein frisch auf Werkseinstellungen zurückgesetztes Google Nexus 5 mit einer Bildschirmauflösung von 1080 mal 1920 Pixel und einer ungefähren Pixeldichte von 445 Pixel pro Inch. Als Betriebssystem kam Android in der Version 5.0.1 - auch als „Android Lollipop“ bezeichnet - zum Einsatz. Somit ist das Betriebssystem das aktuellste derzeit verfügbare. Der Hauptprozessor war ein Qualcomm Snapdragon 800 mit einem Takt von 2,26 GHz und der Grafikprozessor ein Adreno 330 mit einem Takt von 450 MHz. [4]

Bei jeder getesteten App sollten die folgenden Punkte abgearbeitet und analysiert werden:

[1] Gehring et al: Zukunftstrend „Medical Apps“ [37] (S. 1402f)
[2] siehe Kapitel 3.1
[3] siehe Kapitel 3.2
[4] Google: Google Nexus 5 [42]

Abbildung 4.1: Testgerät Google Nexus 5
Google: Google Nexus 5 [42]

- **Entwickler** - Der Name und die Herkunft des Herstellers sowie der Speicherort der Daten sollen festgehalten werden.
- **Datenschutzbestimmungen** - Sofern vorhanden, soll festgehalten werden, wie leicht diese vor bzw. bei der Installation aufzufinden sind und welche möglichen Risiken sich darin verbergen.
- **Installation** - Der gesamte Installationsprozess soll dokumentiert werden.
- **Benutzerkonto** - Es soll analysiert werden, ob ein Benutzerkonto zwingend für das Verwenden der App erforderlich ist und welche Daten dafür verwendet werden müssen.
- **Funktionen** - Alle Funktionen, welche diese App anbietet, sollen auch auf datenschutzrechtliche Bedenken hin analysiert werden.

Abbildung 4.2: Runtastic Logo
Runtastic [108]

- **Unterstützte Geräte** - Es soll eruiert werden, ob die App die Möglichkeit bietet, weitere Geräte, wie etwa Pulsmesser, einzubinden und anzusprechen.
- **Erfasste Daten** - In diesem Punkt sollen alle Daten, welche eindeutig von der App erhoben werden, zusammengefasst werden.
- **Rechtskonformität** - Abschließend wird ein Gesamtbild der Rechtskonformität auf Basis der bisher erworbenen Erkenntnisse erstellt.

Es wurden fünf Apps aufgrund Beliebtheit, Funktionsumfang und Qualität ausgewählt. [5]

4.2 Runtastic

Adresse: https://play.google.com/store/apps/details?id=com.runtastic.android

[5] Android Authority: 15 best Android fitness apps and workout apps [8]

Als Entwickler dieser App zeichnet die Firma runtastic GmbH in Pasching bei Linz, Österreich. Über den Speicherort der Daten kann lediglich eine Vermutung angestellt werden. Nach einem Nachverfolgen der Internetadresse „www.runtastic.com“, welche dem Entwickler gehört, antwortet ein Server in Österreich. Ob dies auch im Endeffekt der Speicherort der Daten ist, kann nicht mit Sicherheit gesagt werden.

Die Datenschutzbestimmungen sind, wie im Google Play Store allgemein gehandhabt, nicht leicht zu finden, da sie sich ganz am Ende der Installationsseite befinden. Dies bedeutet für den Benutzer ein mehrseitiges Scrollen, vorbei an der Möglichkeit zur Installation, Screenshots der App, der App-Beschreibung und Bewertungen von anderen Nutzern. Sogar Empfehlungen für andere ähnliche Apps werden noch vor dem Link zu den Datenschutzbestimmungen angezeigt. [6]

Bemerkenswert ist, dass, selbst wenn der Benutzer sich den langen Weg zu den Bestimmungen aufbürdet, diese auf den ersten Blick den Eindruck erwecken, als hätten sie nur zwei kurze Absätze. Dies ist einem Anzeigefehler auf dem Smartphone zu schulden. Die Bestimmungen wurden nämlich mittels iFrame eingebunden und diesem fehlt in der mobilen Ansicht der Scrollbalken - weswegen der Benutzer nicht erkennen kann, dass die Bestimmungen eigentlich viel länger sind, als auf den ersten Blick gedacht. [7]
Der Entwickler macht in seinen Datenschutzbestimmungen eindeutig klar, dass er personenbezogene Daten wie Vorname, Nachname, Wohnadresse und eMail-Adresse seiner Nutzer sammelt. Darüber hinaus erfasst er Daten über die sportlichen Aktivitäten der Nutzer, wie Länge und Art der Aktivität sowie den Ort oder den Puls. Diese sind eindeutig als sensible Daten einzustufen. Weiters macht Runtastic klar, dass jeder Nutzer selbst das Bestimmungsrecht behält, welche seiner Informationen andere Nutzer sehen dürfen. Die Sammlung der personenbezogenen Daten jeglicher Art wird von Runtastic nicht an Dritte weitergegeben, ausgenommen im Falle einer gesetzlichen Verpflichtung oder der ausdrücklichen Genehmigung des Benutzers. Weiters legt Runtastic fest, dass nicht individualisierbare Daten von Runtastic oder seinen Partnern zur In-App-Werbung oder auf der Webseite des Herstellers verwendet und gespeichert werden dürfen. Für die sensiblen Gesundheitsdaten gibt Runtastic klar an, dass diese Daten niemals an Vermarktungsnetzwerke oder ähnliche Anbieter weitergegeben werden.
Speziell bei den sensiblen Gesundheitsdaten lässt der Entwickler das generelle Verbot der Weitergabe aus, sondern verpflichtet sich lediglich, diese Daten nicht an Werbenetzwerke weiterzugeben.

Der Installationsprozess selbst gestaltet sich erwartungsgemäß leicht. Lediglich die Zugriffsberechtigungen, welche vorher akzeptiert werden müssen, sind auf den ersten Blick sehr umfangreich. Speziell die Berechtigungen auf den Zugriff von Fotos, der Kamera und das Mikrofons des Smartphones lösen Unbehagen aus. [8] Sie decken sich allerdings mit den offiziellen Funktionen und den dafür notwendigen Hard- bzw. Software Zugriffen. Auffällig in Hinsicht auf die Da-

[6] siehe Abbildung 4.3 und 4.4
[7] siehe Abbildung 4.5
[8] siehe Abbildung 4.6

tenschutzbestimmungen ist allerdings, dass auf diese kein einziges Mal hingewiesen wird oder diese explizit zu akzeptieren wären.

Bei dem ersten Start der App empfiehlt diese das Anlegen oder Eingeben eines Benutzerkontos. Es ist sowohl der Login mittels der Plattformen Google+ und Facebook als auch ein eigenes Konto bei Runtastic direkt möglich. [9] Lediglich klein und farblich gut versteckt am unteren Rand des Bildschirms liegt die Möglichkeit, diesen Punkt zu überspringen. Überspringt man dies, wird man direkt nochmals mittels einer Präsentation, welche die Vorteile eines Accounts darlegt, dazu aufgefordert, sich ein Benutzerkonto anzulegen. Erst in dem jeweils letzten Schritt eines Logins - welcher Plattform ist dabei unerheblich - wird man klein und erneut versteckt auf die Datenschutzbestimmungen hingewiesen, welche man mit einem Login automatisch akzeptiert.

Die App bietet eine Vielzahl von sehr ausgefeilten Funktionen. So erwartet den Nutzer am ersten Schirm direkt die Möglichkeit, sofort mit einem Training zu starten. [10] Außerdem kann der Aktivitätenverlauf [11] sowie die persönliche Statistik [12] eingesehen werden. Es lassen sich auch manuell Aktivitäten nachträglich hinzufügen. Die Auswahlmöglichkeiten erstrecken sich über einen sehr großen Bereich und man kann alle gängigen Sportarten darin finden. Darüber hinaus können Trainingspläne abgerufen werden [13], manche davon sogar kostenlos. Die Funktion „Story Running“ [14] ist eine etwas andere Art, bei der sportlichen Aktivität nicht die Motivation zu verlieren. Man kann hier - oft kostenpflichtige - Geschichten auswählen, welche während des Laufens abgespielt werden können. Es ist somit eine Mischung aus kurzem Hörbuch mit motivierenden Musikeinlagen, speziell abgestimmt auf die sportliche Aktivität. In der kostenpflichtigen Variante der App stehen neben kompletter Werbefreiheit einige zusätzliche Funktionen zur Verfügung. So können die bisherigen Routen gespeichert und wieder abgerufen werden. [15] Weiters bietet sich eine Intervalltrainings-Funktion an, um das Training noch spezieller an die eigenen Bedürfnisse anzupassen. [16] Darüber hinaus bietet sie die Möglichkeit, ein Pulsmessgerät anzuschließen, dessen Daten mit denen der sportlichen Aktivität gemeinsam erfasst, kombiniert und ausgewertet werden können. [17]

Wie bereits am Ende des vorhergehenden Absatzes angesprochen, bietet Runtastic in seiner kostenpflichtigen Variante die Möglichkeit, ein Gerät zur Pulsmessung zu verbinden und dessen Daten mit auszuwerten. Hierzu stellt die Firma selbst Hardware zum Kauf bereit. Es wird aber eine Vielzahl von Geräten anderer Hersteller ebenfalls unterstützt. Außerdem ist Runtastic be-

[9] siehe Abbildung 4.7
[10] siehe Abbildung 4.8
[11] siehe Abbildung 4.9
[12] siehe Abbildung 4.10
[13] siehe Abbildung 4.11
[14] siehe Abbildung 4.12
[15] siehe Abbildung 4.13
[16] siehe Abbildung 4.14
[17] siehe Abbildung 4.15

reits für die Benutzung einer Smartwatch optimiert und kann an diese Informationen senden und empfangen.

Die erfassten Daten sind sehr umfangreich. Es werden sowohl vollständige Verläufe von Standortdaten während einer Aktivität erfasst, als auch, sofern vorhanden, die Herzfrequenz aus einem entsprechenden Gerät abgegriffen und verarbeitet. Damit kann ein komplettes Bewegungsprofil erstellt werden; das heißt, wie schnell sich der Nutzer während seiner Aktivität genau bewegte, sowie von welchem Ort zum nächsten. Darüber hinaus kombiniert Runtastic die Daten mit den Pulsmessgeräten und ermöglicht damit, auf lange Sicht ein Gesundheitsprofil zu erstellen. Zusätzlich können Rückschlüsse auf die Sportlichkeit des Nutzers gezogen werden. Durch die Bindung an ein eindeutiges Benutzerkonto lassen sich die Daten zusätzlich sehr leicht einer bestimmten Person zuordnen, umso leichter, wenn die Person als Login-Variante eine Social-Network-Plattform wie etwa Facebook wählt. Es ist davon auszugehen, dass bei einer Verwendung eines Benutzerkontos alle erfassten Daten an die Server von Runtastic übertragen werden. Dieser Schluss ergibt sich aus folgenden zwei Tatsachen: Einerseits kann der Nutzer alle am Smartphone erfassten Daten ohne zusätzliches Zutun auch auf der Webseite von Runtastic einsehen. Dafür ist lediglich ein Login mit dem gleichen Benutzerkonto nötig. Andererseits sind alle Daten nach einer vollständigen Neuinstallation und erneutem Login mit dem gleichen Benutzerkonto wieder in der App sichtbar. Dies kann nur den Grund haben, dass alle Daten sofort an die Server übertragen werden und somit in der Cloud gespeichert sind.

Die Rechtskonformität an sich ist nicht ganz trivial, da aktuell davon auszugehen ist, dass die Daten ausschließlich im europäischen Inland, in diesem speziellen Fall in Österreich, gespeichert werden und keine Übertragung in Drittländer stattfindet. Ob die Zustimmung zu der Datenschutzerklärung durch einen bloßen Login mit einem Benutzerkonto erfolgen kann, ist fraglich. Es wird niemals augenscheinlich und explizit auf die Datenschutzerklärung hingewiesen. Sie ist eher als ein schlecht sichtbarer Link am Ende der Anzeige zu finden. Zusätzlich beinhaltet die Seite mit den Erklärungen Anzeigefehler, welche auf den ersten Blick nicht erkennen lassen, dass diese viel länger sind als anfangs angenommen. Es ist rechtlich nicht eindeutig klargestellt, ob dieses Vorgehen einer echten Einwilligung zu einer Datenschutzerklärung gleichkommt [18] - speziell in diesem heiklen Fall der Sammlung von personenbezogenen sensiblen Daten. Zusätzlich ist nicht klar, welche Daten von den Werbeeinblendungen der kostenlosen Variante der App gesammelt und verarbeitet werden. Darüber hinaus ist es ungewiss, ob diese Daten in Drittländer exportiert werden.

[18] Bodden et al.: Schutzmaßnahmen gegen datenschutz-unfreundliche Smartphone-Apps [12] (S. 723)

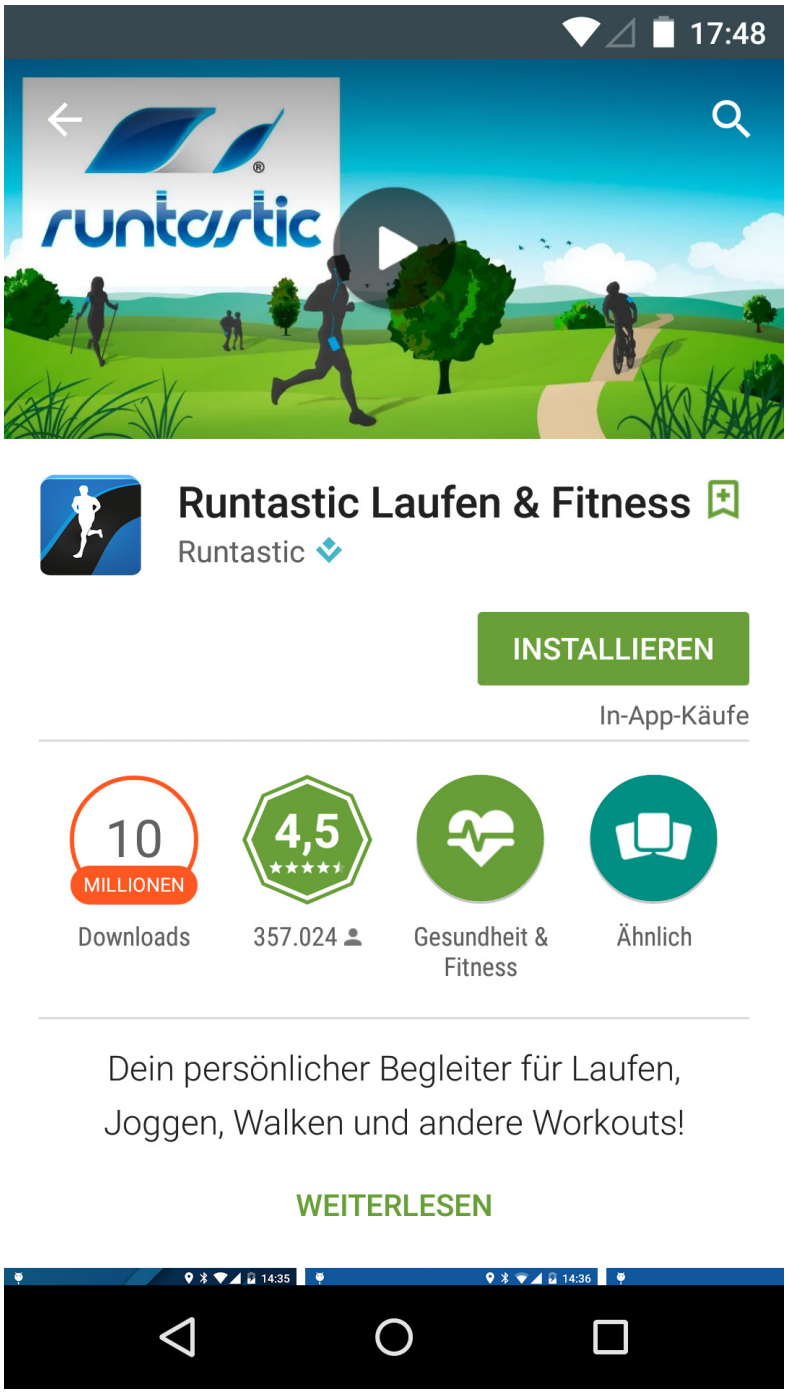


Abbildung 4.3: Runtastic - 1 - Installation
Runtastic [108]

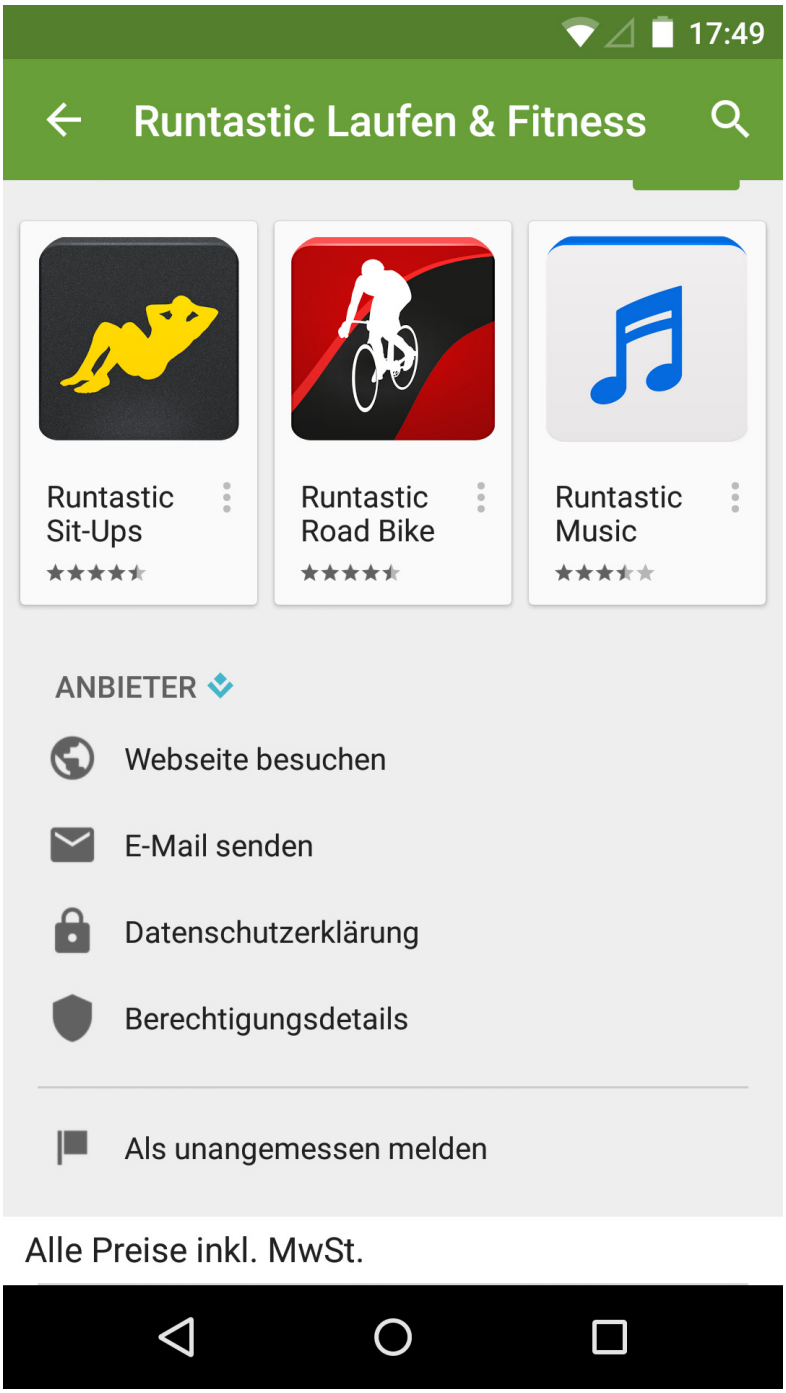


Abbildung 4.4: Runtastic - 2 - Installation
Runtastic [108]

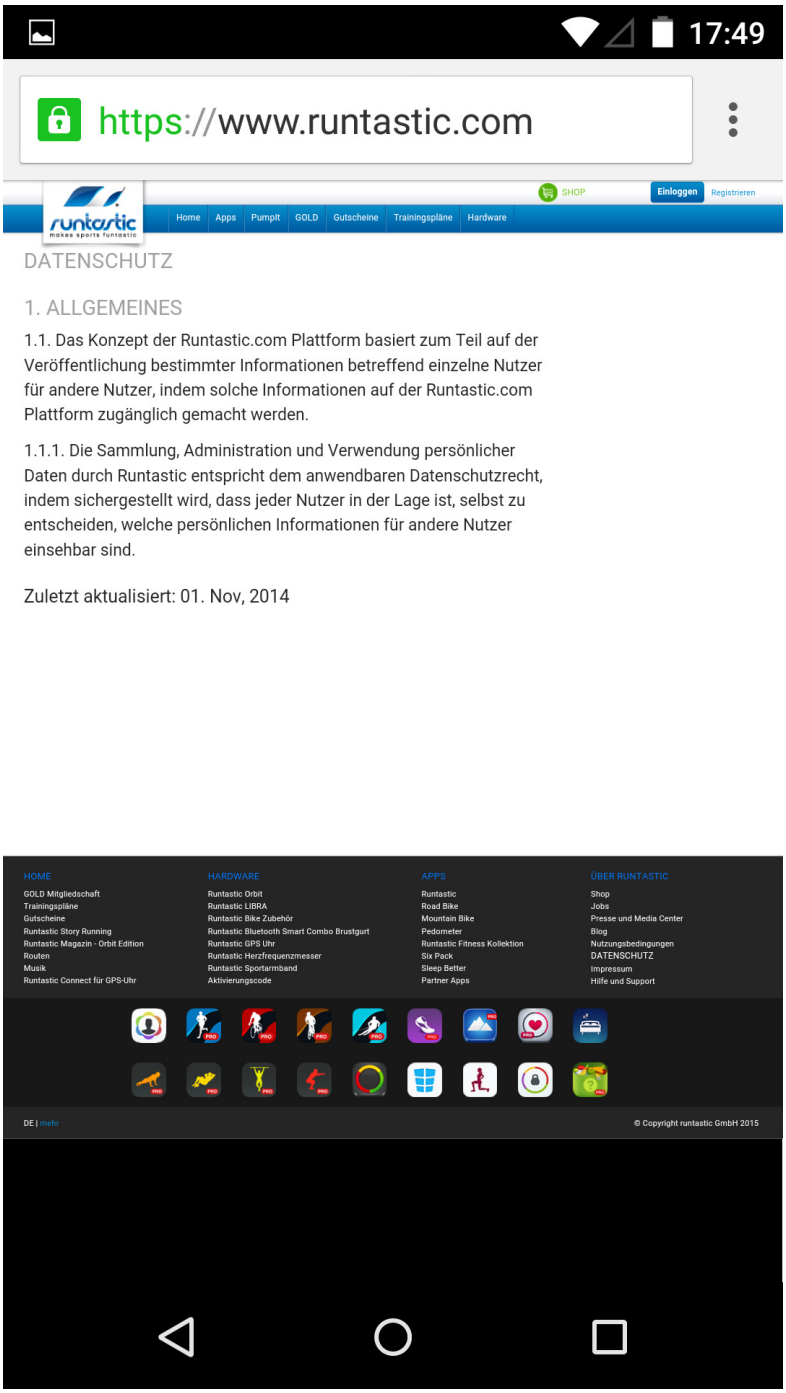


Abbildung 4.5: Runtastic - 3 - Datenschutzbestimmungen
Runtastic [108]

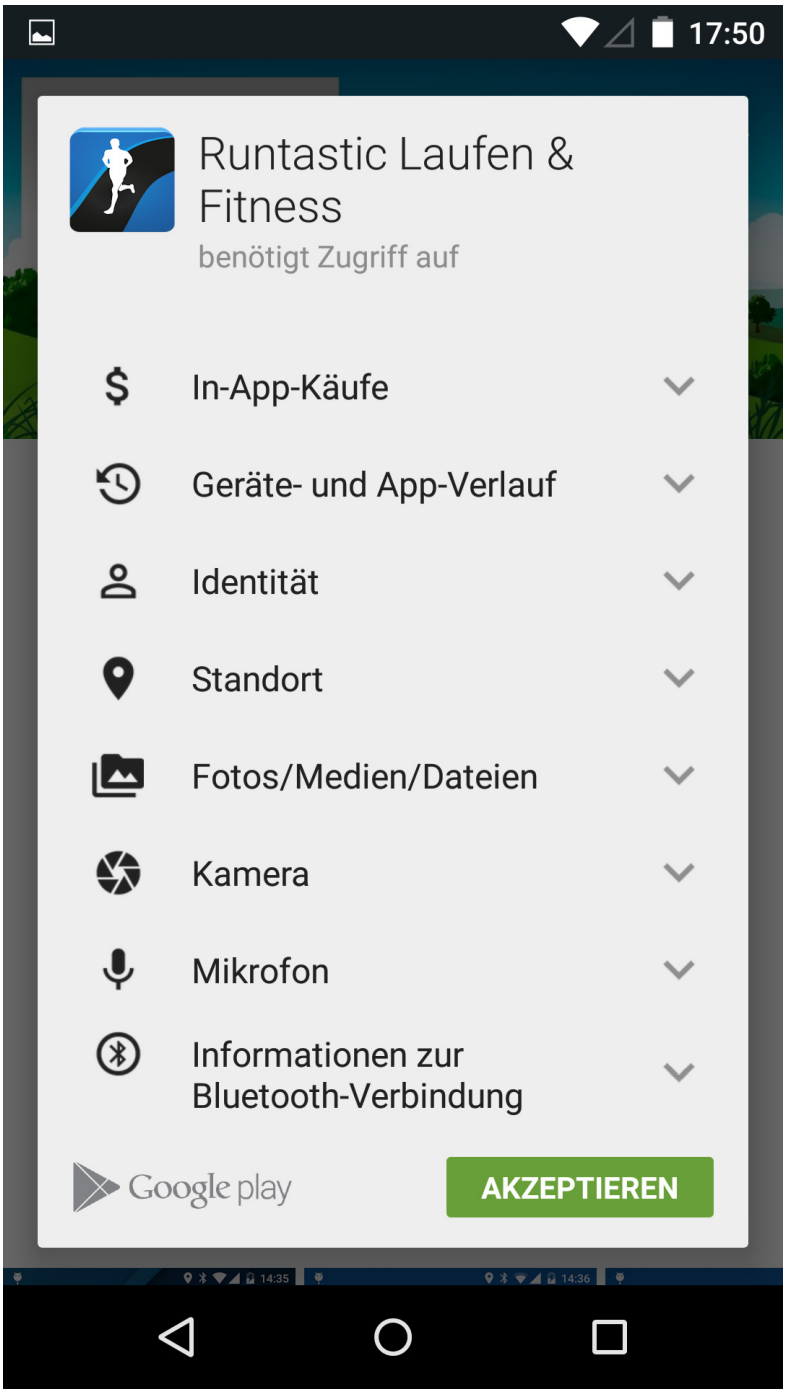


Abbildung 4.6: Runtastic - 4 - Berechtigungen
Runtastic [108]

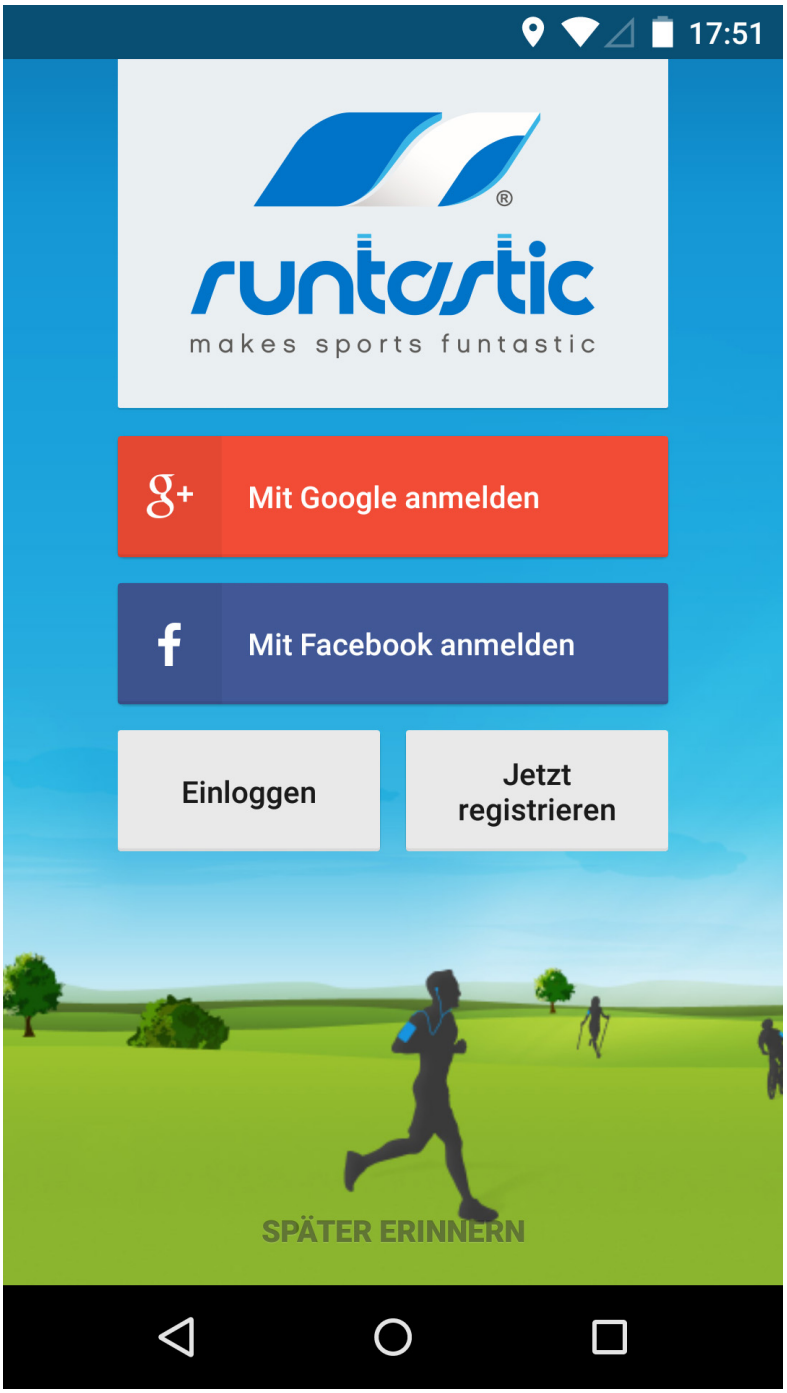


Abbildung 4.7: Runtastic - 5 - Benutzerkonto
Runtastic [108]

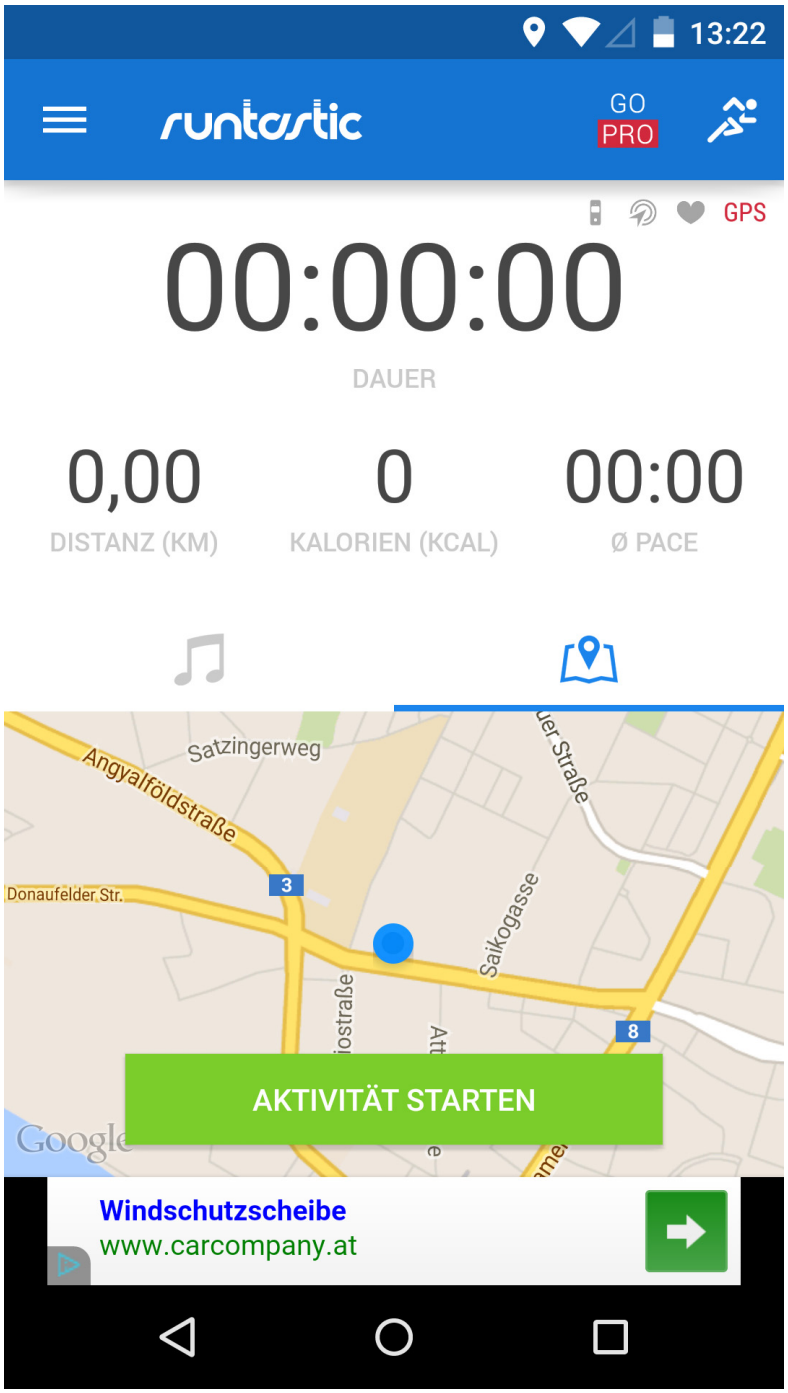


Abbildung 4.8: Runtastic - 6 - Funktionen - Start
Runtastic [108]

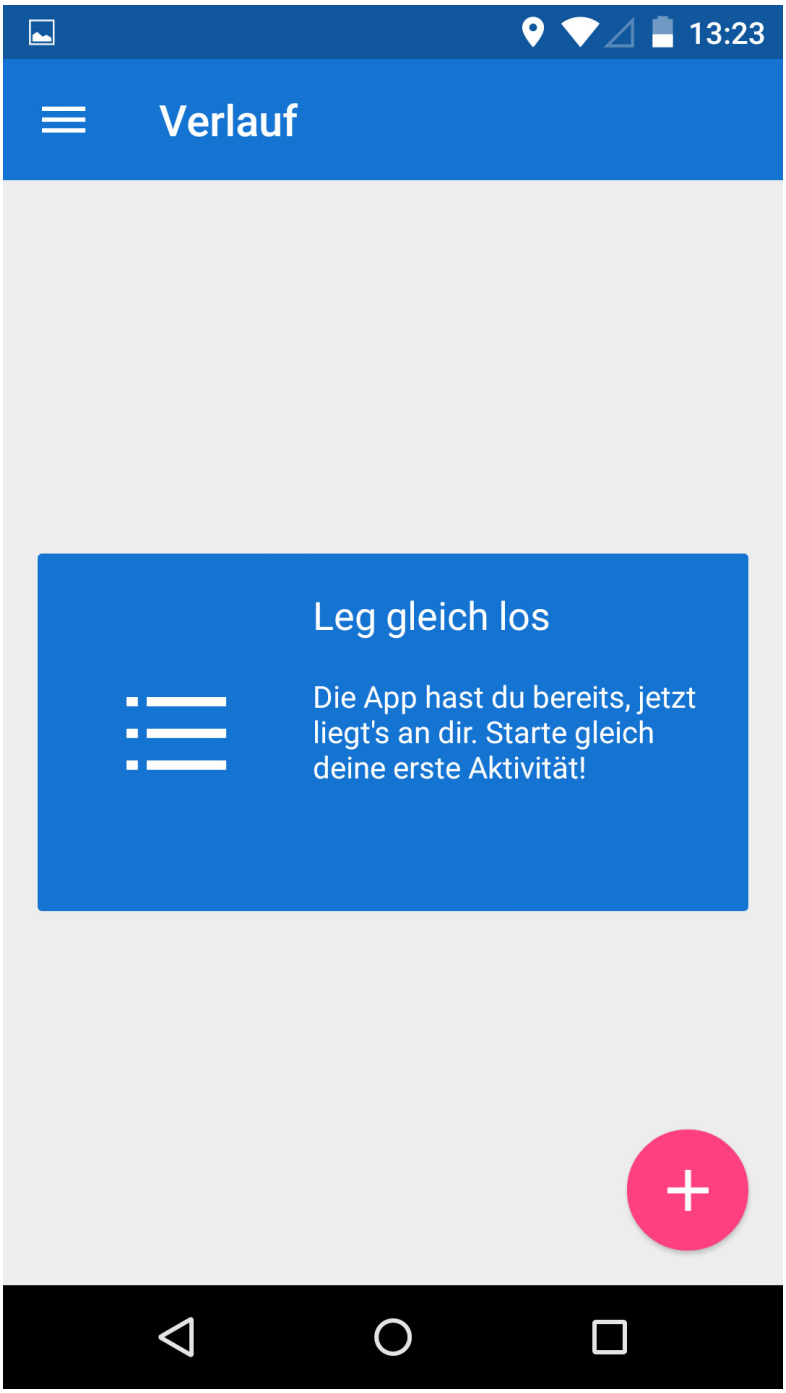


Abbildung 4.9: Runtastic - 7 - Funktionen - Verlauf
Runtastic [108]

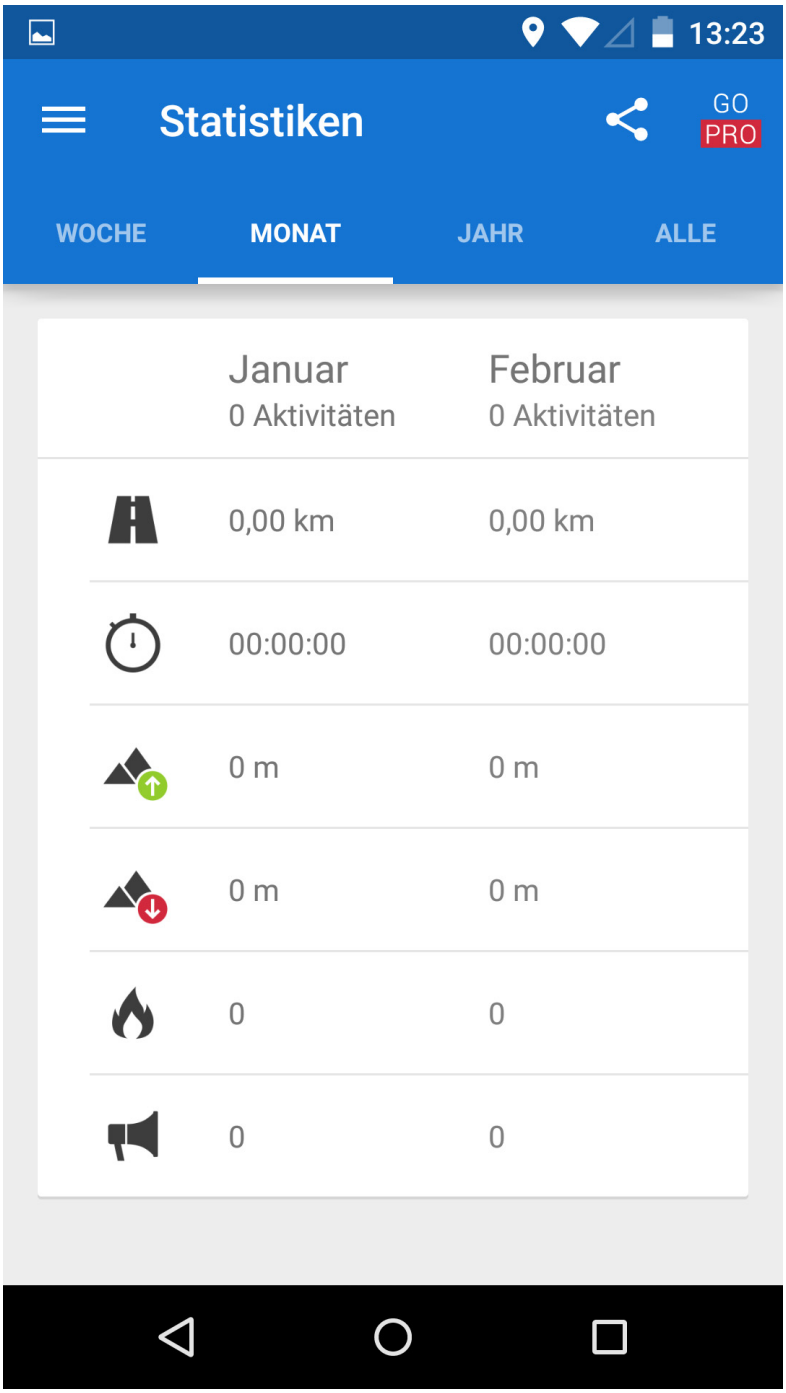


Abbildung 4.10: Runtastic - 8 - Funktionen - Statistiken
Runtastic [108]

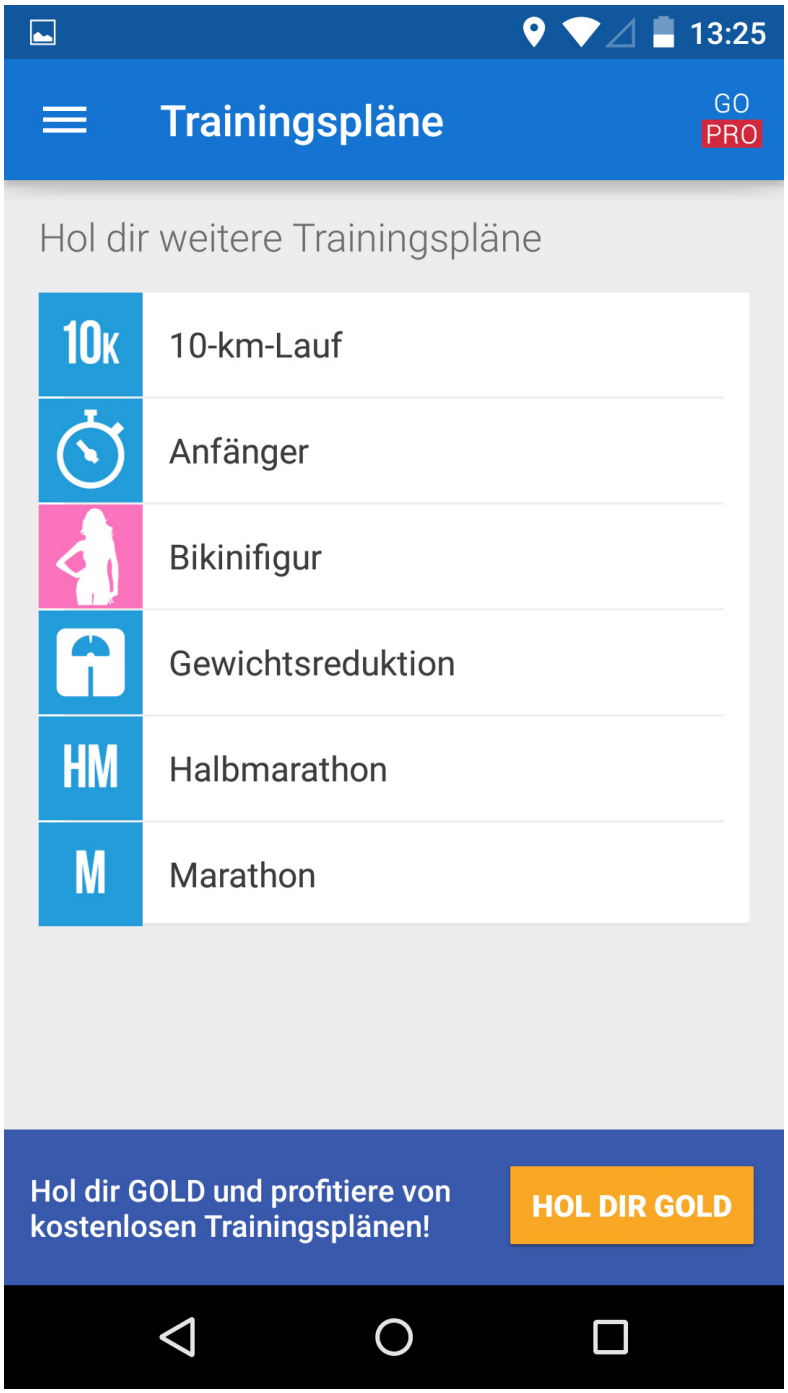


Abbildung 4.11: Runtastic - 9 - Funktionen - Trainingspläne
Runtastic [108]

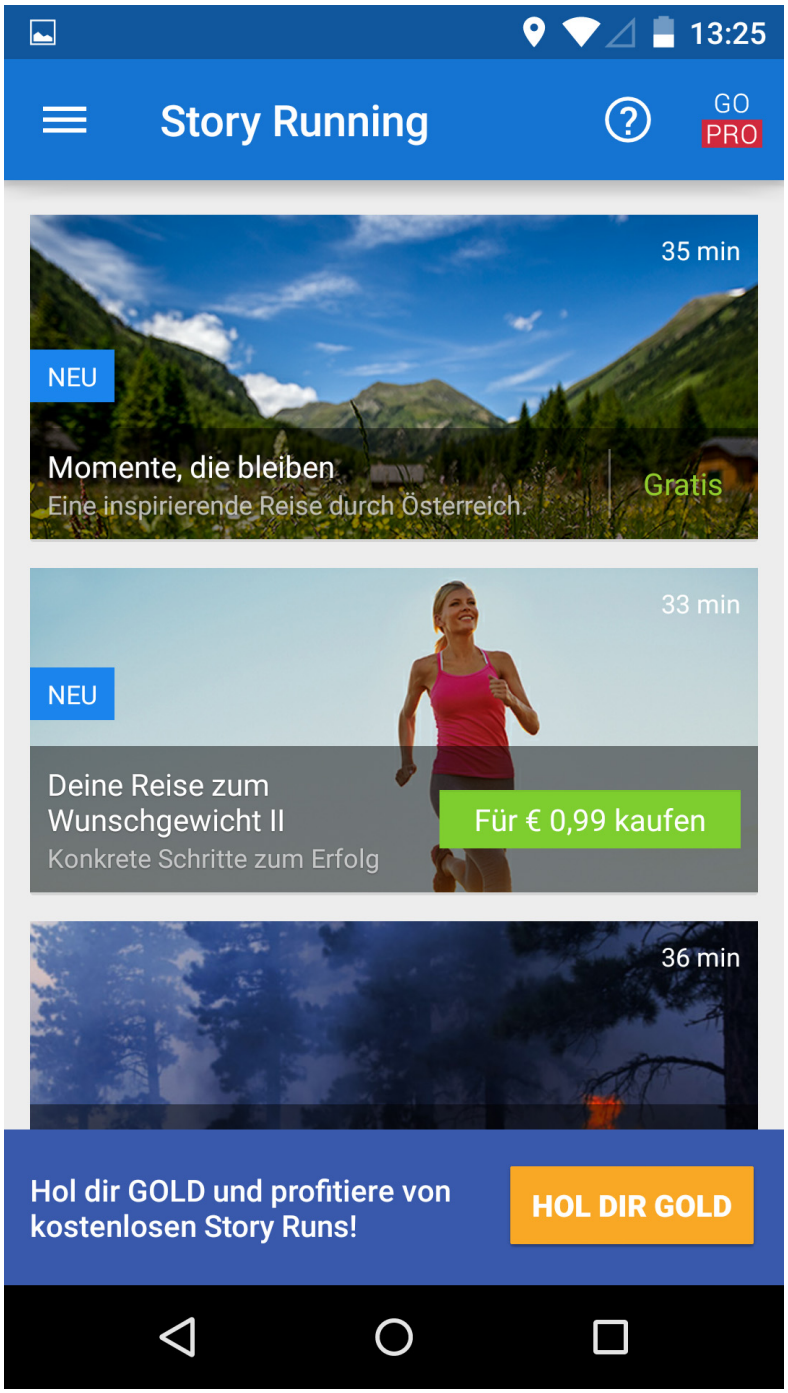


Abbildung 4.12: Runtastic - 10 - Funktionen - Story Running
Runtastic [108]

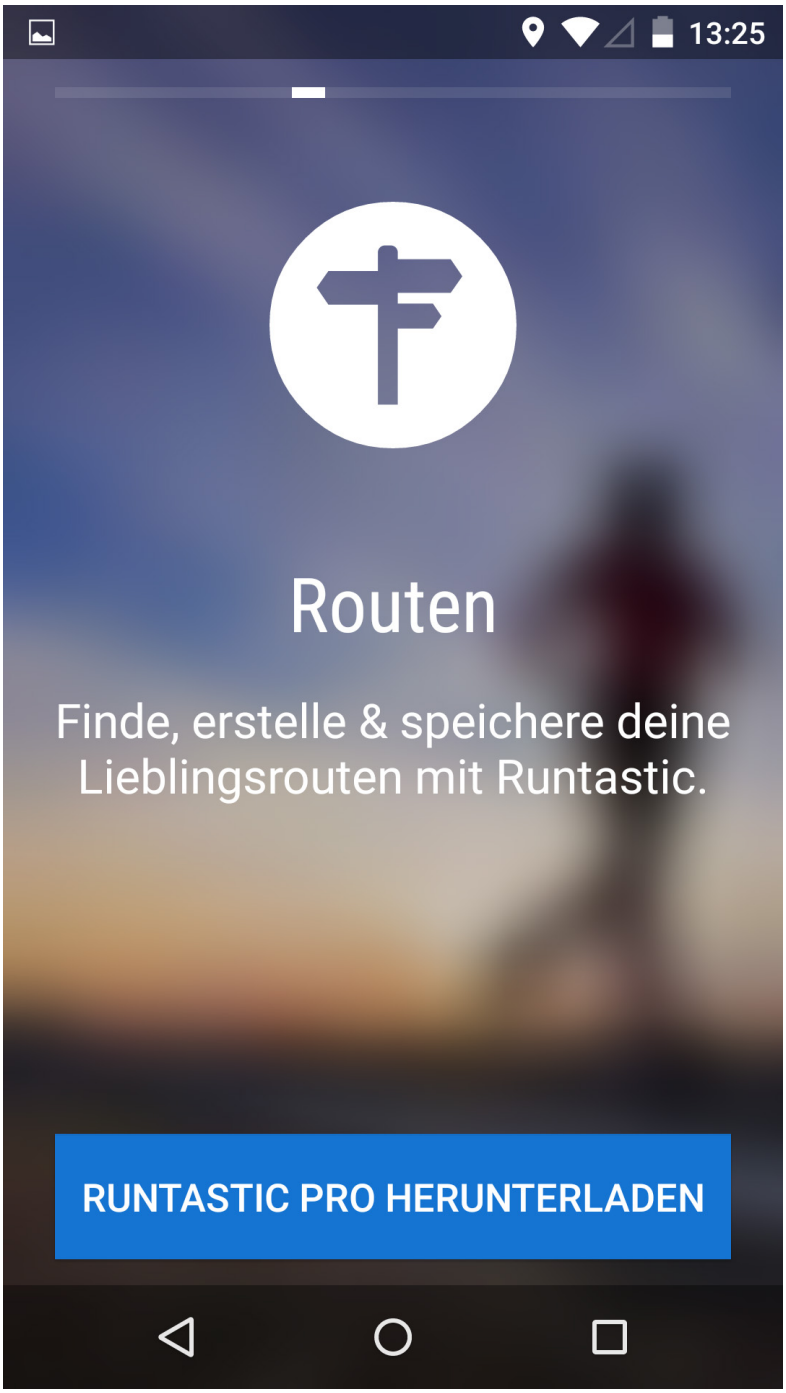


Abbildung 4.13: Runtastic - 11 - Funktionen - Routen
Runtastic [108]

Abbildung 4.14: Runtastic - 12 - Funktionen - Intervalltraining
Runtastic [108]

Abbildung 4.15: Runtastic - 13 - Funktionen - Herzfrequenzmessung
Runtastic [108]

Abbildung 4.16: Google Fit Logo
Google Fit [43]

4.3 Google Fit

Adresse: https://play.google.com/store/apps/details?id=com.google.android.apps.fitness

Der Entwickler von Google Fit ist Google selbst mit seinem Firmensitz in Mountain View, Kalifornien, USA. Es ist anzunehmen, dass alle Daten in Googles Datenzentren in den Vereinigten Staaten von Amerika gespeichert werden und aus europäischer Sicht ein Datentransfer in ein Drittland stattfindet.

Die Datenschutzbestimmungen sind, wie im Google Play Store üblich, vor der Installation lediglich ganz unten auf der App-Seite zu finden. [19] Die verlinkten Bestimmungen an sich beziehen sich allerdings keinesfalls auf die App Google Fit im Speziellen, sondern sind die allgemeinen Datenschutzbestimmungen des gesamten Konzerns Google Inc. Dies hat zur Folge, dass diese sehr allgemein gehalten sind und auf die spezielle Thematik dieser einen App, wenn überhaupt, nur sehr am Rande eingehen. Speziell das Thema Gesundheitsdaten findet sich in den Bestimmungen nirgends. Google erklärt darin, dass auch personenbezogene Daten, wie zum Beispiel Name, Adresse, Telefonnummer, Kreditkarten- und Standortdaten, erhoben werden und diese auch außerhalb des Landes des Benutzers gespeichert werden könnten. Zum Speicherort selbst

[19] siehe Abbildung 4.17 und Abbildung 4.18

wird Google in diesem Dokument allerdings nicht konkreter. Somit ist für den Nutzer keinerlei Klarheit gegeben, ob diese Daten nun den Europäischen Wirtschaftsraum verlassen oder nicht. Klar herausgestrichen wird die Möglichkeit, die Daten mit erhobenen Daten aus anderen Google-Diensten zu verknüpfen. Welche damit allerdings gemeint sind oder ob dies für alle Dienste gilt, bleibt offen. Man stellt in weiterer Folge klar, dass, sofern die Daten für andere Zwecke als die bisher erklärten genutzt werden sollen, eine eindeutige Einwilligung der Benutzer eingeholt werden wird. Google selbst legt sich für die Weitergabe von personenbezogenen Daten eine Art Generalverbot auf. Dies ist allerdings nur auf den ersten Blick ein echter Schutz, da das Unternehmen direkt im Anschluss eine Aufzählung von Ausnahmen anführt. Einerseits verspricht Google eine ausdrückliche Einwilligung des Nutzers einzuholen, bevor diese Daten weitergegeben werden können, allerdings bleibt auch in diesem Punkt die Bestimmung absolut unkonkret. Andererseits gibt es einen noch viel alarmierenderen Punkt. Google räumt sich nämlich die vorbehaltlose Weitergabe dieser personenbezogenen Daten an von ihm gewählte Partnerunternehmen ein. Diese sollen zwar unter der Aufsicht von Google arbeiten und die Weisungen sowie Googles Datenschutzbestimmungen befolgen, allerdings kann dies realistischerweise kein Unternehmen der Welt garantieren. Vor allem unter dem Aspekt der Sanktionierbarkeit von Verstößen wirkt dieser Absatz noch um einiges schwerer als ohnehin.

Der Installationsprozess selbst entfällt ab der Android Version 5.0, da Google Fit bereits vorinstalliert, allerdings bis zum erstmaligen Starten der App nicht aktiviert ist. Die Zustimmung zu den Zugriffsrechten entfällt dadurch auch. Die App räumt sich allerdings keinerlei Rechte ein, welche nicht für den Betrieb ihrer Funktionen notwendig wäre. [20]

Das Benutzerkonto ist zwangsläufig das ohnehin vorhandene Google-Konto. Beim ersten Starten der App wird man aufgefordert, die Nutzungs- und Datenschutzbestimmungen explizit zu bestätigen und diesen zuzustimmen. Diese sind keinesfalls versteckt, sondern mit einem gut lesbaren Link gekennzeichnet. [21] Danach wird nochmals darauf hingewiesen, dass die Daten, welche Google Fit verarbeitet, auf allen Geräten, sprich Notebook, Tablet, Smartwatch und Smartphone, mittels diesem Benutzerkonto abgerufen werden können. Dies streicht für den nicht versierten Benutzer allerdings viel zu wenig heraus, dass alle Daten damit unweigerlich in die Cloud wandern. Es fehlt auch die Möglichkeit, Letzteres zu unterbinden. [22] Im nächsten Schritt weist die App explizit darauf hin, dass sie auf Daten von Körper- und Bewegungssensoren sowie Standortdaten zugreifen möchte und fordert die Einwilligung des Benutzers ein. [23]

Der wohl größte Unterschied von Google Fit zu anderen Fitness Apps liegt darin begründet, dass Google Fit immer aktiv ist. Es will den ganzen Tag des Benutzers aufzeichnen, jeden Schritt und jede Bewegung. Es will sozusagen den klassischen Schrittzähler mit ersetzen. Dies spiegelt sich auch direkt im Startbildschirm der App wieder. Dort findet man eine schnelle Übersicht über

[20] siehe Abbildung 4.20
[21] siehe Abbildung 4.21
[22] siehe Abbildung 4.22
[23] siehe Abbildung 4.23

seine am heutigen Tag zurückgelegten Schritte bzw. wie viele Minuten man heute schon gegangen ist. [24] Zusätzlich können andere Aktivitäten manuell nachträglich hinzugefügt werden. Hier ist die Sportart aus einer sehr langen Liste frei wählbar. [25] Außerdem kann man sein Gewicht immer wieder mitschreiben. Somit übernimmt Google Fit auch direkt die Funktion eines Körpergewichts-Tagebuch und bringt diese Daten im späteren Verlauf in Kombination mit den sportlichen Aktivitäten. [26]

Speziell Pulsmessgeräte, wie sie in Smartwatches oft integriert sind, können von Google Fit ausgewertet werden. Diese Daten speichert die App und bringt sie in Kombination mit den übrigen erfassten Daten.

Die erfassten Daten sind schnell aufgezählt. Es handelt sich um Standort- sowie Bewegungsdaten. Dazu kommen noch Gesundheitsdaten, wie das Gewicht und der Puls des Benutzers, sofern dieser ein Pulsmessgerät verbunden hat. Die Personalisierbarkeit ergibt sich durch die zwangsweise Verwendung des Google Accounts. Somit ergibt sich ein Gesamtbild von personenbezogenen sensiblen Daten, welche Gesundheitsdaten beinhalten.

Die Konzeption der Datenschutzverträge ist großteils einwandfrei. Eine Nutzung der App ist ohne vorheriges eindeutiges Akzeptieren dieser Verträge nicht möglich. Allerdings gleicht die Datenschutzbestimmung selbst eher einer beschwichtigenden Aufzählung von Punkten, die ein Kunde in diesem Zusammenhang gerne liest, als einem rechtsverbindlichem Dokument. Sie kann bestenfalls als gut gemeinte Absichtserklärung gedeutet werden. Darüber hinaus ist sie durch ihre Geltung für den ganzen Konzern derart allgemein gehalten, dass sich eine konkrete Anwendung auf eine einzige App kaum ableiten lässt. Die wenigen Punkte, welche mehr oder weniger konkret deklariert sind, lassen allerdings keine Zweifel offen, dass Google sich alle Rechte einräumt, um die Daten nach seinem Belieben zu verwenden. Es wird immer wieder beteuert, dass die Daten klar dem Benutzer gehören und damit rechtskonform agiert wird. Allerdings ist die Legitimation für die Weitergabe der personenbezogenen Daten an Partnerunternehmen ohne der Einschränkung, an welche Unternehmen bzw. um welche Daten es sich handeln soll, ein klarer „Freifahrtschein“ für Google. Die Rechtskonformität muss aus europäischer Sicht daher sehr kritisch betrachtet werden. Die freiwillige Einwilligung in derartig vage Datenschutzbestimmungen kann nicht ausreichend für eine Rechtskonformität sein.

[24] siehe Abbildung 4.24
[25] siehe Abbildung 4.25
[26] siehe Abbildung 4.26

Abbildung 4.17: Google Fit - 1 - Installation
Google Fit [43]

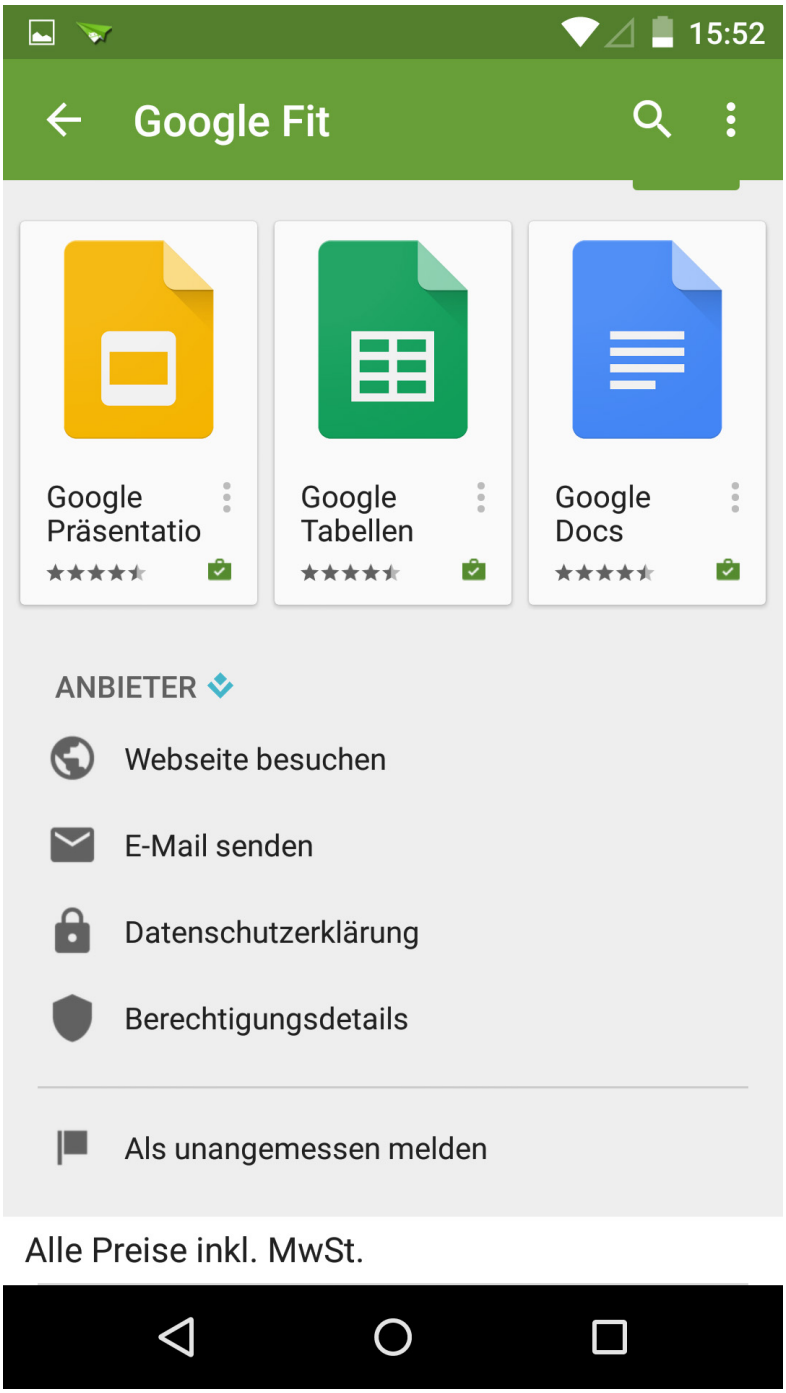


Abbildung 4.18: Google Fit - 2 - Installation
Google Fit [43]

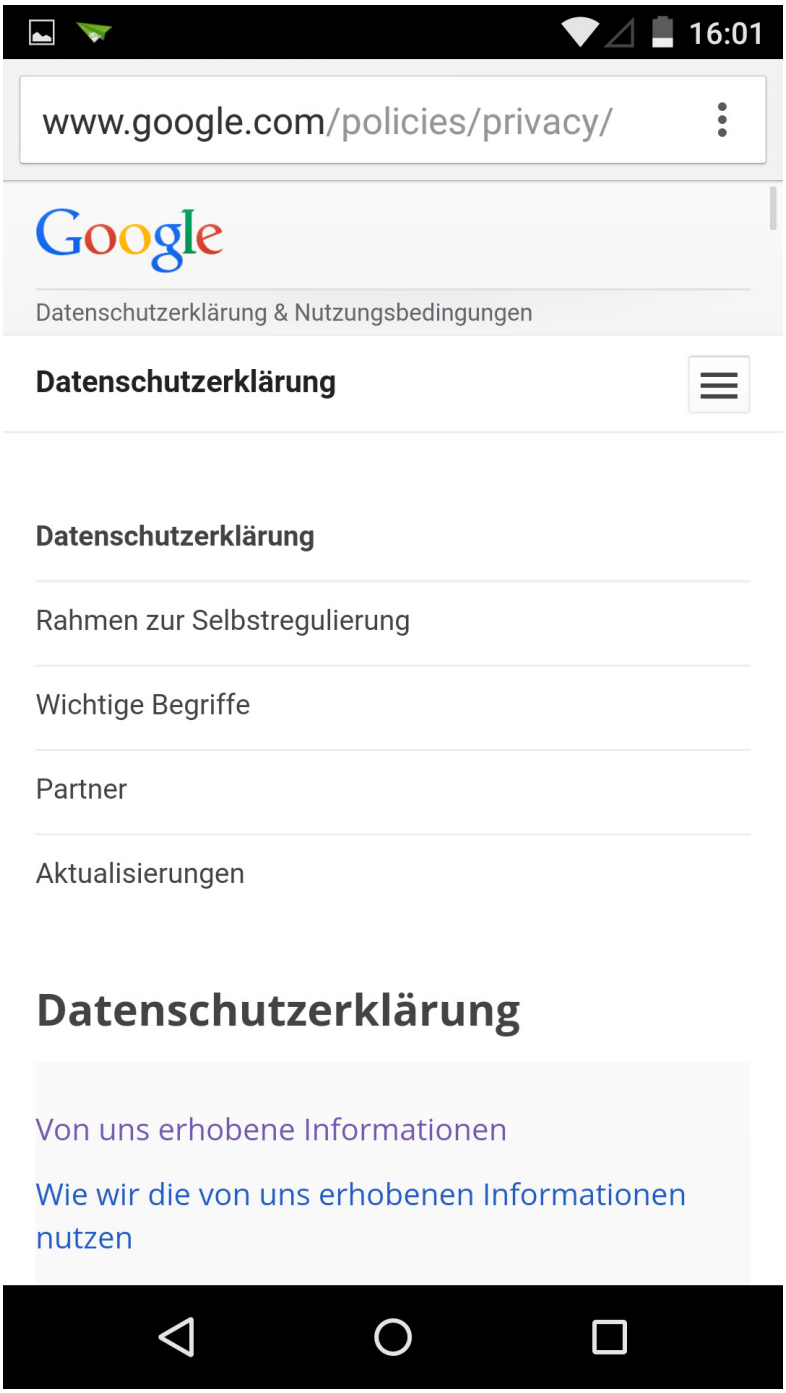


Abbildung 4.19: Google Fit - 3 - Datenschutzbestimmungen
Google Fit [43]

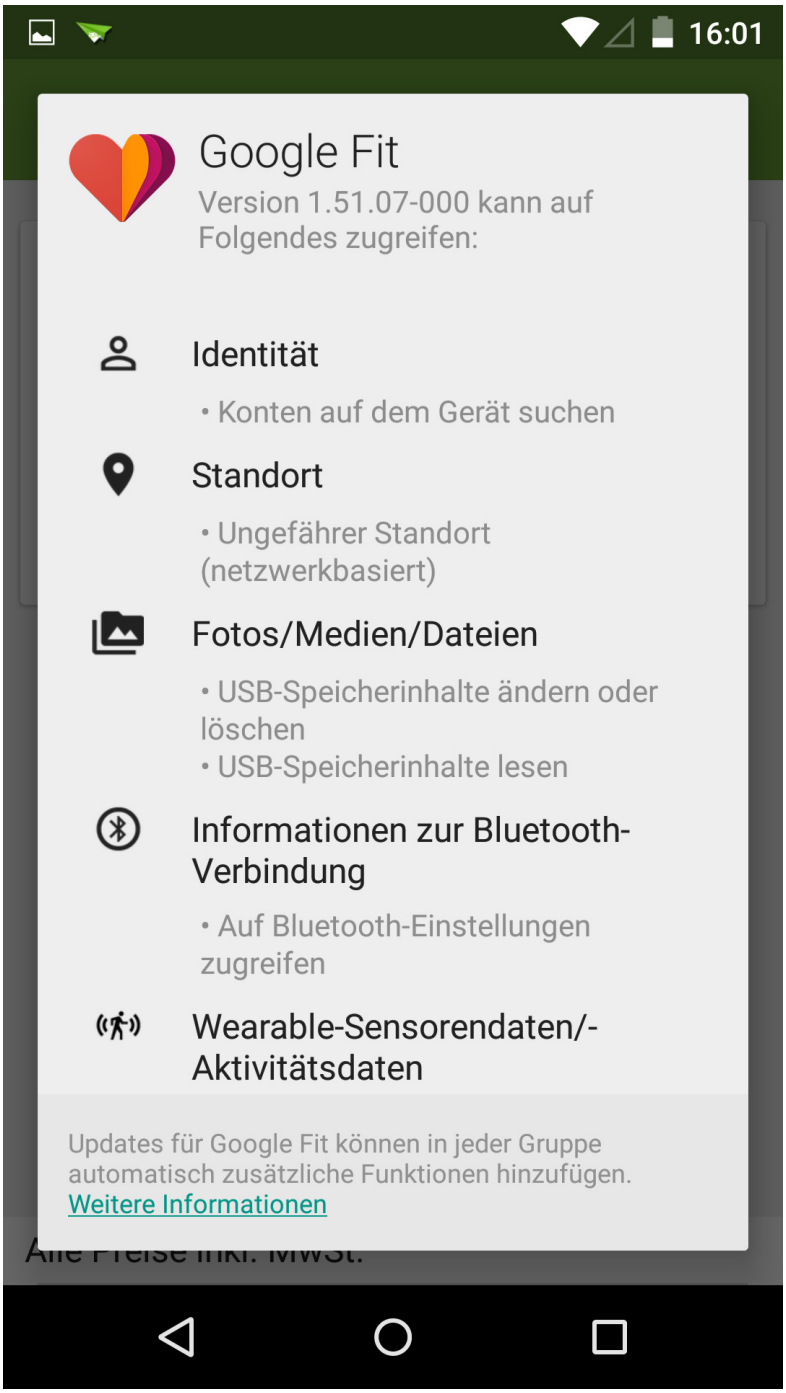


Abbildung 4.20: Google Fit - 4 - Berechtigungen
Google Fit [43]

Abbildung 4.21: Google Fit - 5 - Benutzerkonto
Google Fit [43]

Abbildung 4.22: Google Fit - 6 - Einrichtung - Cloud
Google Fit [43]

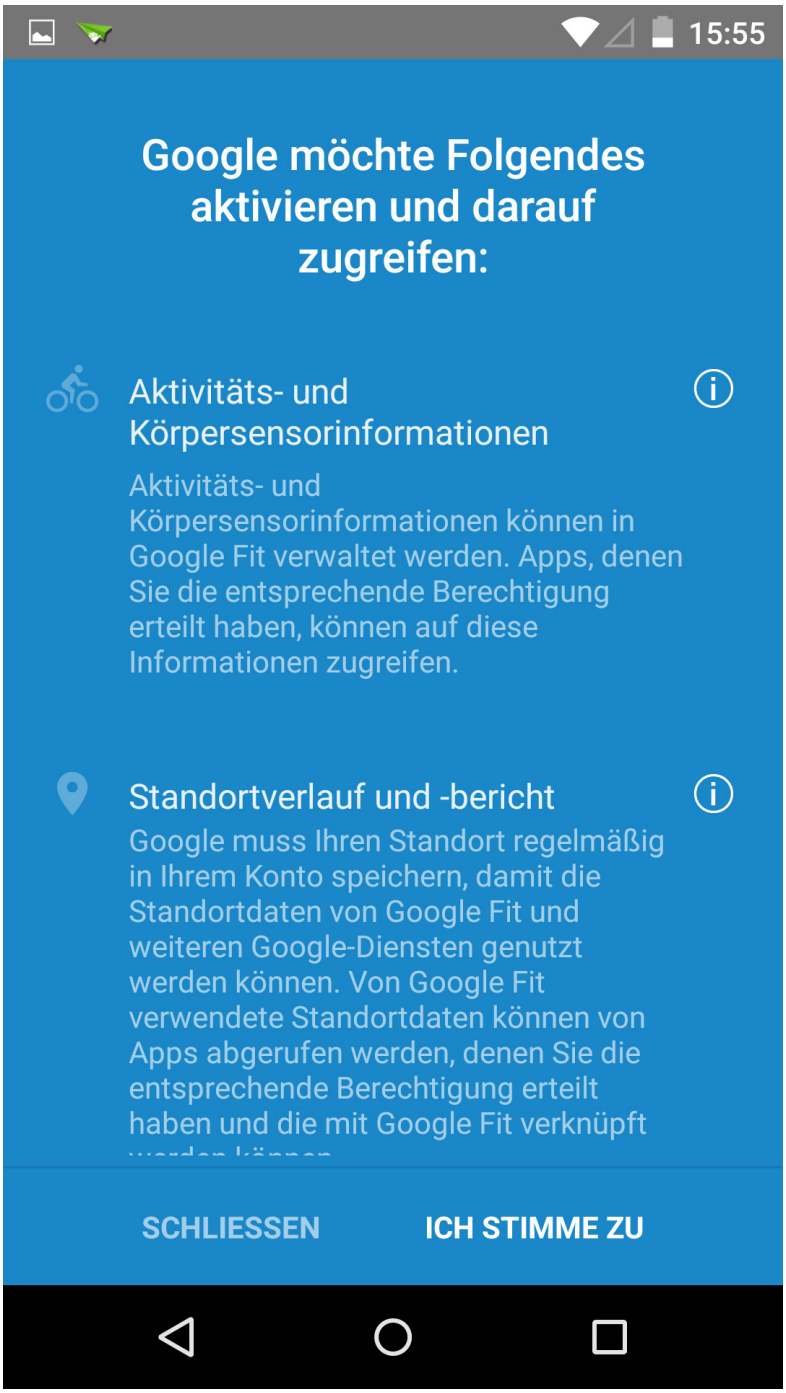


Abbildung 4.23: Google Fit - 7 - Einrichtung - Zustimmung
Google Fit [43]

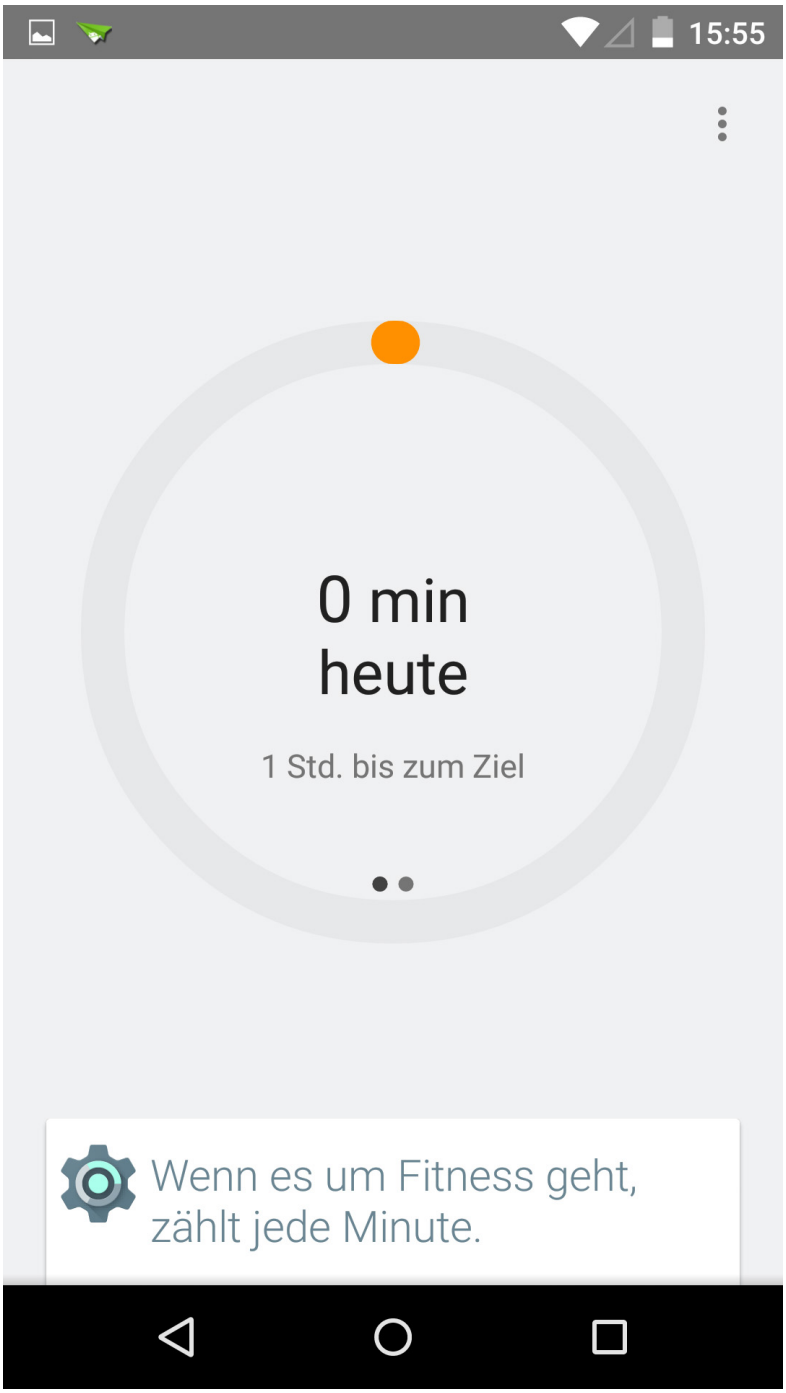


Abbildung 4.24: Google Fit - 8 - Funktionen - Start
Google Fit [43]

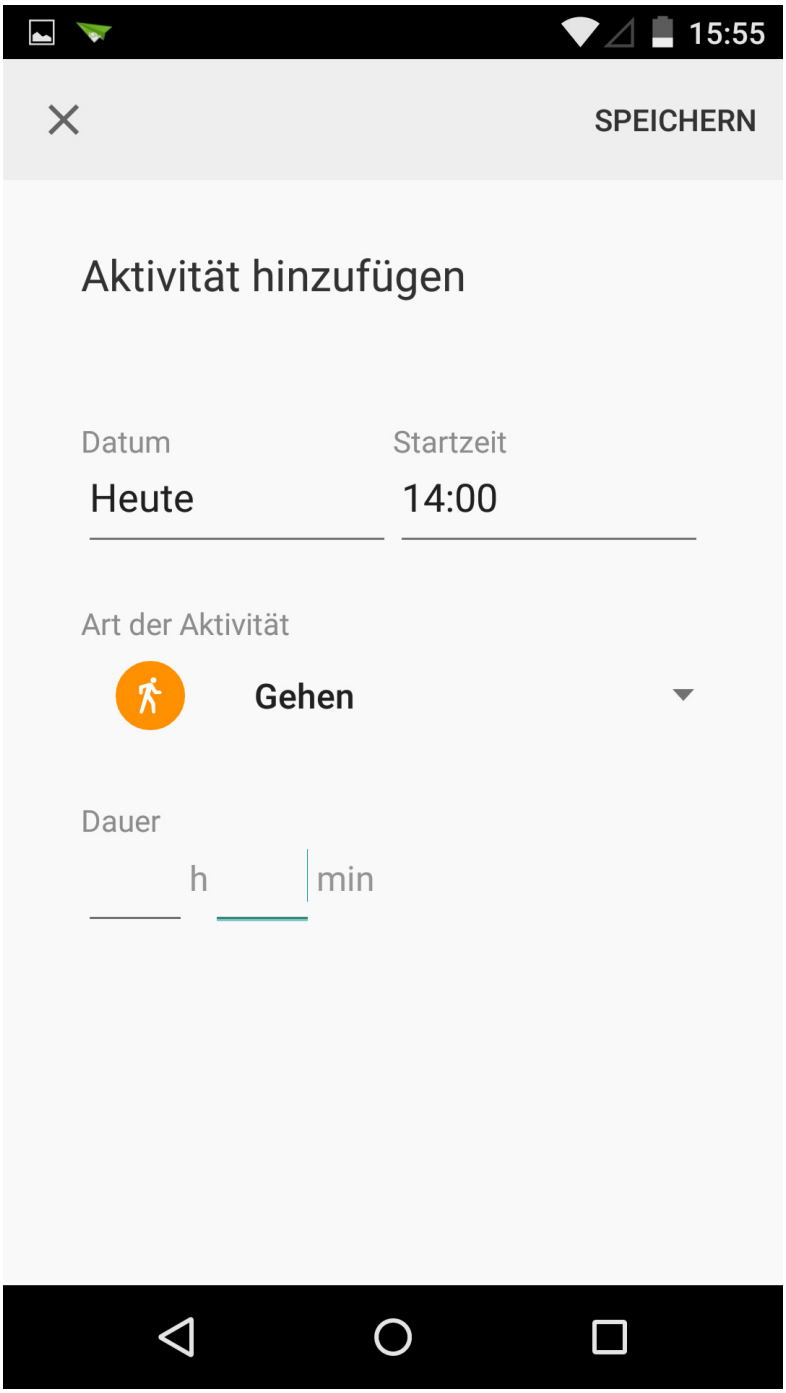


Abbildung 4.25: Google Fit - 9 - Funktionen - Aktivität hinzufügen
Google Fit [43]

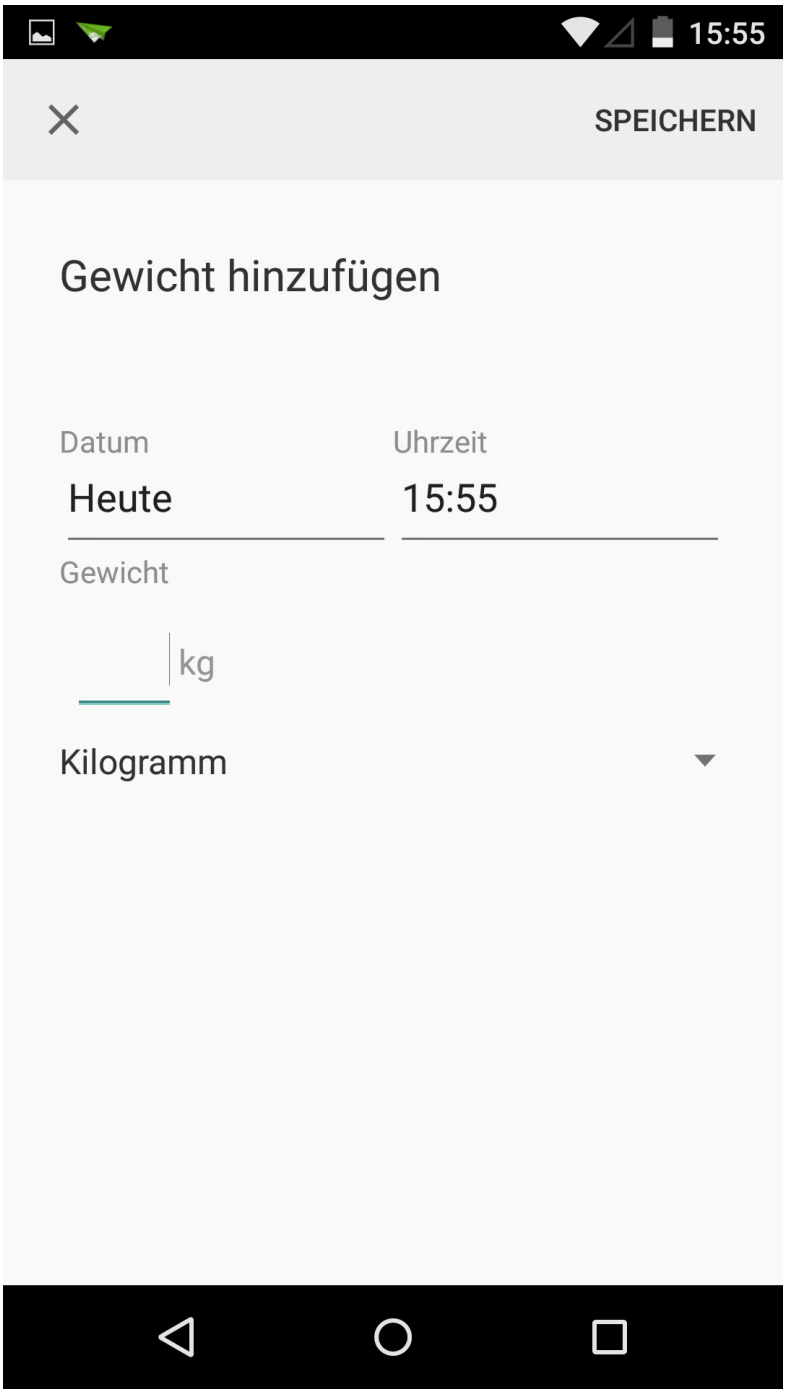


Abbildung 4.26: Google Fit - 10 - Funktionen - Gewicht hinzufügen
Google Fit [43]

Abbildung 4.27: FitNotes Logo
FitNotes - Gym Workout Log [34]

4.4 FitNotes Gym Workout Log

Adresse: https://play.google.com/store/apps/details?id=com.github.jamesgay.fitnotes

Die App Fit Notes wird von einer Privatperson mit dem Namen James Gay entwickelt und kostenlos zur Verfügung gestellt. Dementsprechend findet sich keine Anschrift des Entwicklers im Google Play Store.

Datenschutzbestimmungen sind im Google Play Store keine zu finden ebensowenig wie ein Link auf eine Homepage des Entwicklers. [27]

Die Installation erfolgt wie gewohnt einfach mit einem Klick. Die Berechtigungen der App sind beschränkt auf den Zugriff des Medienspeichers. Dies ist für diese App absolut vertretbar und verständlich. [28]

[27] siehe Abbildung 4.28 und Abbildung 4.29
[28] siehe Abbildung 4.30

Die App verlangt kein Benutzerkonto oder Login. Man wird beim ersten Start der App gefragt, ob man das metrische oder das angloamerikanisches Maßsystem bevorzugt. [29] Darüber hinaus erfordert die App keine weitere Einrichtung.

Die Funktionen erinnern an ein Tage- bzw. Logbuch, welches auf das Mitschreiben von Trainingseinheiten spezialisiert ist. Der Benutzer hat die Möglichkeit, alle Trainingseinheiten sehr granular zu protokollieren. Zum Beispiel gibt es für das Gewichtstraining die Option, jede einzelne Übung mit ihren einzelnen Sätzen, Gewichten und Wiederholungen exakt zu erfassen. Beim Hinzufügen eines neuen Datensatzes steht in der App bereits eine vorgefertigte Liste aus Übungen zur Auswahl bereit. Darüber hinaus kann das eigene Gewicht mitgeschrieben und es können grafische Statistiken erstellt werden.

Es werden keine externen Geräte von Fit Notes unterstützt. Somit werden auch keine zusätzlichen Daten erhoben.

Die erfassten Daten beschränken sich auf die Daten, welche der Benutzer manuell und explizit eingibt. Somit ergeben sich lediglich Daten, welche die Art der Fitness-Übung sowie das Gewicht und die Wiederholungen in Kombination mit einem Zeitstempel beschreiben. Darüber hinaus kann das Körpergewicht in Kombination mit einem Zeitstempel erfasst werden. Ein echter Personenbezug kann nicht hergestellt werden, da kein Benutzerkonto erforderlich ist und die Daten das Smartphone nie verlassen.

Die Rechtskonformität ist alleine schon durch den Umstand gegeben, dass die Daten das Smartphone des Benutzers nicht verlassen und somit auch nie übertragen oder veröffentlicht werden.

[29] siehe Abbildung 4.31

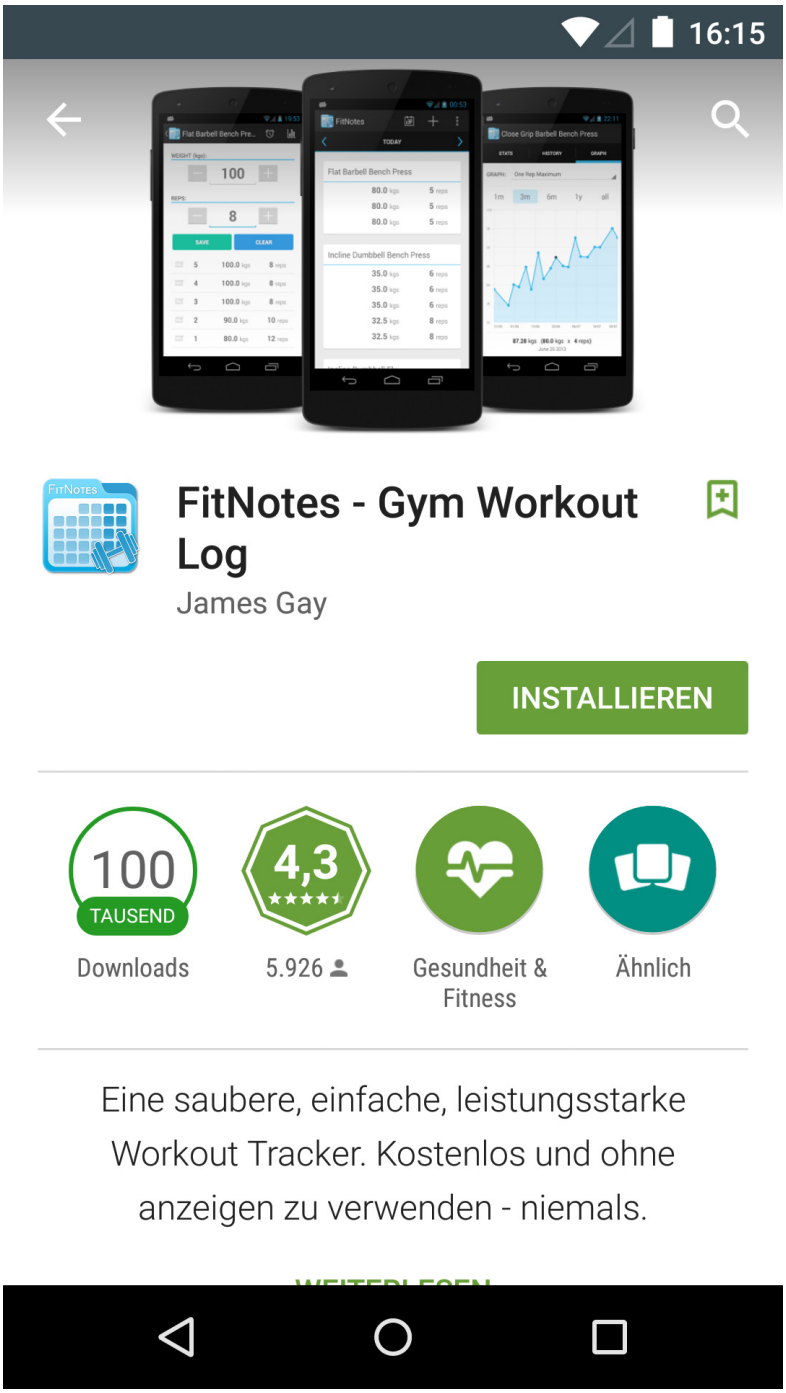


Abbildung 4.28: FitNotes - 1 - Installation
FitNotes - Gym Workout Log [34]

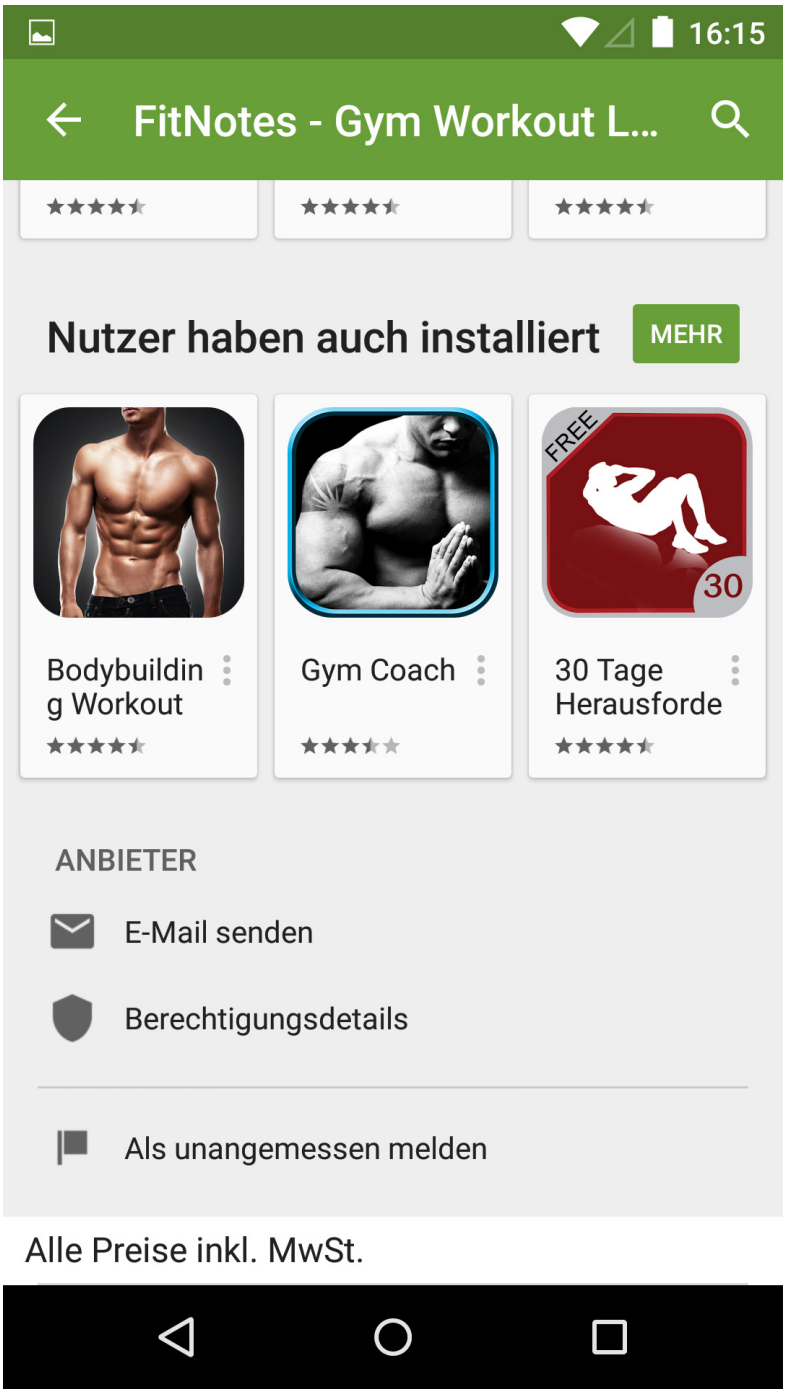


Abbildung 4.29: FitNotes - 2 - Installation
FitNotes - Gym Workout Log [34]

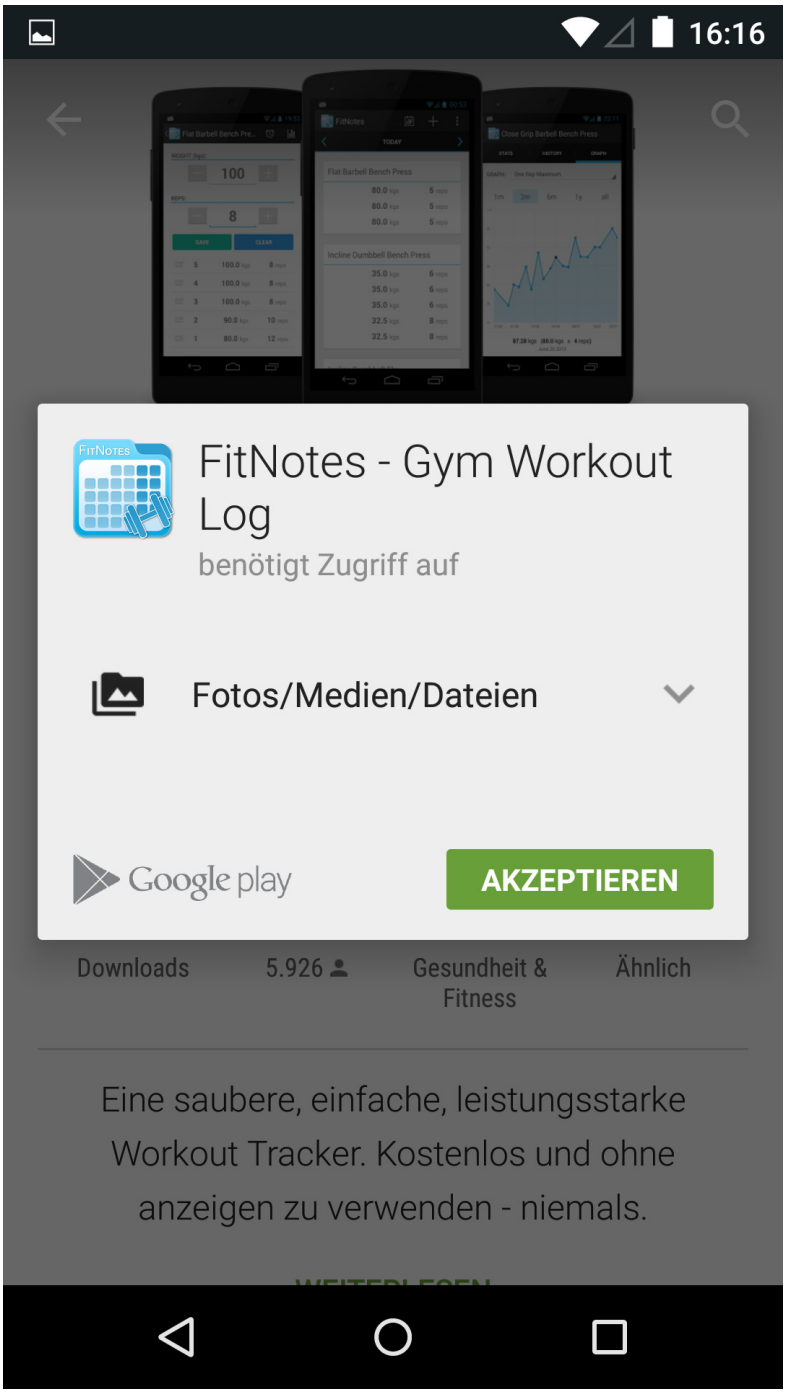


Abbildung 4.30: FitNotes - 3 - Berechtigungen
FitNotes - Gym Workout Log [34]

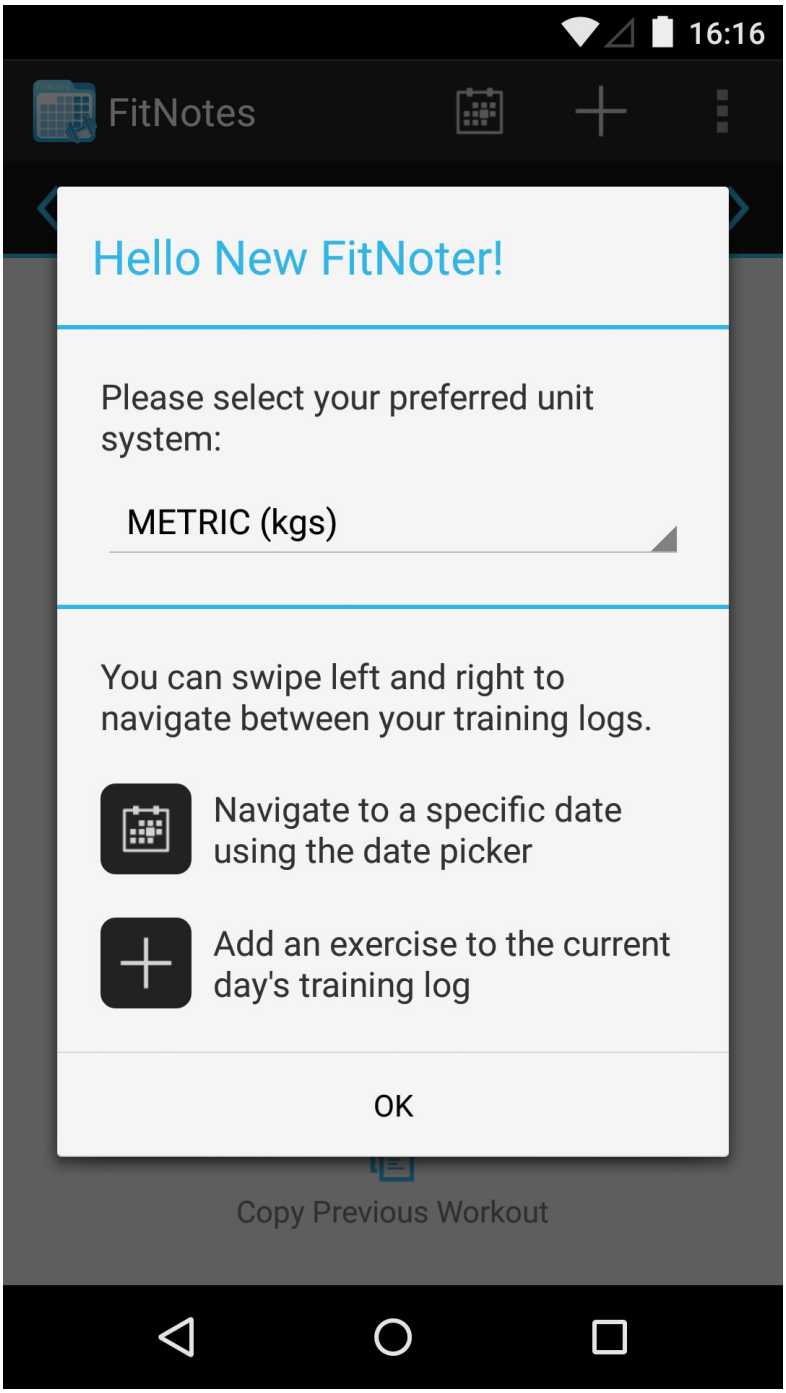


Abbildung 4.31: FitNotes - 4 - Einrichtung
FitNotes - Gym Workout Log [34]

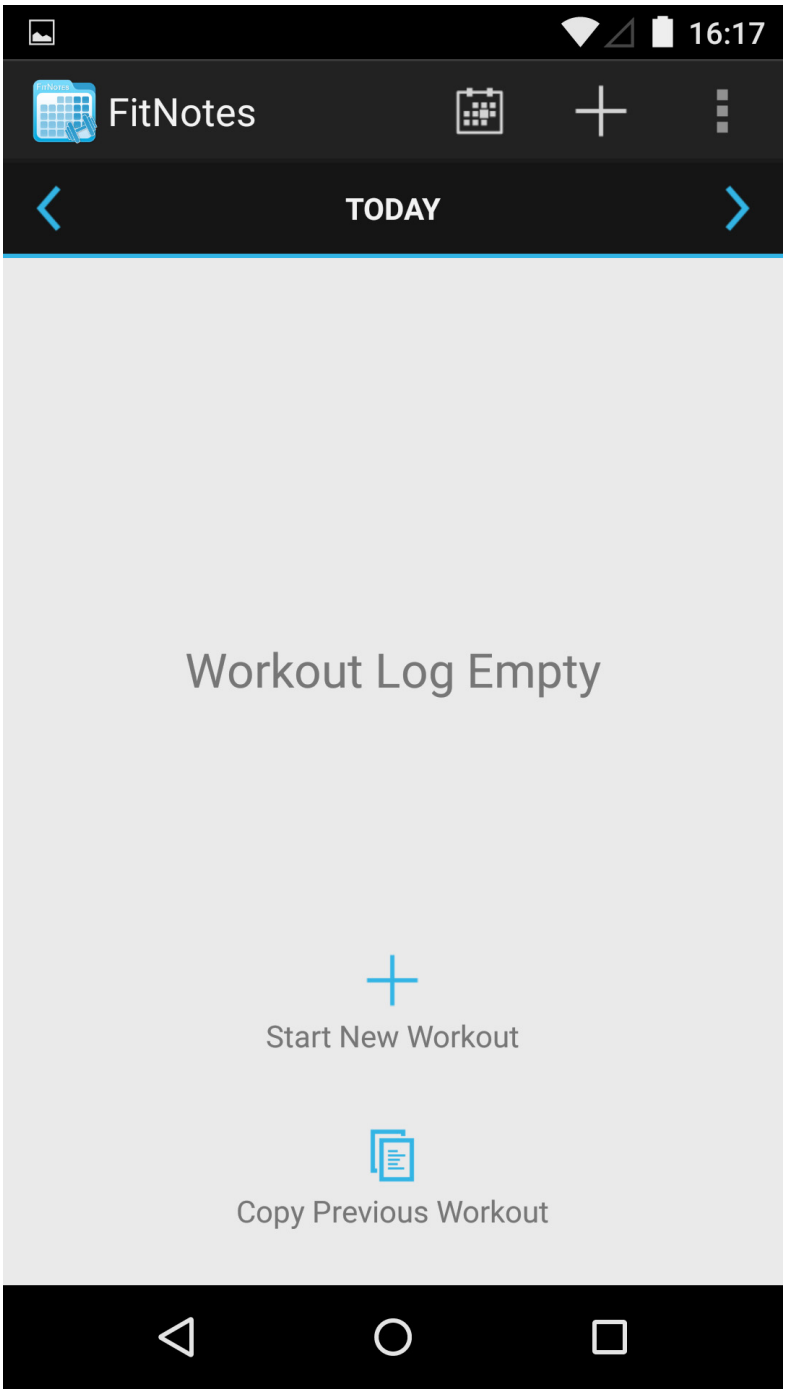


Abbildung 4.32: FitNotes - 5 - Funktionen - Start
FitNotes - Gym Workout Log [34]

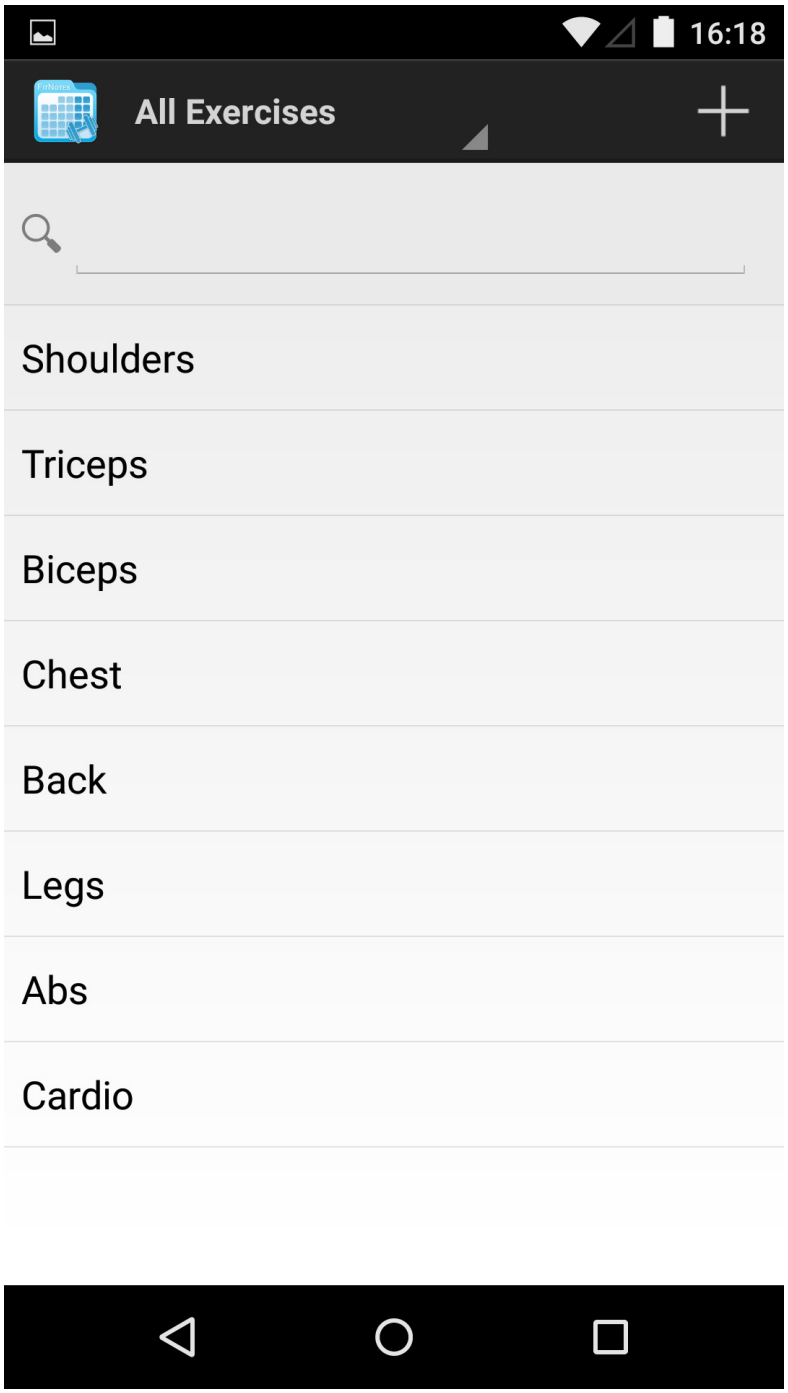


Abbildung 4.33: FitNotes - 6 - Funktionen - Aktivität hinzufügen
FitNotes - Gym Workout Log [34]

Abbildung 4.34: Endomondo Logo
Endomondo Running Cycling Walk [31]

4.5 Endomondo

Adresse: https://play.google.com/store/apps/details?id=com.endomondo.android

Als Entwickler der Endomondo App zeichnet die Firma Endomondo ApS aus Kopenhagen in Dänemark. Diese Information ist auf der Webseite des Herstellers keinesfalls einfach zu finden, sondern lediglich in den Nutzungsbestimmungen verzeichnet. Eine durchaus interessante Entdeckung ist allerdings die Tatsache, dass bei einem Nachverfolgen der Internetadresse des Entwicklers am Ende kein dänischer Serverstandort antwortet, sondern vielmehr einer der europäisch zugeordneten Cluster der Amazon-Cloud, welche geographisch an der Ostküste der USA betrieben werden. Sollte dies auch der Speicherort der Nutzerdaten sein, könnte dies durchaus ein Problem im Hinblick auf den Datenschutz bilden. Entgegen dieser Nachverfolgung findet sich in den Datenschutzbestimmungen die Deklaration, dass alle Benutzerdaten auf Servern innerhalb der EU lagern.

Die Datenschutzbestimmungen sind wie gewohnt über einen Link am Ende der Installations-

seite der App im Google Play Store aufrufbar. [30] Ungewöhnlich ist allerdings die Tatsache, dass, trotz der Spracheinstellung Deutsch, welche sich auch in den Menüs korrekt widerspiegelt, die Bestimmungen in Englisch dargestellt werden. [31] Ein Anzeigefehler des mobilen Webbrowsers ist auszuschließen, da sich bei einem Test auf einem normalen Computer das gleiche Bild gezeigt hat. Die Bestimmungen selbst stellen direkt anfangs fest, dass eine Reihe von personenbezogenen Daten wie etwa Name, E-Mail-Adresse, Anschrift, Geburtsdatum, Geschlecht, sportliches Interesse, Körpergröße und Körpergewicht für die Durchführung der Leistungen erhoben werden. Des Weiteren können Daten wie ein exakter Standortverlauf und die Herzfrequenz während der diversen sportlichen Tätigkeiten aufgezeichnet werden. Der Benutzer erklärt sich auch damit einverstanden, dass Endomondo diverse persönliche Informationen im Zuge seiner Tätigkeiten öffentlich zugänglich macht. Die Bestimmungen stellen darüber hinaus klar, dass viele der Informationen grundsätzlich die Einstellung „öffentlich“ tragen, sofern der Benutzer dies in der Konfiguration nicht explizit manuell ändert. Ein sehr interessanter Punkt ist die Übertragung der persönlichen Daten an Geschäftspartner von Endomondo. In erster Linie stellen die Bestimmungen klar, dass niemals Benutzerdaten an Partner ohne die Zustimmung des Nutzers übertragen werden. Allerdings räumt sich das Unternehmen einige Ausnahmen ein, welche sich nicht nur auf die Durchführung der Leistungen beschränken, sondern auch auf die Marktanalyse und Werbung ausdehnen. Eine Einschränkung, welche Daten dazu verwendet werden, fehlt gänzlich. Somit ist nicht auszuschließen, dass ohne Wissen und Zustimmung der Nutzer auch sensible gesundheitsrelevante Daten an durchaus fragwürdige Empfänger, wie zum Beispiel die Werbeindustrie, weitergeleitet werden.

Die Installation funktioniert, wie bei bei Android üblich, mittels eines simplen Klicks im Google Play Store. Die für den Betrieb der App notwendigen Berechtigungen sind umfangreich, aber im Hinblick auf die Funktionen der App vertretbar. [32]

Der erste Start der App vermittelt direkt ein unbehagliches Gefühl im Hinblick auf den Datenschutz. So ist es nicht möglich, das Einrichten eines Benutzerkontos bzw. die Verwendung eines bestehenden Kontos zu überspringen. Zusätzlich ist zu bemerken, dass man lediglich bei einer Neuregistrierung auf die Nutzungsbestimmungen mittels Link hingewiesen wird, auf die Datenschutzbestimmungen allerdings in keiner der möglichen Optionen. Darüber hinaus hat man die Möglichkeit, einen eigenen Endomondo-Account anzulegen oder ein bereits bestehendes Facebook bzw. Google+ Konto zu verwenden. [33]

Die Funktionen der App sind sehr umfangreich. Der Startbildschirm bietet die Möglichkeit, direkt mit einem Training zu beginnen. [34] Bei einer Aktivität werden durchgehend der Standort, die Zeit und die daraus resultierende Bewegungsgeschwindigkeit protokolliert. Weiters kann

[30] siehe Abbildung 4.35 und Abbildung 4.36
[31] siehe Abbildung 4.37
[32] siehe Abbildung 4.39
[33] siehe Abbildung 4.40, Abbildung 4.41 und Abbildung 4.42
[34] siehe Abbildung 4.44

man sich mit Freunden innerhalb der App verbinden, um gemeinsame Aktivitäten zu planen oder sich auszutauschen [35] - ähnlich einem sozialen Netzwerk. Durch die dauernde Protokollierung aller Aktivitäten ist auch ein Verlauf abrufbar. [36] Weitere Funktionen sind kostenpflichtige Trainingspläne [37], die Möglichkeit, sich wöchentliche Ziele, genannt Commitments, zu setzen [38] und seine Freunde zu Wettkämpfen herauszufordern [39]. Alle zurückgelegten Strecken, unabhängig von der Sportart, können gespeichert und mit Freunden oder „der ganzen Welt“ geteilt werden. Somit ist es möglich, sich beispielsweise gute Laufstrecken in der Nähe anzeigen zu lassen. [40]

Durch die Unterstützung von Herzfrequenzmessgeräten bietet sich die Möglichkeit, diese Gesundheitsdaten mit den Aktivitätsdaten zu kombinieren.

Die Menge der erfassten Daten ist keinesfalls gering. Durch den Benutzerkontenzwang ergeben sich eindeutig personenbezogene Daten im Bereich des Namens und der E-Mail-Adresse. Je nach Kontowahl können darüber hinaus auch das Geburtsdatum, die Körpergröße und das Körpergewicht entweder automatisch erfasst oder manuell hinzugefügt werden. [41] Durch die Aufzeichnung der Aktivitäten ergibt sich darüber hinaus ein vollständiges Bewegungsprofil während dieser Tätigkeiten, inklusive exaktem Ort, Zeitpunkt und Bewegungsgeschwindigkeit. Durch die Angabe, welche Sportart ausgeführt wird, lässt sich in Kombination mit einem Herzfrequenzmessgerät ein Gesundheitsstatus kalkulieren. Daraus ergeben sich sensible gesundheitsrelevante Daten.

Bevor auf die Rechtskonformität auf Grundlage der Datenschutzbestimmungen eingegangen wird, ist ein weiteres Thema zu behandeln: Die App bietet durch seinen Kontenzwang und die integrierten Social-Media-Funktionen ein durchaus großes Potential, Informationen unwissentlich und ungewollt an andere Personen zu verbreiten. Dieser Umstand verstärkt sich dadurch, dass die Privatsphäreeinstellungen der App in fast allen Punkten ursprünglich auf „öffentlich“ stehen. Selbst Informationen wie der Geburtstag, die Körpergröße oder die Dauer und Geschwindigkeit der aufgezeichneten Aktivitäten sind ohne Eingreifen des Benutzers für das komplette Netzwerk sichtbar. [42] Durch diese Situation ergibt sich noch ein weiterer Problempunkt: nämlich die ungefragte vollständige Synchronisation aller Daten auf die Server der App. Dies wird ohne explizite Einwilligung oder Information der Benutzer durchgeführt und lässt sich auch nicht deaktivieren. Trotz eines offenbaren Unternehmenssitzes innerhalb der EU sowie der Deklaration in den Datenschutzbestimmungen, dass alle Kundendaten ausschließlich im europäischen Inland gespeichert werden, ist die Optik ein wenig verzerrt. Einerseits ergibt eine Nachverfolgung der Internetadresse eine Antwort eines Servers in den USA, andererseits existieren die Bestimmun-

[35] siehe Abbildung 4.45
[36] siehe Abbildung 4.46
[37] siehe Abbildung 4.47
[38] siehe Abbildung 4.48
[39] siehe Abbildung 4.49
[40] siehe Abbildung 4.50
[41] siehe Abbildung 4.51
[42] siehe Abbildung 4.52, Abbildung 4.53 und Abbildung 4.54

gen lediglich in der Sprache Englisch, obwohl die App selbst in viele Sprachen übersetzt wurde. Darüber hinaus räumt sich das Unternehmen in den Datenschutzbestimmungen ein fast uneingeschränktes Sammel- und Weitergaberecht jeglicher Daten seiner Nutzer ein. Weder findet sich eine echte Einschränkung auf die Datenqualität noch -quantität noch den Empfänger. Somit ist es dem Unternehmen möglich, laut den Datenschutzbestimmungen auch sensible Gesundheitsdaten an die Werbeindustrie weiterzugeben. Dies alles passiert, gleich wie die automatische und zwangsweise Übertragung aller Daten auf deren Server, ohne Wissen und zusätzliche Information des Benutzers. Die Rechtskonformität kann alleine schon durch das Fehlen einer in die Landessprache übersetzten Datenschutzbestimmung keinesfalls einwandfrei festgestellt werden. Darüber hinaus gibt es einige durchaus bedenkliche Punkte im Umgang mit sensiblen Daten.

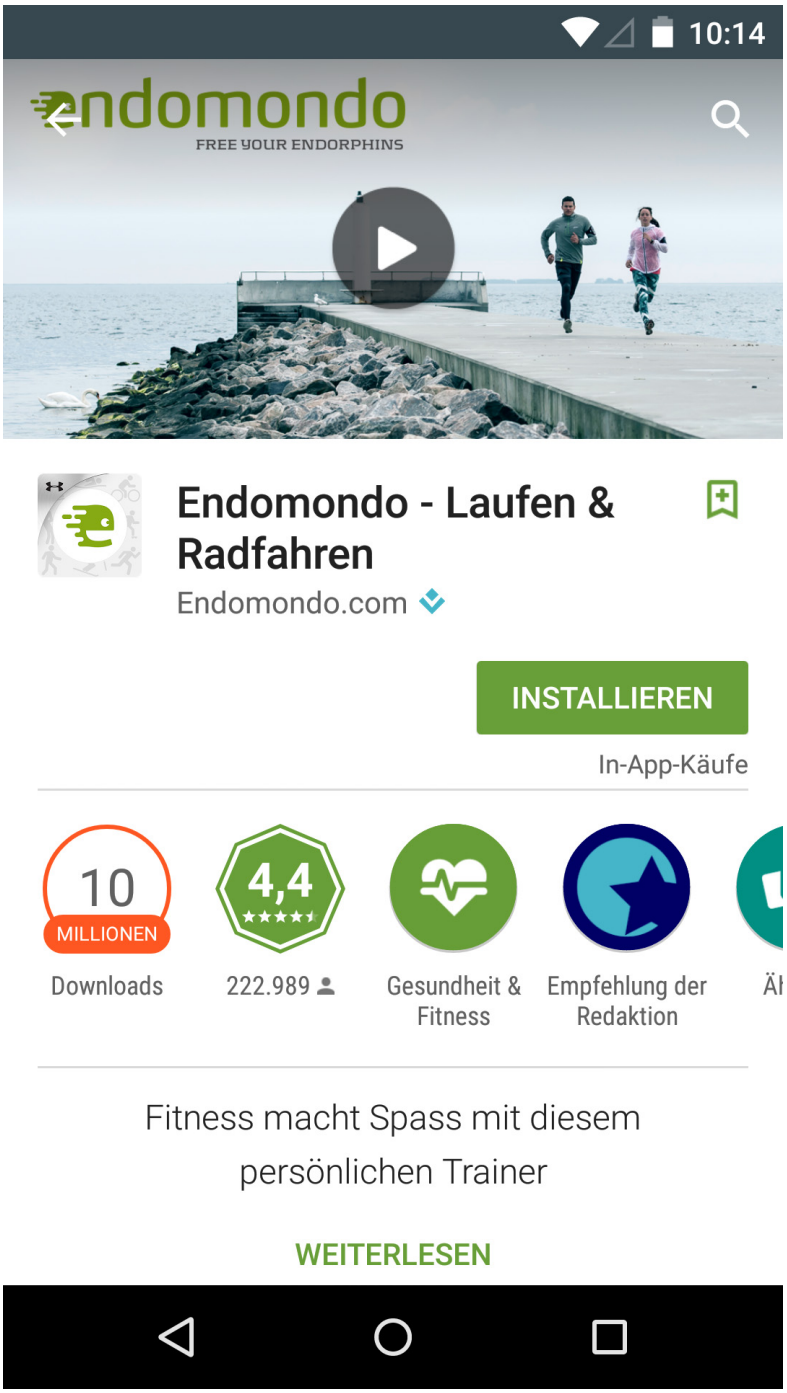


Abbildung 4.35: Endomondo - 1 - Installation
Endomondo Running Cycling Walk [31]

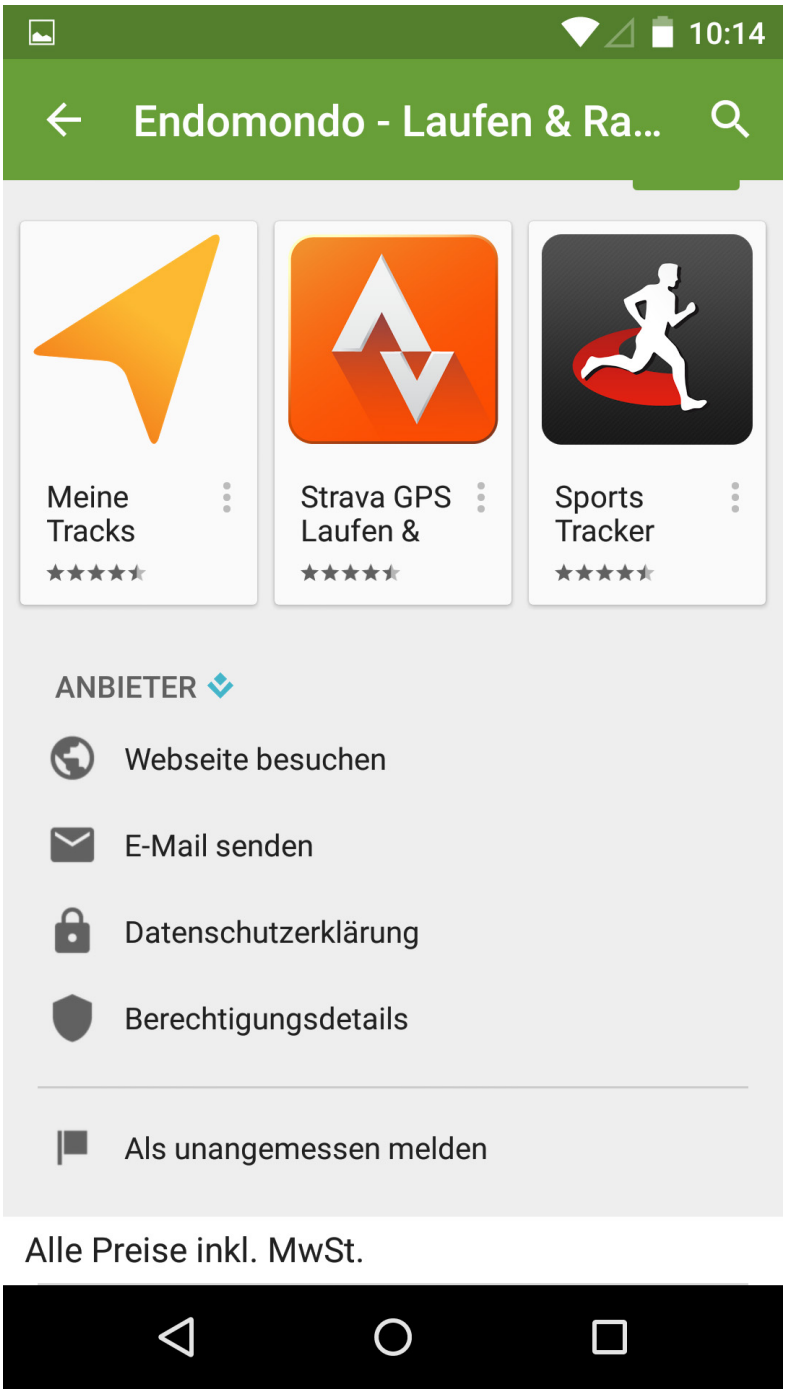


Abbildung 4.36: Endomondo - 2 - Installation
Endomondo Running Cycling Walk [31]

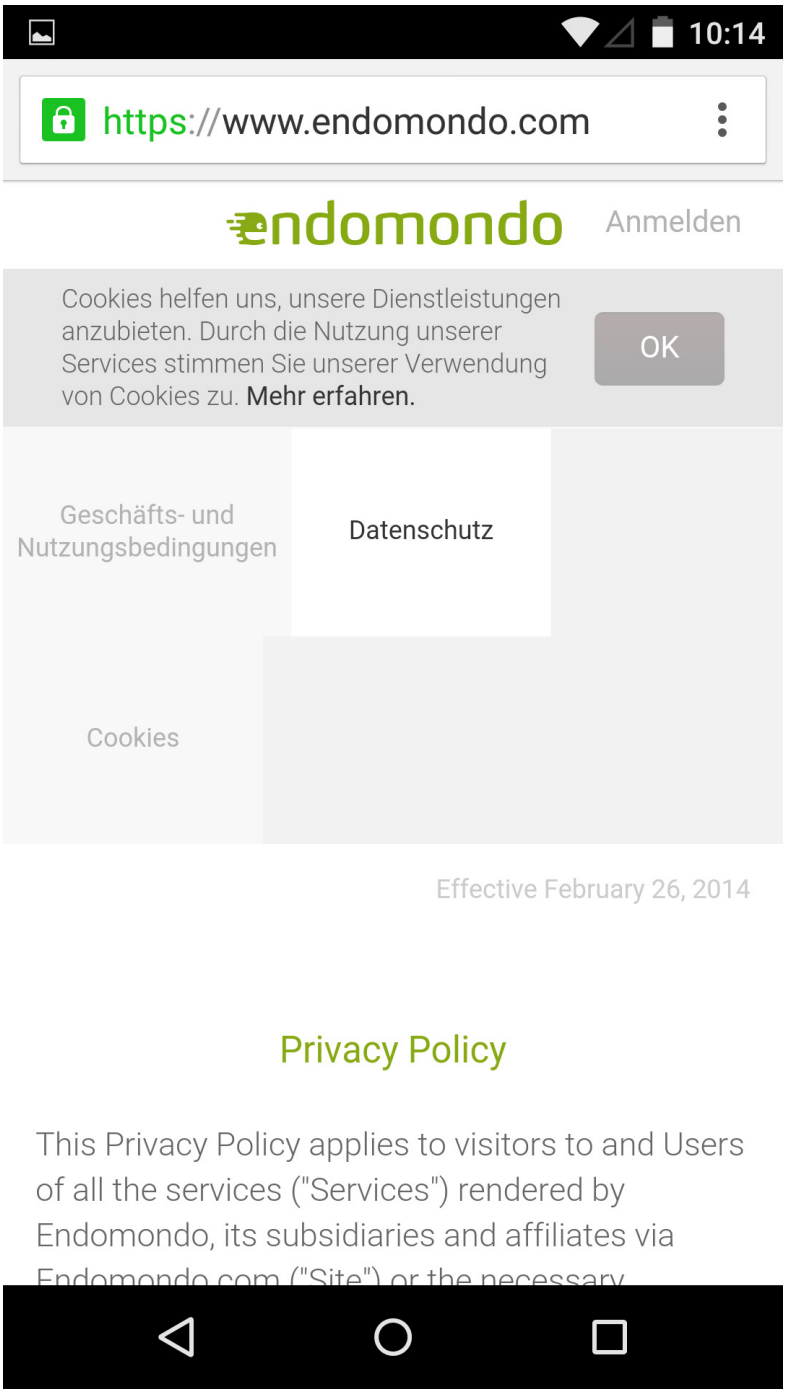


Abbildung 4.37: Endomondo - 3 - Datenschutzbestimmungen
Endomondo Running Cycling Walk [31]

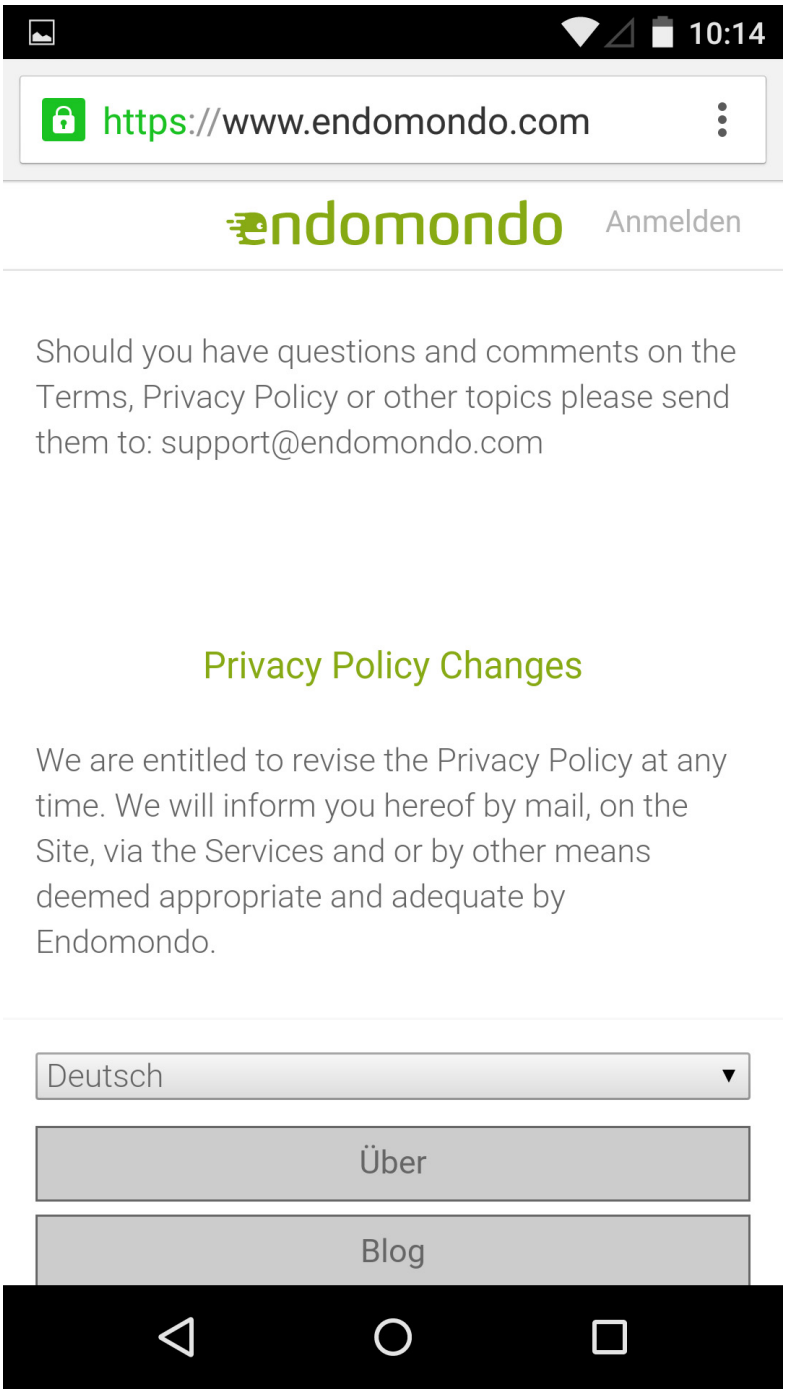


Abbildung 4.38: Endomondo - 4 - Datenschutzbestimmungen
Endomondo Running Cycling Walk [31]

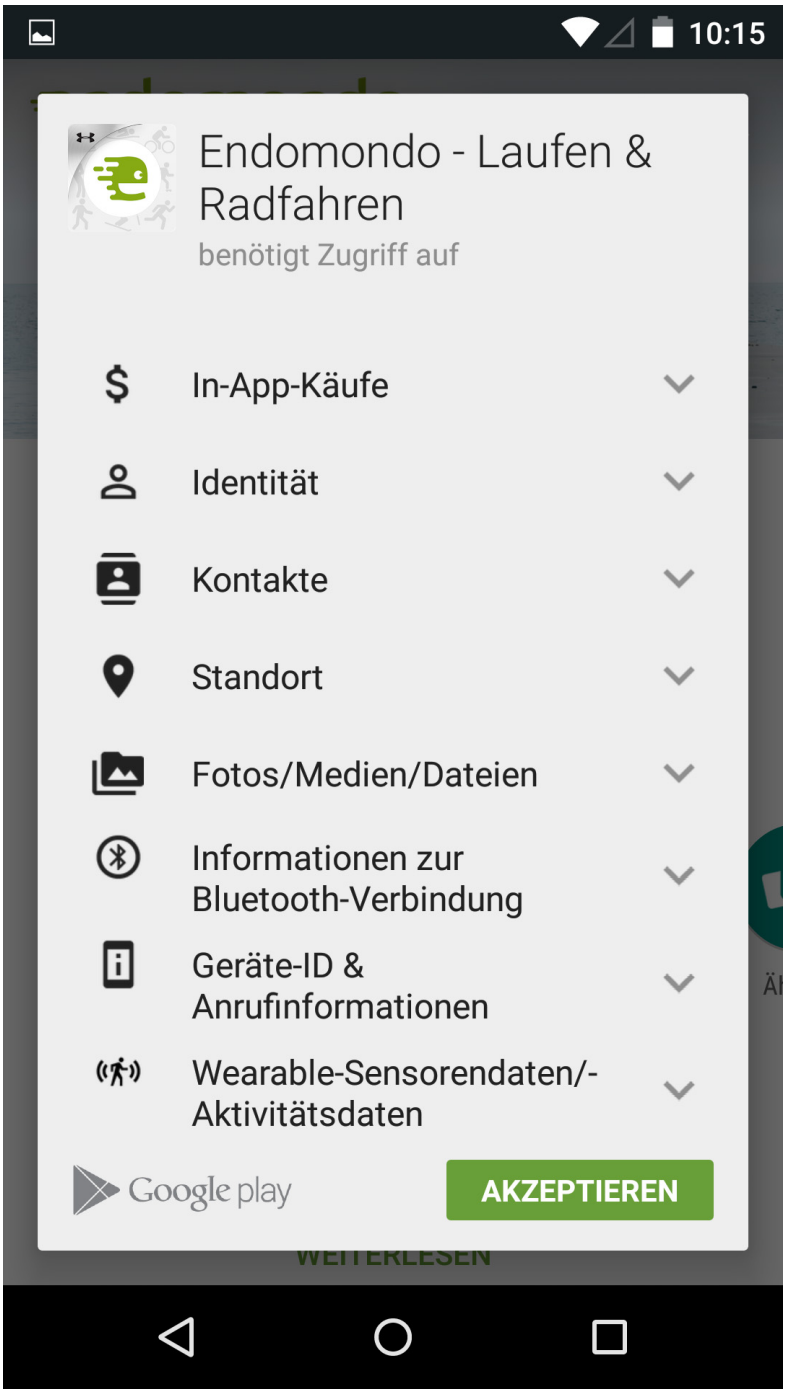


Abbildung 4.39: Endomondo - 5 - Berechtigungen
Endomondo Running Cycling Walk [31]

Abbildung 4.40: Endomondo - 6 - Benutzerkonto
Endomondo Running Cycling Walk [31]

Abbildung 4.41: Endomondo - 7 - Benutzerkonto
Endomondo Running Cycling Walk [31]

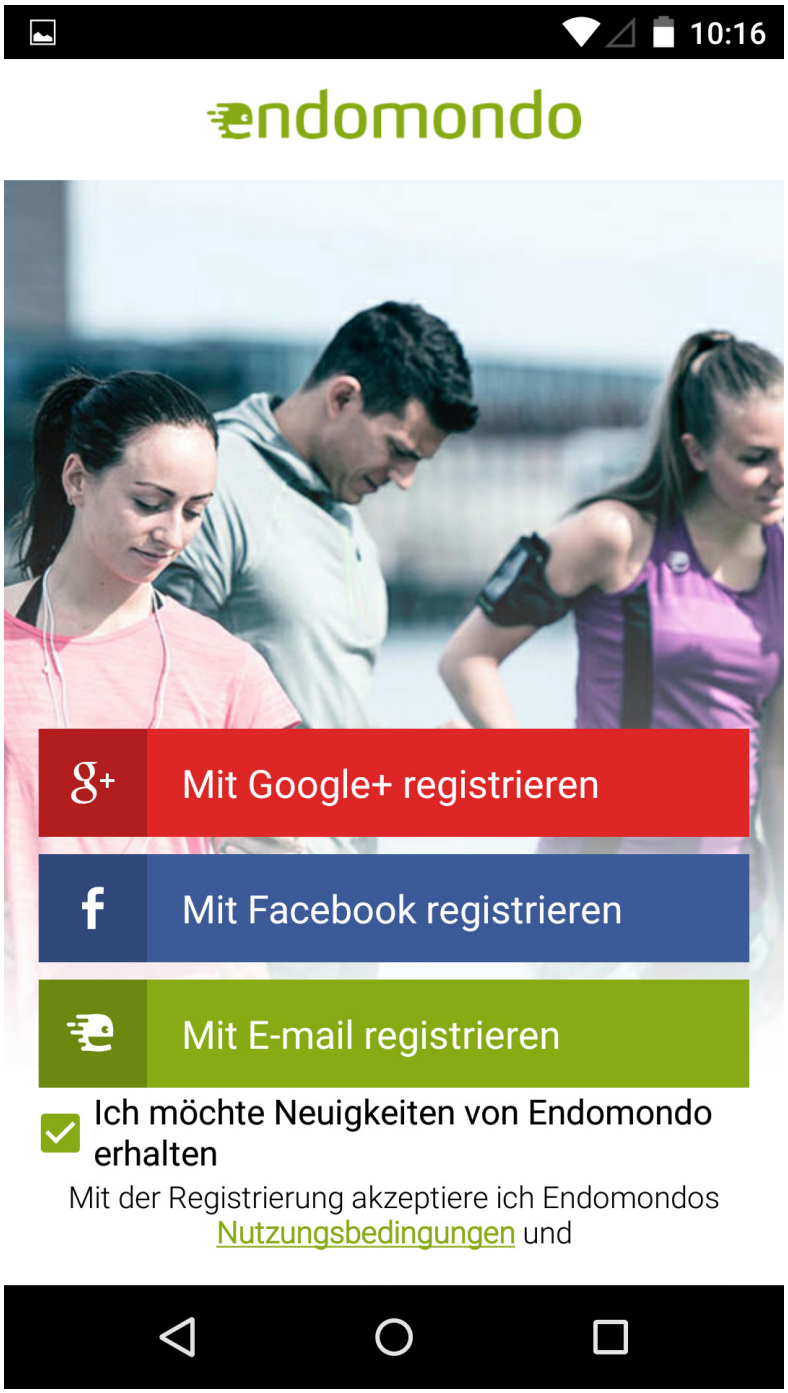


Abbildung 4.42: Endomondo - 8 - Benutzerkonto
Endomondo Running Cycling Walk [31]

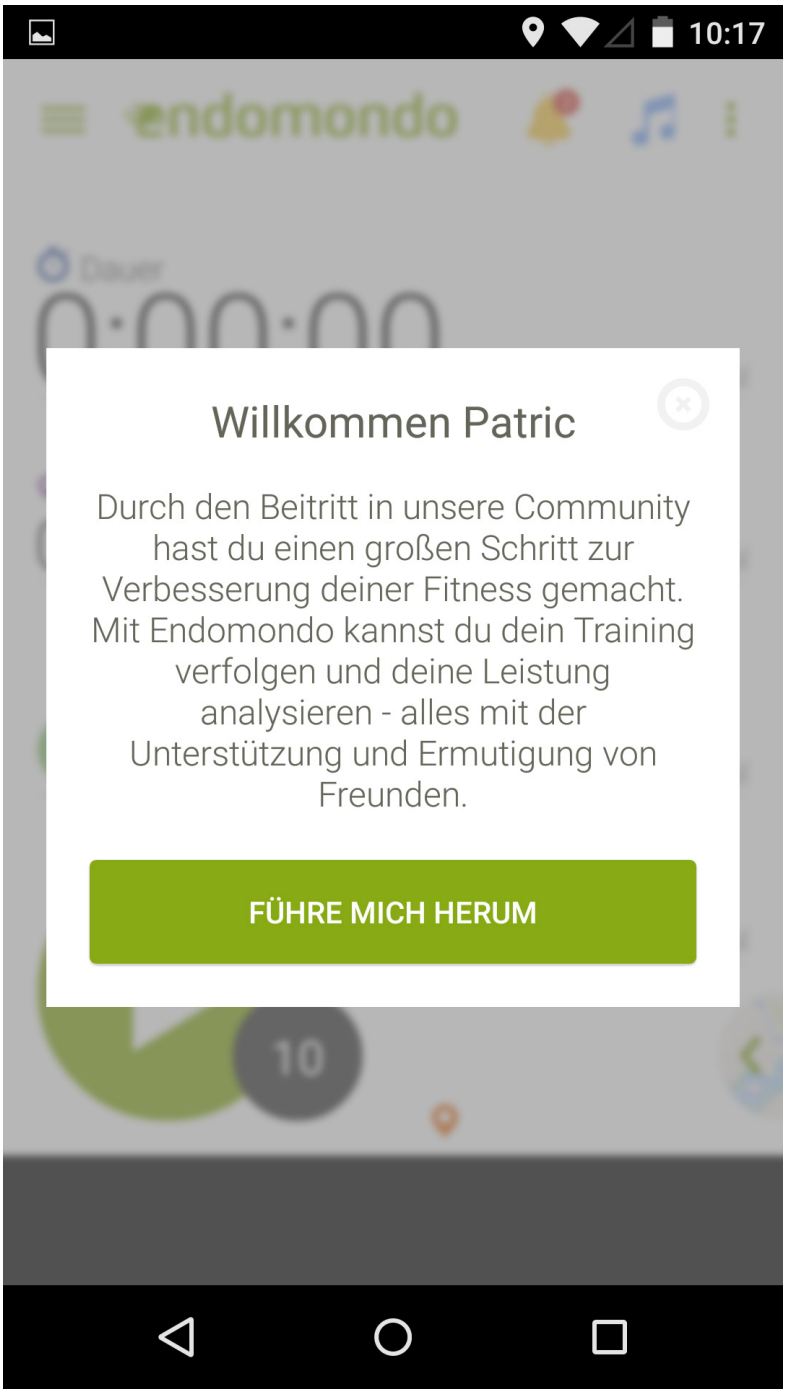


Abbildung 4.43: Endomondo - 9 - Funktionen - Start
Endomondo Running Cycling Walk [31]

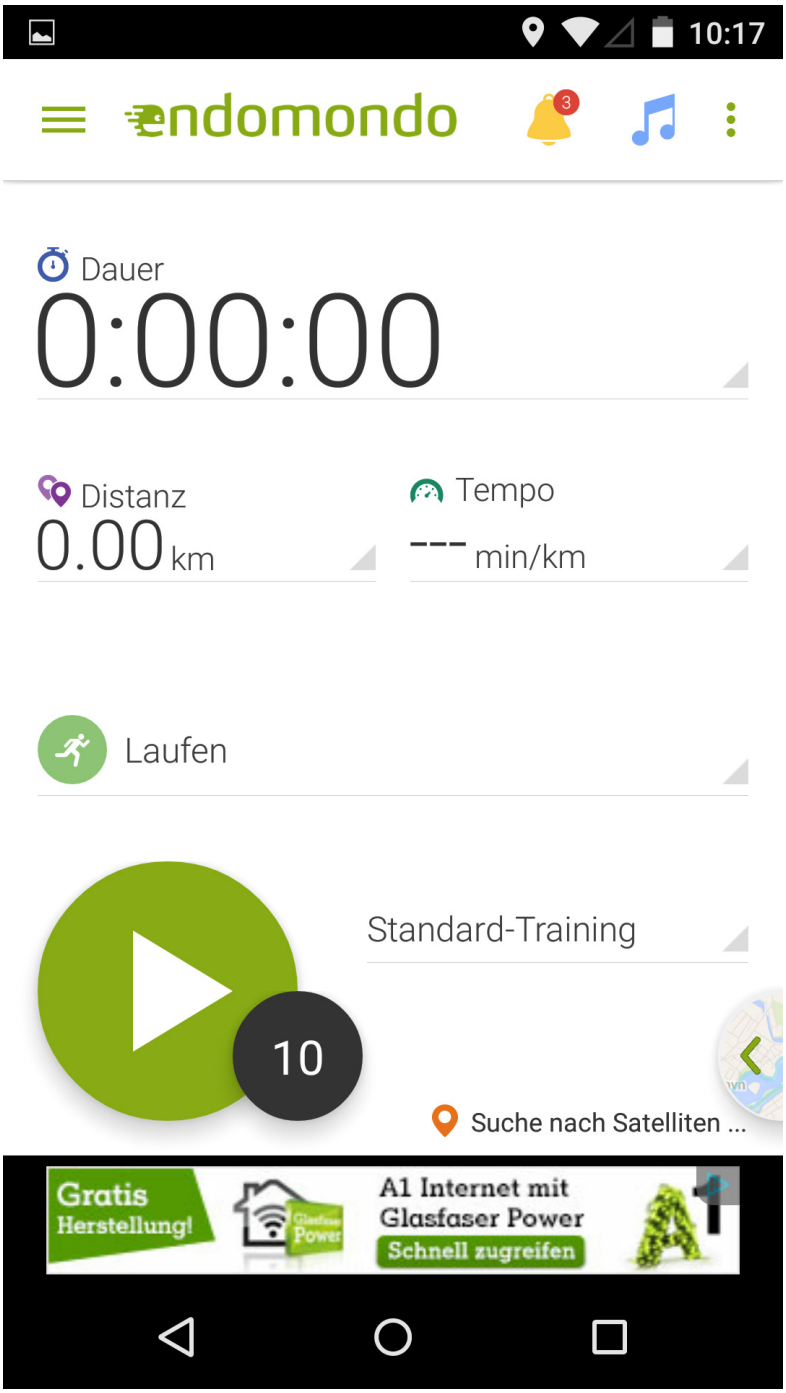


Abbildung 4.44: Endomondo - 10 - Funktionen - Start
Endomondo Running Cycling Walk [31]

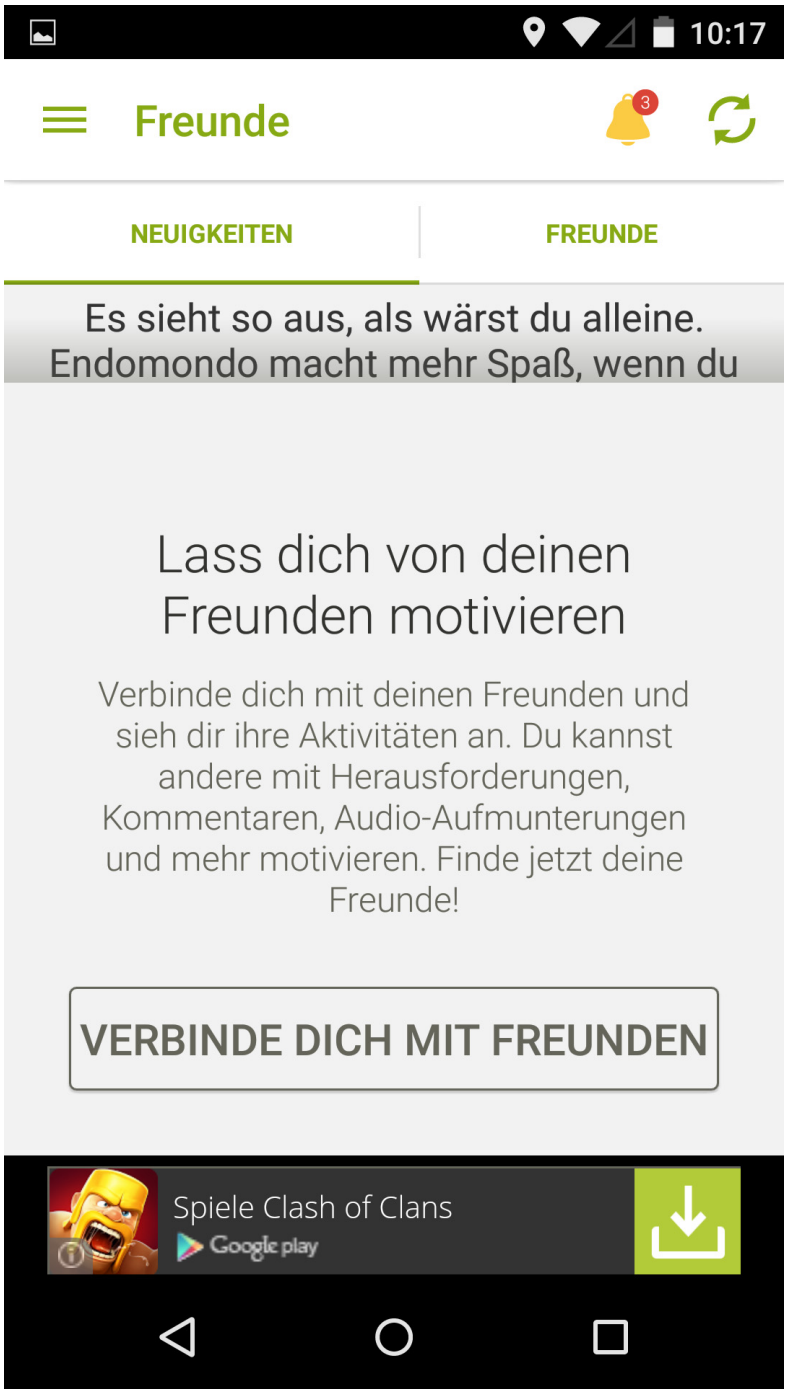


Abbildung 4.45: Endomondo - 11 - Funktionen - Freunde
Endomondo Running Cycling Walk [31]

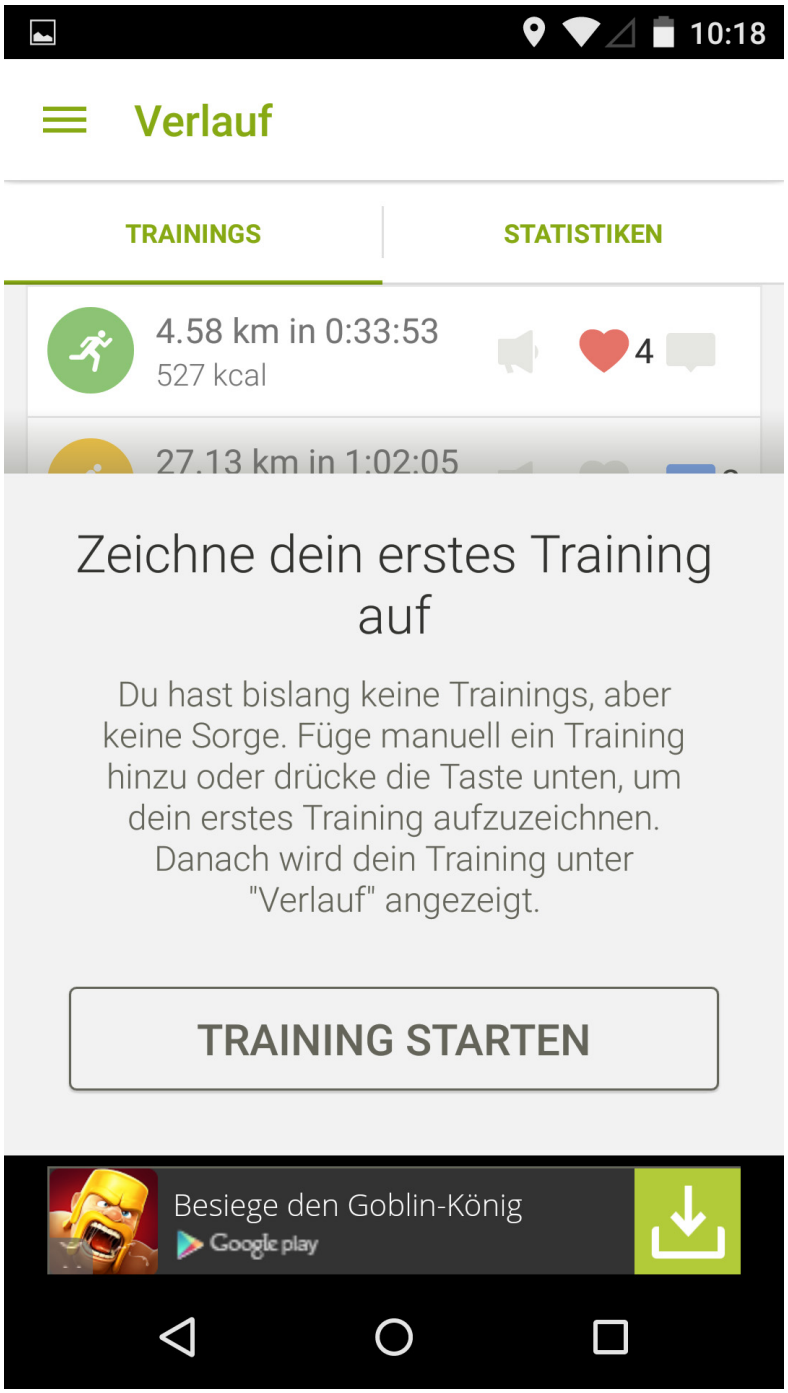


Abbildung 4.46: Endomondo - 12 - Funktionen - Verlauf
Endomondo Running Cycling Walk [31]

Abbildung 4.47: Endomondo - 13 - Funktionen - Trainingspläne
Endomondo Running Cycling Walk [31]

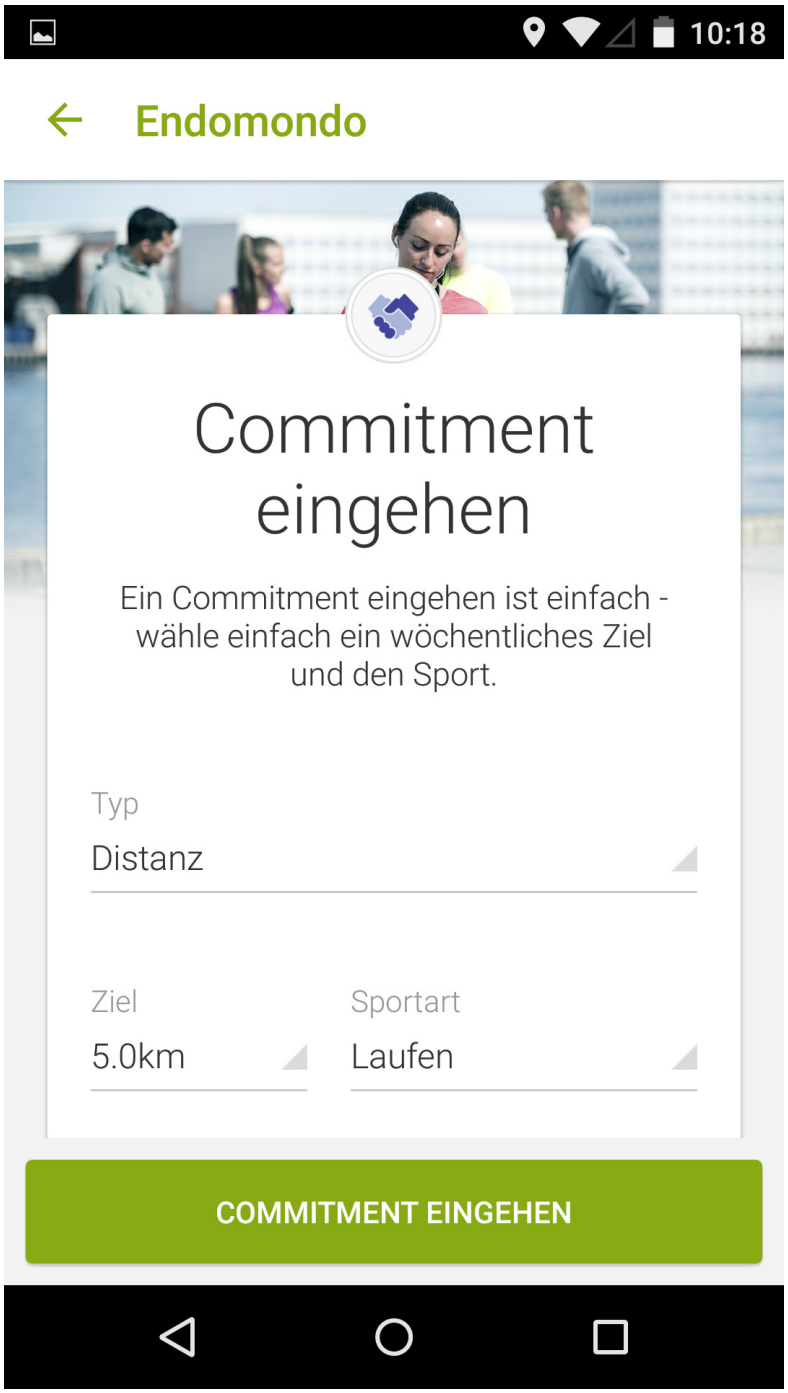


Abbildung 4.48: Endomondo - 14 - Funktionen - Commitment eingehen
Endomondo Running Cycling Walk [31]

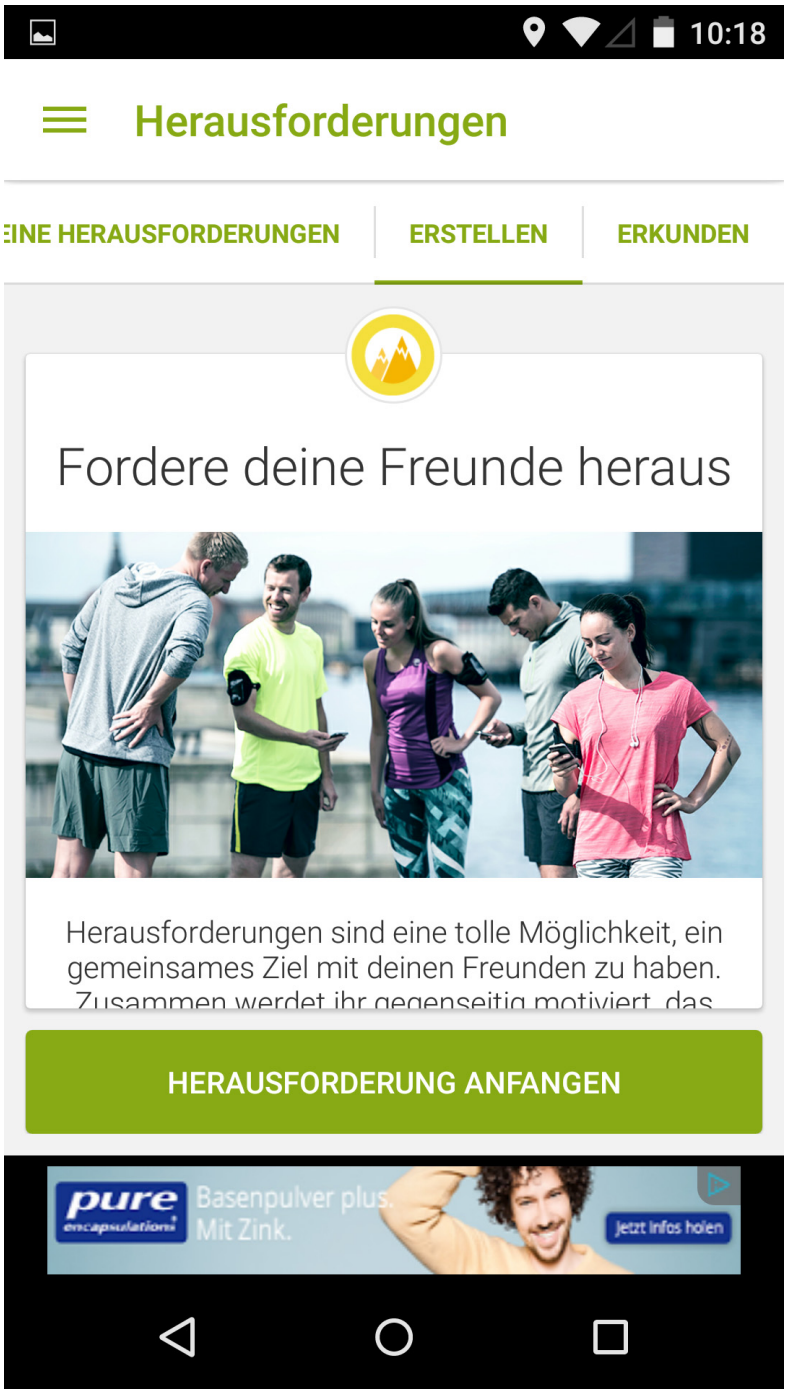


Abbildung 4.49: Endomondo - 15 - Funktionen - Herausforderungen
Endomondo Running Cycling Walk [31]

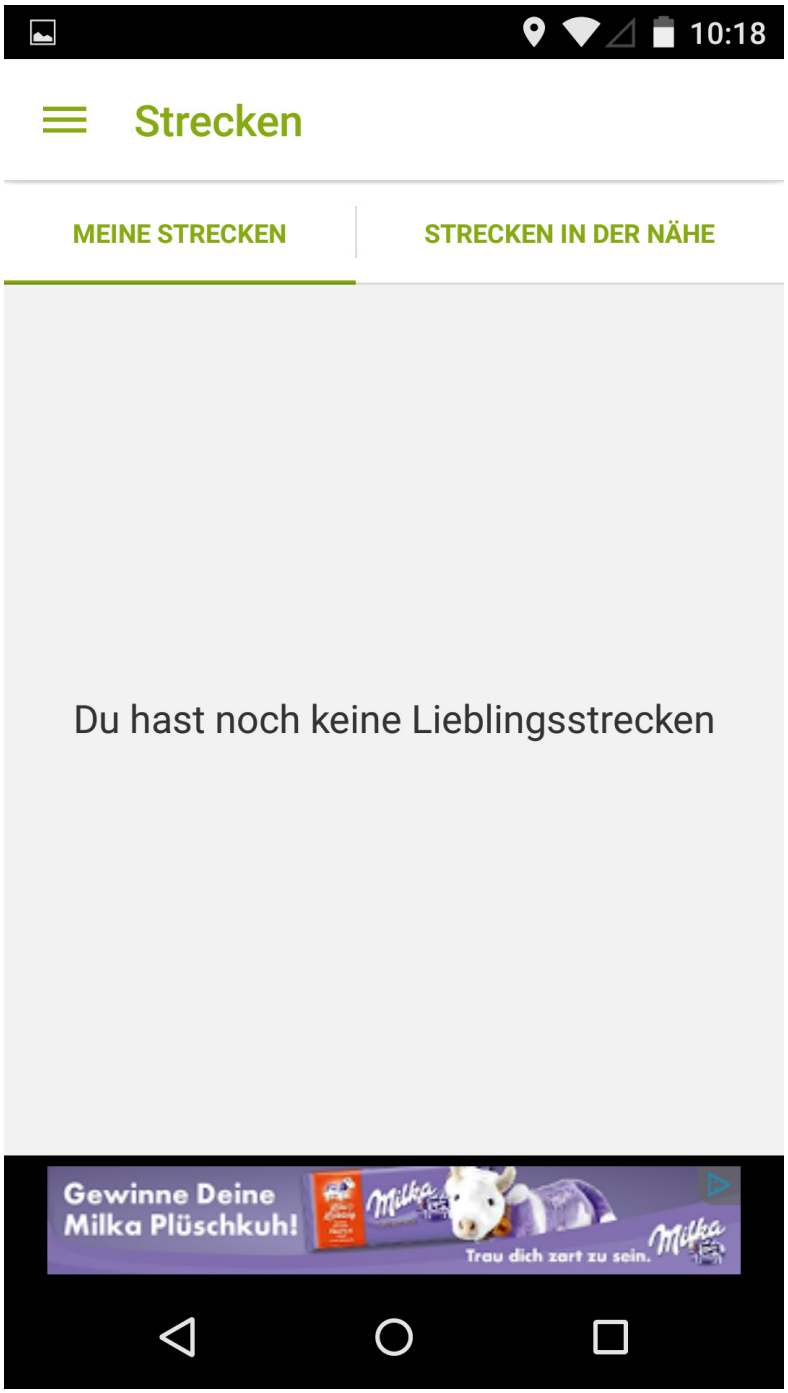


Abbildung 4.50: Endomondo - 16 - Funktionen - Strecken
Endomondo Running Cycling Walk [31]

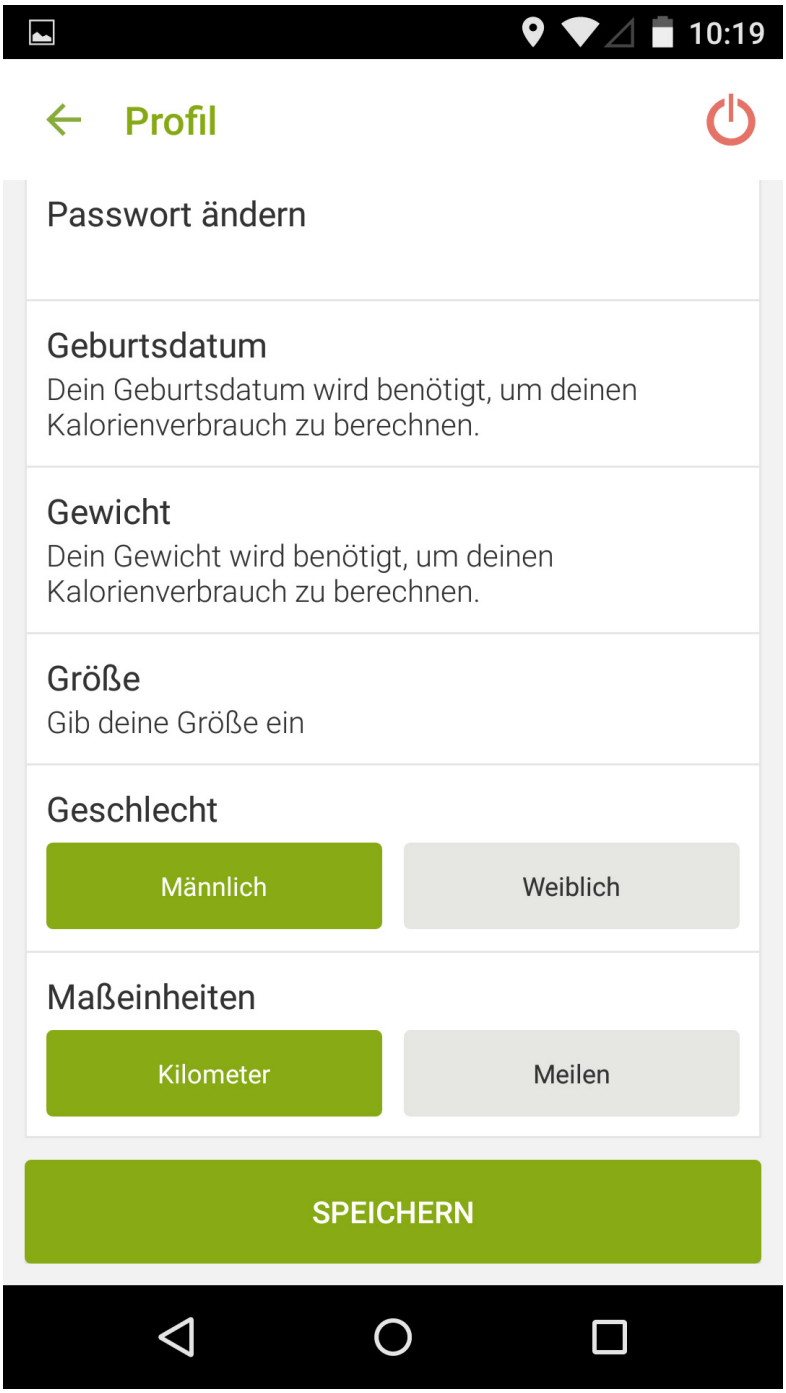


Abbildung 4.51: Endomondo - 17 - Privatsphäre
Endomondo Running Cycling Walk [31]

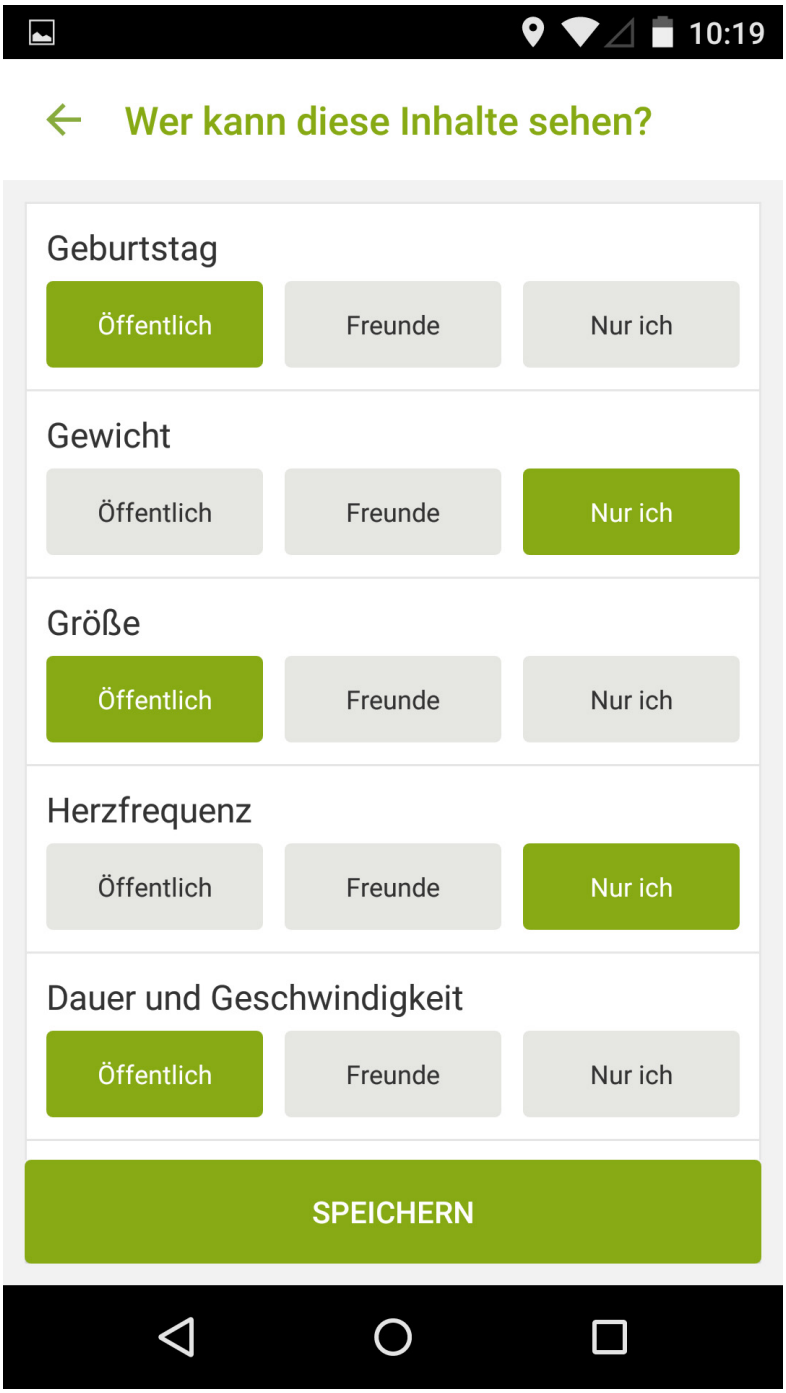


Abbildung 4.52: Endomondo - 18 - Privatsphäre
Endomondo Running Cycling Walk [31]

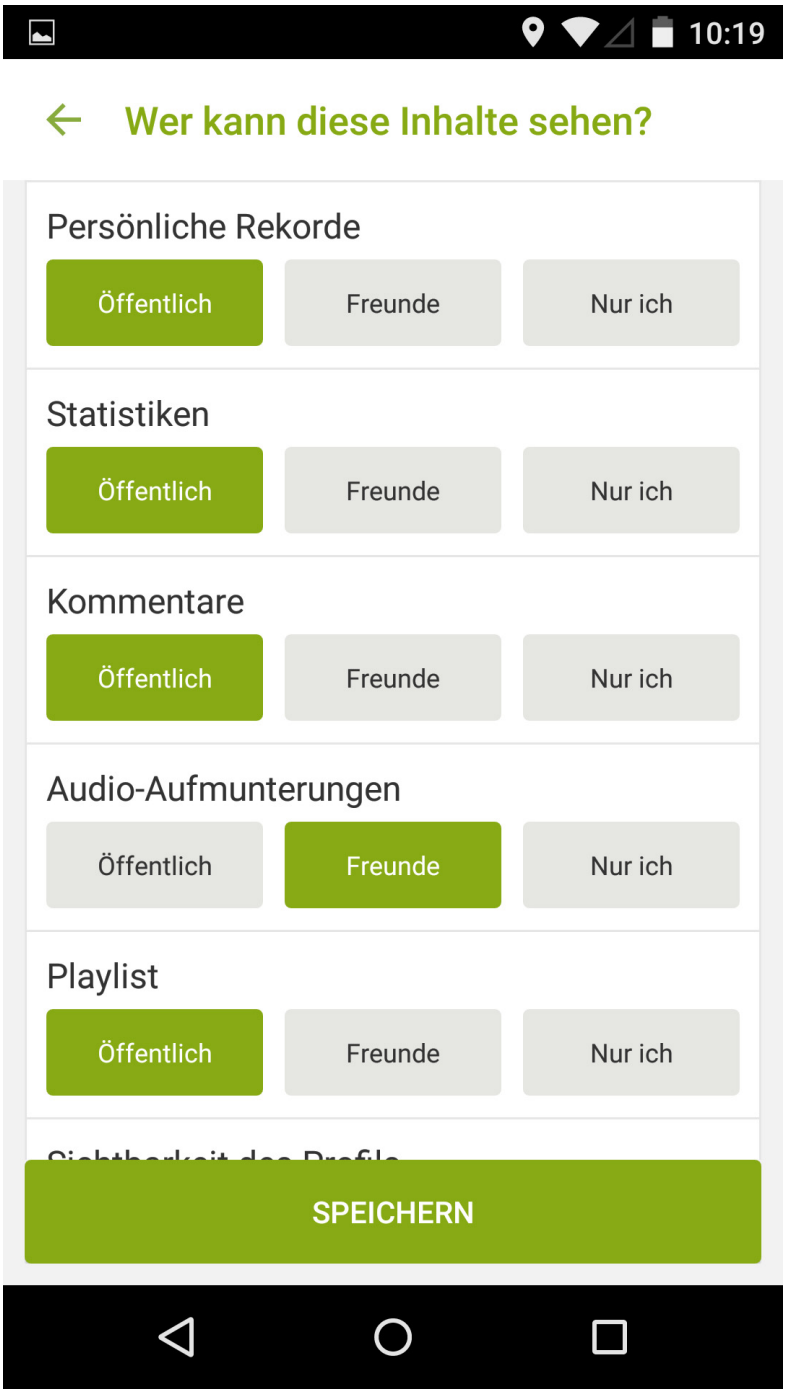


Abbildung 4.53: Endomondo - 19 - Privatsphäre
Endomondo Running Cycling Walk [31]

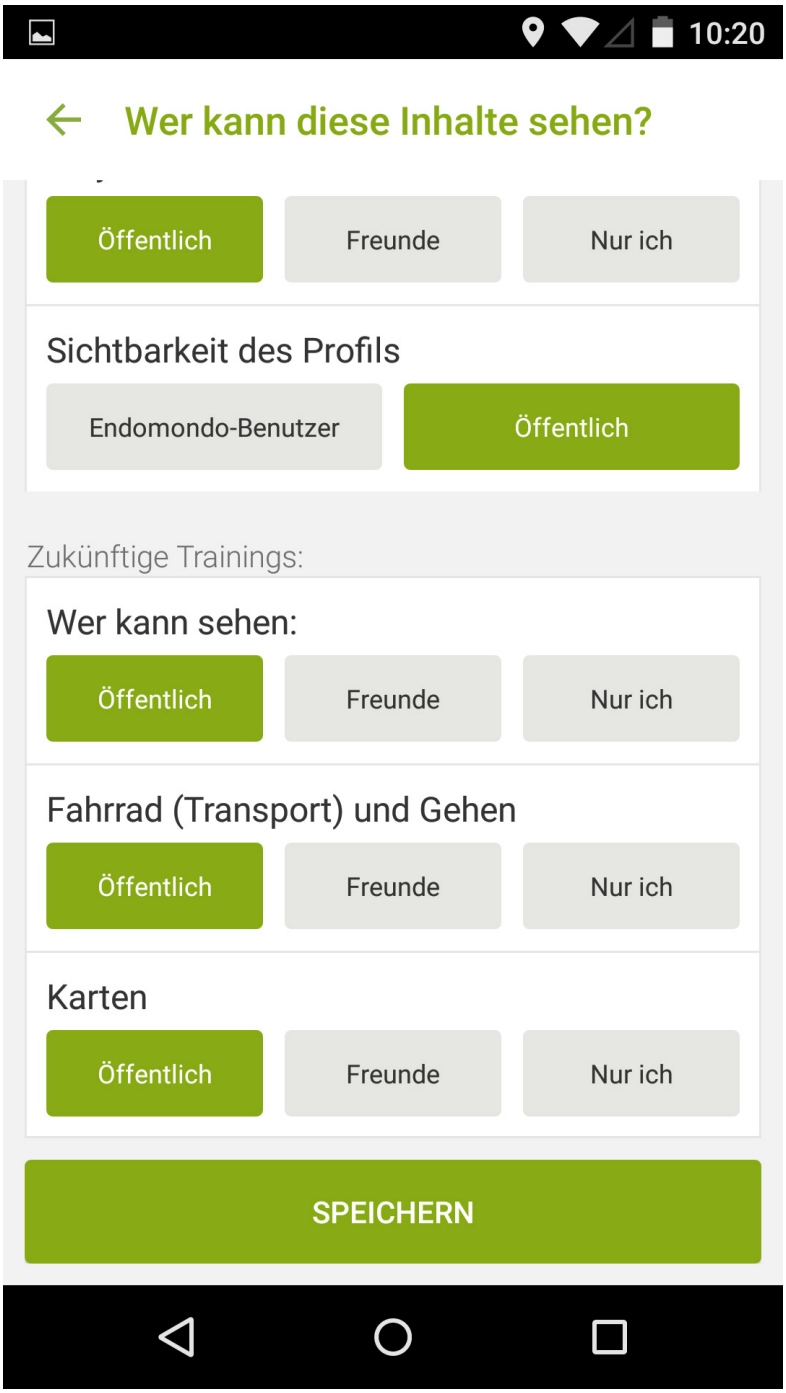


Abbildung 4.54: Endomondo - 20 - Privatsphäre
Endomondo Running Cycling Walk [31]

Abbildung 4.55: Kalorienzähler – MyFitnessPal Logo
Kalorienzähler – MyFitnessPal [75]

4.6 Kalorienzähler – MyFitnessPal

Adresse: https://play.google.com/store/apps/details?id=com.myfitnesspal.android

Als Entwickler der App zeichnet laut Google Play Store und der offiziellen Homepage die Firma MyFitnessPal Inc., wobei der Standort bzw. das Herkunftsland des Unternehmens nirgends ersichtlich ist. Ein Nachverfolgen der Adresse der Webseite ergab einen Serverstandort in den USA. Ob dies auch der Speicherort für die Kundendaten ist, kann nicht mit Sicherheit gesagt werden, ist allerdings als sehr wahrscheinlich anzusehen. Versteckt in den Datenschutzbestimmungen findet sich eine Beschwerdeanschrift, welche auf den Firmennamen zu verweisen scheint. Diese befindet sich in San Francisco, Kalifornien, USA. Darüber hinaus deklariert die Bestimmung als letzten Punkt, dass alle Daten innerhalb der USA gespeichert werden.

Die Datenschutzbestimmungen sind, entgegen der üblichen Praxis, im Google Play Store nicht

verlinkt [43] und lediglich über die Homepage auffindbar. Man wird beim Einrichten des Benutzerkontos allerdings auf diese hingewiesen. [44] Die Bestimmungen selbst räumen dem Unternehmen ein äußerst hohes Maß an Rechten zur Sammlung, Verwertung und Verbreitung von Nutzerdaten ein. So wird jeder Benutzer bei Anmeldung bereits verpflichtet, ein öffentliches Profil zu erstellen, welches Informationen wie Alter, Standort, Gewichtsabnahme insgesamt, ethnische Zugehörigkeit, Familienstand und Religion enthält. Darüber hinaus räumt sich das Unternehmen jegliche Rechte an allen sogenannten Nutzerinhalten ein. Dies sind jegliche Informationen, die von Benutzern der Dienste eingestellt oder geteilt werden. Die Nutzer übertragen somit jegliche Rechte an das Unternehmen und Mitarbeiter. Das Unternehmen räumt sich darüber hinaus das explizite Recht ein, ohne Rücksprache diese Daten zu löschen, zu verändern oder auch zu verwenden. Auch die Verwendung für Werbe- und „Propagandazwecke“ ist explizit erwähnt. Darüber hinaus ist die Veröffentlichung von Daten im Namen des Benutzers ohne Rücksprache mit diesem durch das Unternehmen möglich. Ebenfalls räumt sich das Unternehmen das Recht ein, bei Installation der App Informationen über das Smartphone, welches es eindeutig identifizierbar machen, automatisch und ohne weitere Information des Besitzers zu sammeln und an die Server zu übertragen. Ganz offen wird durch die Bestimmungen klargestellt, dass alle Daten, auch die sensiblen Gesundheitsdaten, zur Auswertung herangezogen werden, damit eine personalisiertere Werbeeinblendung erfolgen kann.

Die Installation ist wie gewohnt einfach und zügig. Abgesehen vom Zugriff auf die Kamera des Smartphones, beinhalten die Berechtigungen der App keine Auffälligkeiten. Diesen benötigt die App allerdings für dokumentierte Funktionen. [45]

Die App setzt vor der möglichen Verwendung die Einrichtung bzw. Eingabe eines Benutzerkontos voraus. Die Option, dieses zu überspringen, fehlt gänzlich. [46] Zusätzlich zur Verwendung eines eigenen Benutzers von MyFitnessPal kann auch alternativ das Login mittels Facebook vollzogen werden. [47] Lediglich bei einer neuen Registrierung wird man auf die Nutzungsbedingungen und Datenschutzbestimmungen hingewiesen. [48] Direkt vor dem erfolgreichen Registrieren werden einige Fragen zur Person und den Fitness-Zielen gestellt, welche nicht überspringbar sind. Unter anderem werden auch sehr persönliche Daten wie Geschlecht [49], Geburtsdatum [50], Körpergröße [51] und Körpergewicht [52] abgefragt.

Direkt zum ersten Start der App wird man aufgefordert, seine letzte Mahlzeit exakt einzutra-

[43] siehe Abbildung 4.56 und Abbildung 4.57
[44] siehe Abbildung 4.61 und Abbildung 4.62
[45] siehe Abbildung 4.58
[46] siehe Abbildung 4.59
[47] siehe Abbildung 4.60
[48] siehe Abbildung 4.61
[49] siehe Abbildung 4.64
[50] siehe Abbildung 4.64
[51] siehe Abbildung 4.65
[52] siehe Abbildung 4.65

gen. Dazu gehört die Tageszeit [53], die Bezeichnung des Essens selbst [54] sowie die relativ exakte Portionsgröße [55]. Danach präsentiert sich der normale Startbildschirm mit einer Übersicht, wie viele Kalorien man heute bereits zu sich genommen hat und wie viele auf das errechnete Tagesmaximum noch ausständig sind. [56] Natürlich können die Einträge bereits vergangener Tage nochmals eingesehen [57] und darüber hinaus in einer genauen Nährwertanalyse betrachtet werden [58]. Ebenfalls ist es möglich, Rezepte einzupflegen und diese sogar nach Mahlzeiten oder Lebensmitteln zu sortieren und filtern. [59] Auch der Fortschritt des Diätplans in Kombination mit dem Körpergewicht kann statistisch mittels einer Visualisierung dargestellt werden. [60] Ebenfalls bietet die App die Möglichkeit, sich mit Freunden zu vernetzen und sogar Nachrichten über die Plattform auszutauschen. [61]

Es können sowohl externe Geräte als auch andere Apps zum Datenimport in MyFitnessPal verbunden werden. [62] Dadurch ergibt sich die Möglichkeit, noch genauere Informationen in einem Datenstamm zusammenzuführen. Dies birgt allerdings auch das Risiko, dass noch mehr sensible Informationen kombiniert und eventuell übertragen werden.

Die Palette der erfassten Daten ist keinesfalls zu unterschätzen. Durch den Benutzerkontenzwang ergibt sich in erster Linie eine eindeutige Zuordenbarkeit aller Daten zu einem Benutzer, welcher über die E-Mail-Adresse, einen Benutzernamen, die Körpergröße, das Geschlecht, den Standort und das Geburtsdatum eindeutig identifizierbar gemacht wird. [63] Darüber hinaus ergeben sich durch die Einträge der Mahlzeiten sehr genaue Ernährungsprofile, welche für sich genommen bereits eine Gesundheitsrelevanz ergeben. In Kombination mit anderen Fitness-Apps bzw. mit externen Geräten wie Pulsmessern lassen sich durchaus vollständige Gesundheitsprofile erzeugen. Damit kann eindeutig die Aussage getroffen werden, dass die App sensible personenbezogene Daten erhebt.

Durch den Kontenzwang ergeht die Vermutung, dass die App jegliche Informationen auf Server des Unternehmens überträgt. Dieser Verdacht kann zweifelsfrei bestätigt werden, da ein einfacher Test mittels simplem Deinstallieren, erneutem Installieren und Einloggen mit den gleichen Benutzerdaten alle bisher eingetragenen Datensätze zum Vorschein bringt. Dies kann lediglich möglich sein, wenn die Daten auf einem externen Server gespeichert und bei Login auf das Gerät synchronisiert werden. Das Synchronisieren der Daten erfolgt ohne eine Information an den

[53] siehe Abbildung 4.68
[54] siehe Abbildung 4.69 und Abbildung 4.70
[55] siehe Abbildung 4.71
[56] siehe Abbildung 4.72
[57] siehe Abbildung 4.73
[58] siehe Abbildung 4.74
[59] siehe Abbildung 4.75
[60] siehe Abbildung 4.77
[61] siehe Abbildung 4.80 und Abbildung 4.81
[62] siehe Abbildung 4.82
[63] siehe Abbildung 4.83

Kunden; auch ist es nicht möglich, dieses zu deaktivieren. Allein dies ist bei derartig sensiblen Daten im Hinblick auf den Datenschutz ein keinesfalls einwandfreies Vorgehen. Darüber hinaus räumt sich das Unternehmen selbst an den sensiblen Gesundheitsdaten jegliches Recht der Verwendung, Veränderung, Verwertung und Übertragung an Dritte ohne Information und Einwilligung des Kunden ein. Dies ist in Anbetracht der Übertragung in ein Drittland zusätzlich problematisch. Die Rechtskonformität ist aufgrund der teilweise undurchsichtigen Datenschutzbestimmungen keinesfalls einwandfrei gegeben.

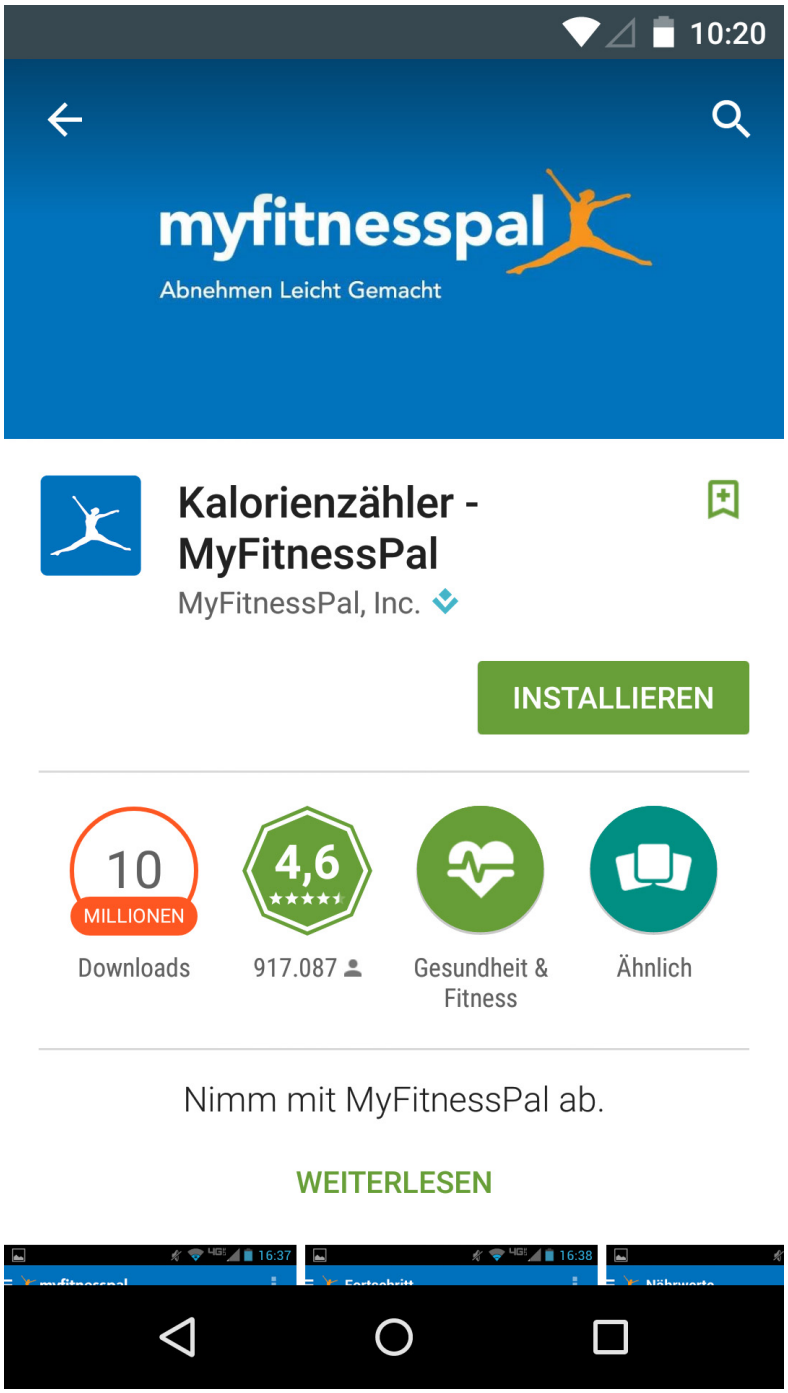


Abbildung 4.56: Kalorienzähler – MyFitnessPal - 1 - Installation
Kalorienzähler – MyFitnessPal [75]

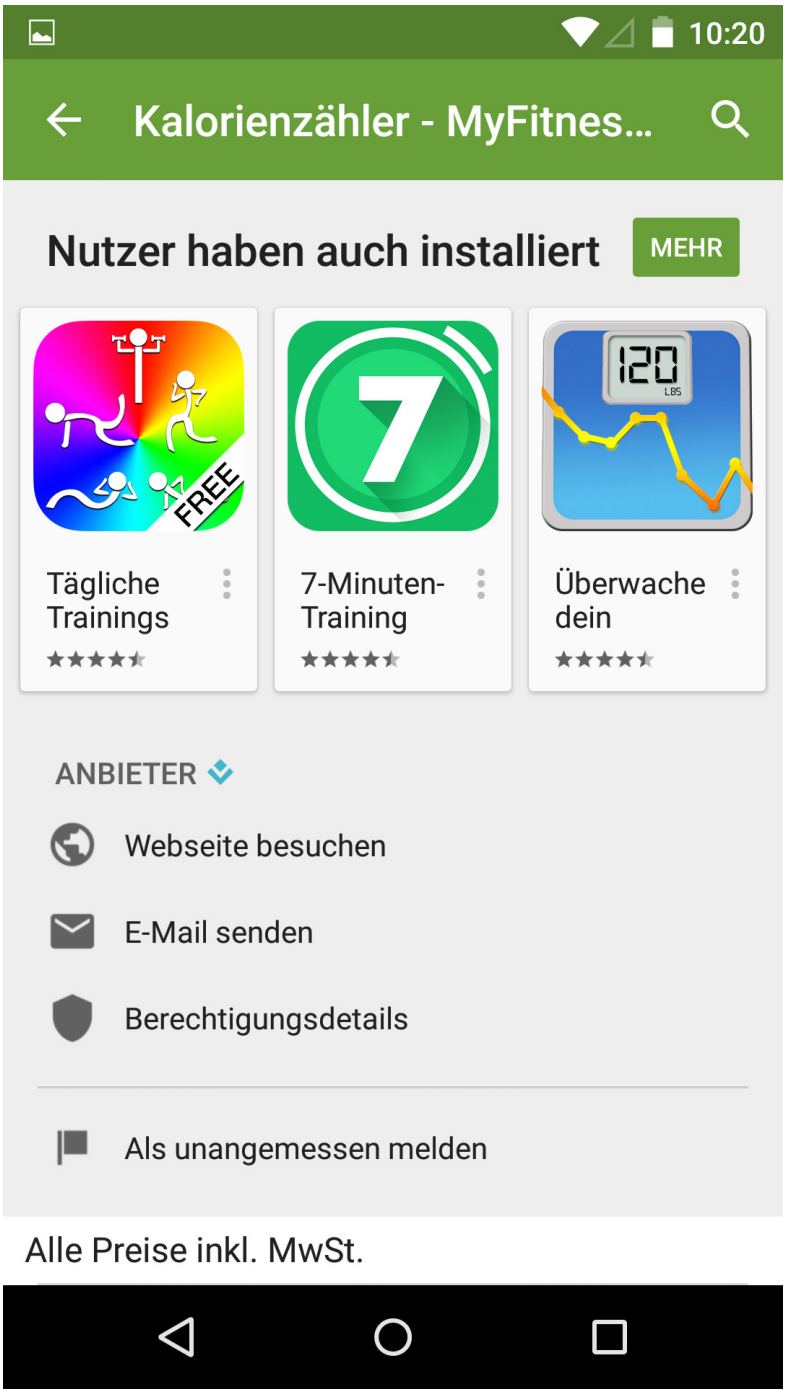


Abbildung 4.57: Kalorienzähler – MyFitnessPal - 2 - Installation
Kalorienzähler – MyFitnessPal [75]

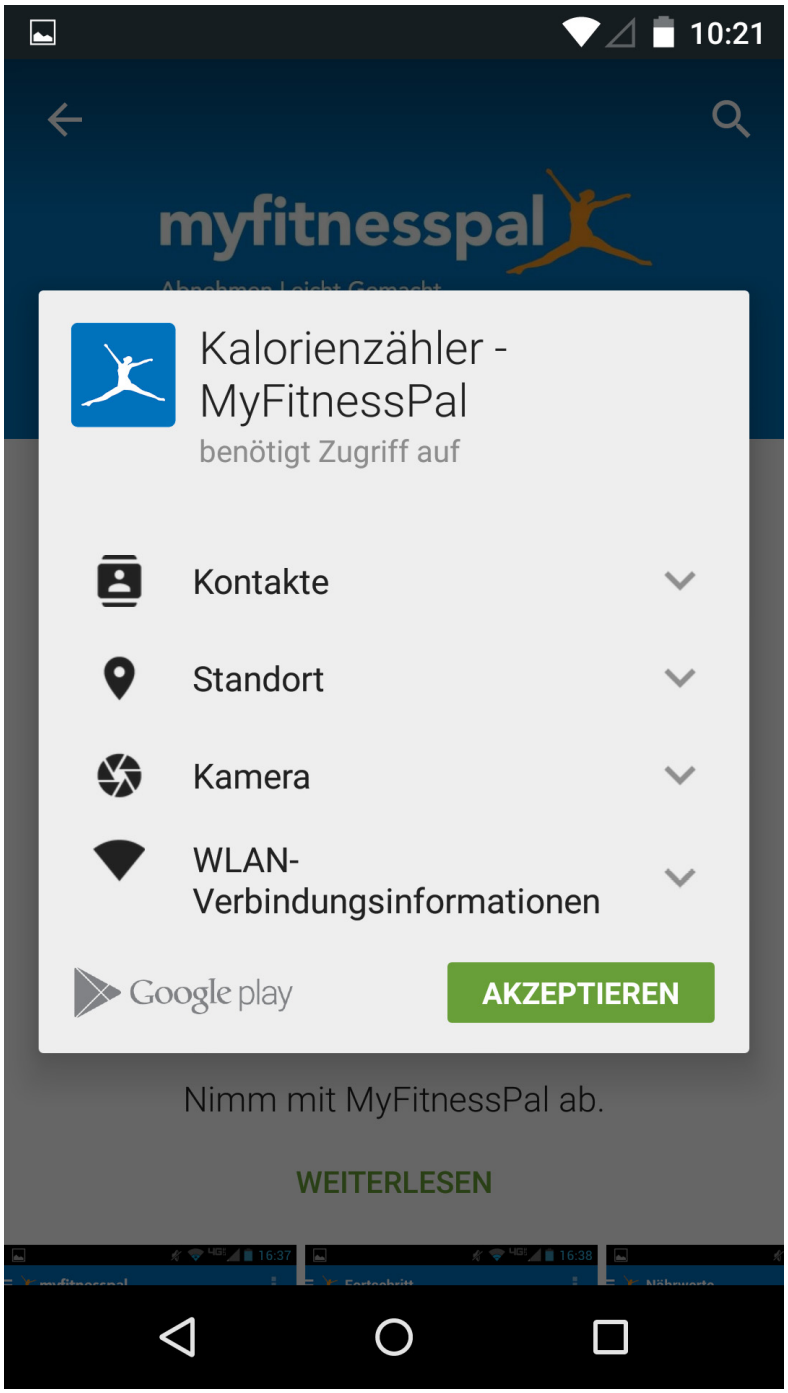


Abbildung 4.58: Kalorienzähler – MyFitnessPal - 3 - Berechtigungen
Kalorienzähler – MyFitnessPal [75]

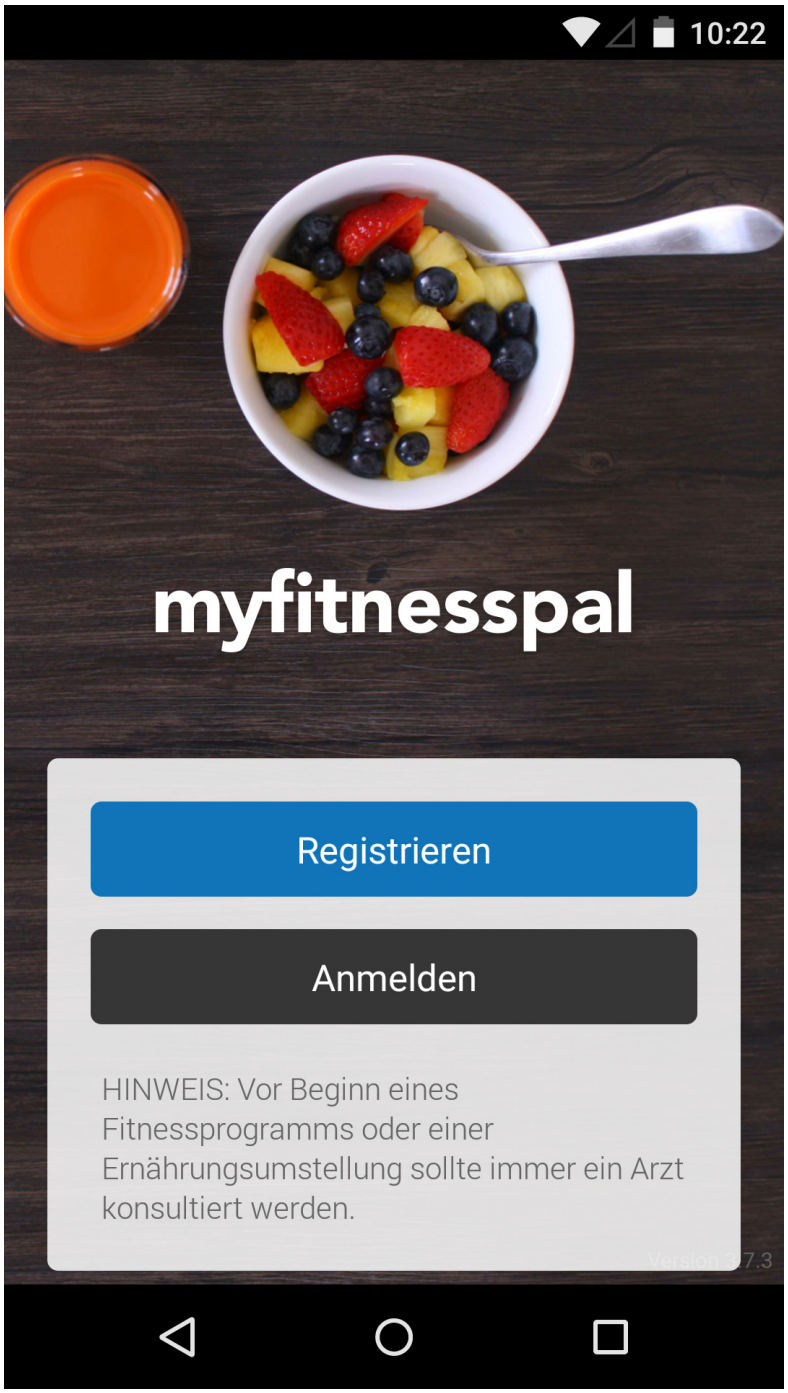


Abbildung 4.59: Kalorienzähler – MyFitnessPal - 4 - Benutzerkonto
Kalorienzähler – MyFitnessPal [75]

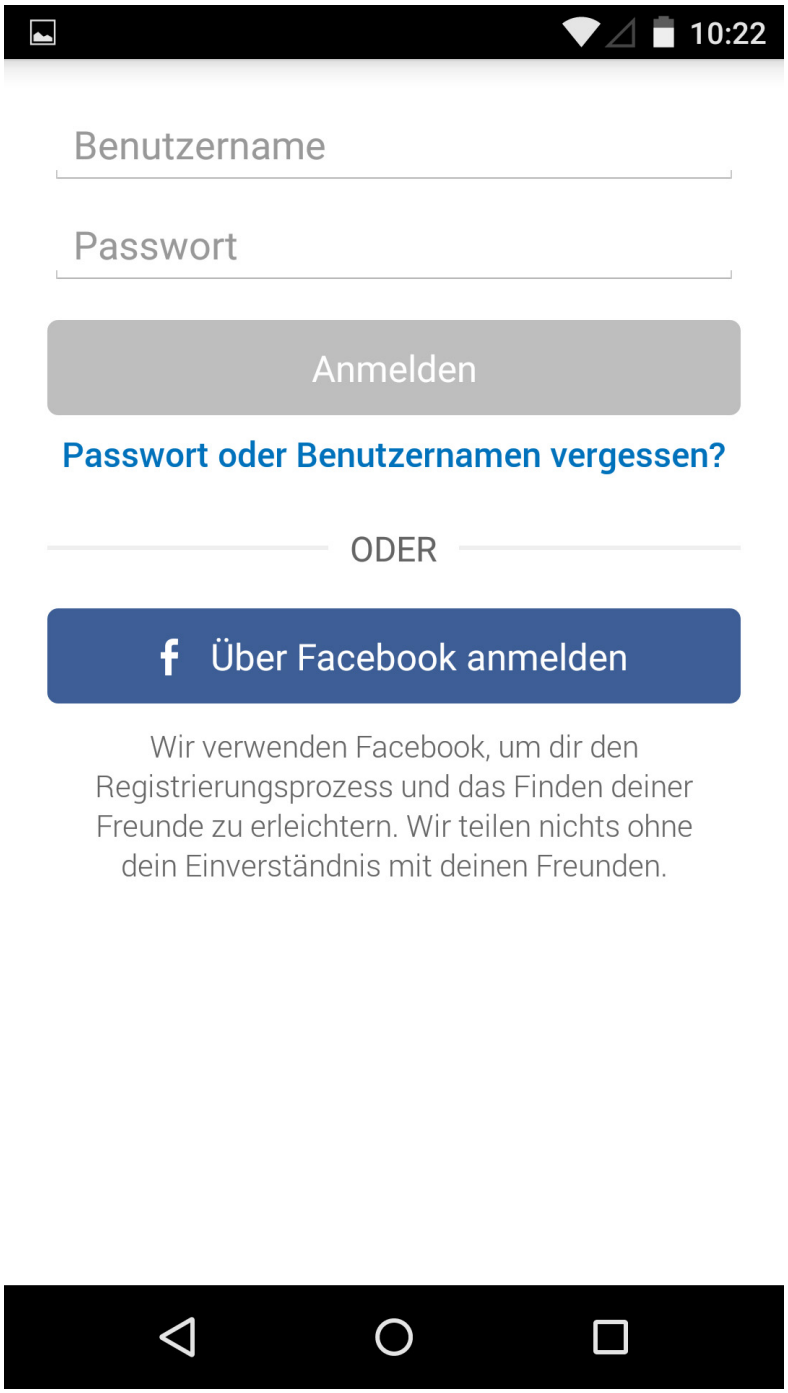


Abbildung 4.60: Kalorienzähler – MyFitnessPal - 5 - Benutzerkonto
Kalorienzähler – MyFitnessPal [75]

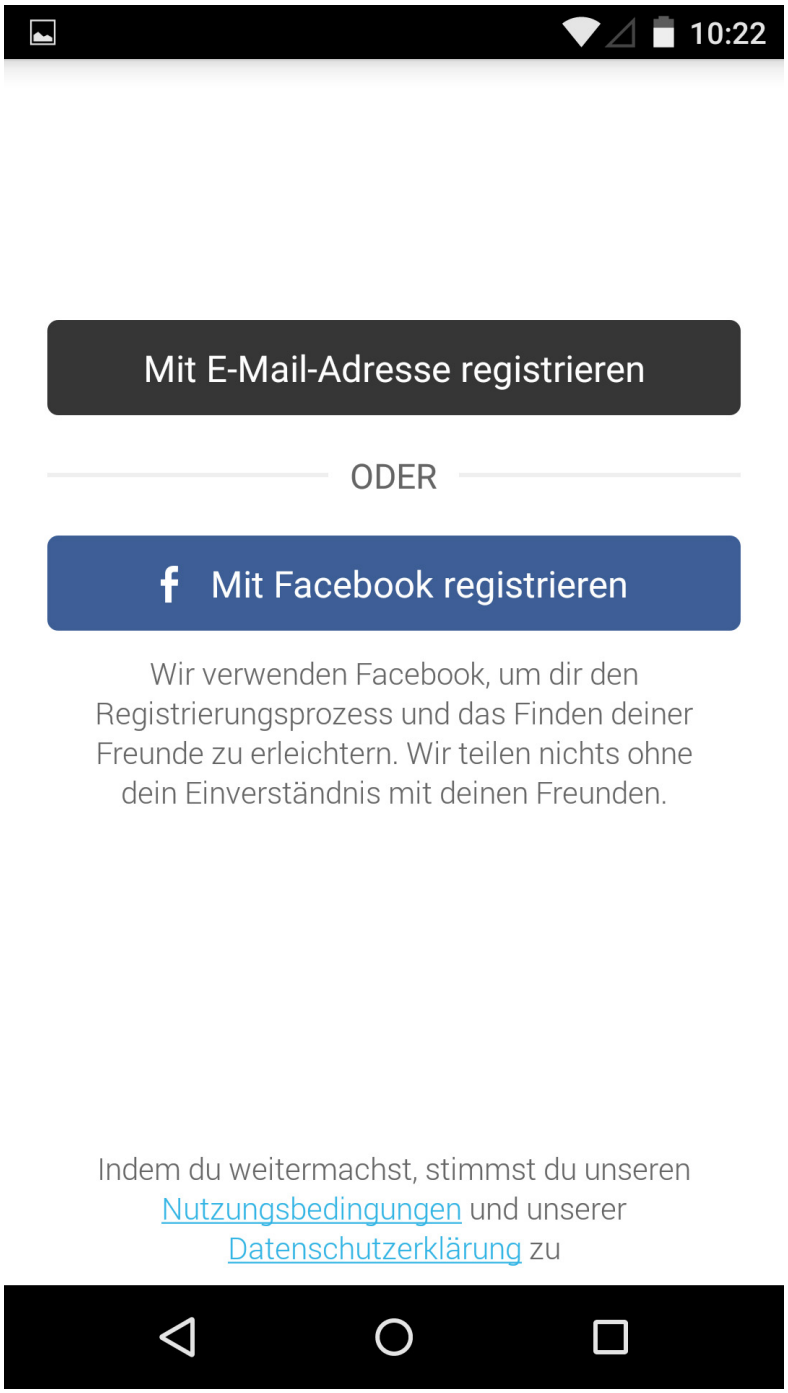


Abbildung 4.61: Kalorienzähler – MyFitnessPal - 6 - Benutzerkonto
Kalorienzähler – MyFitnessPal [75]

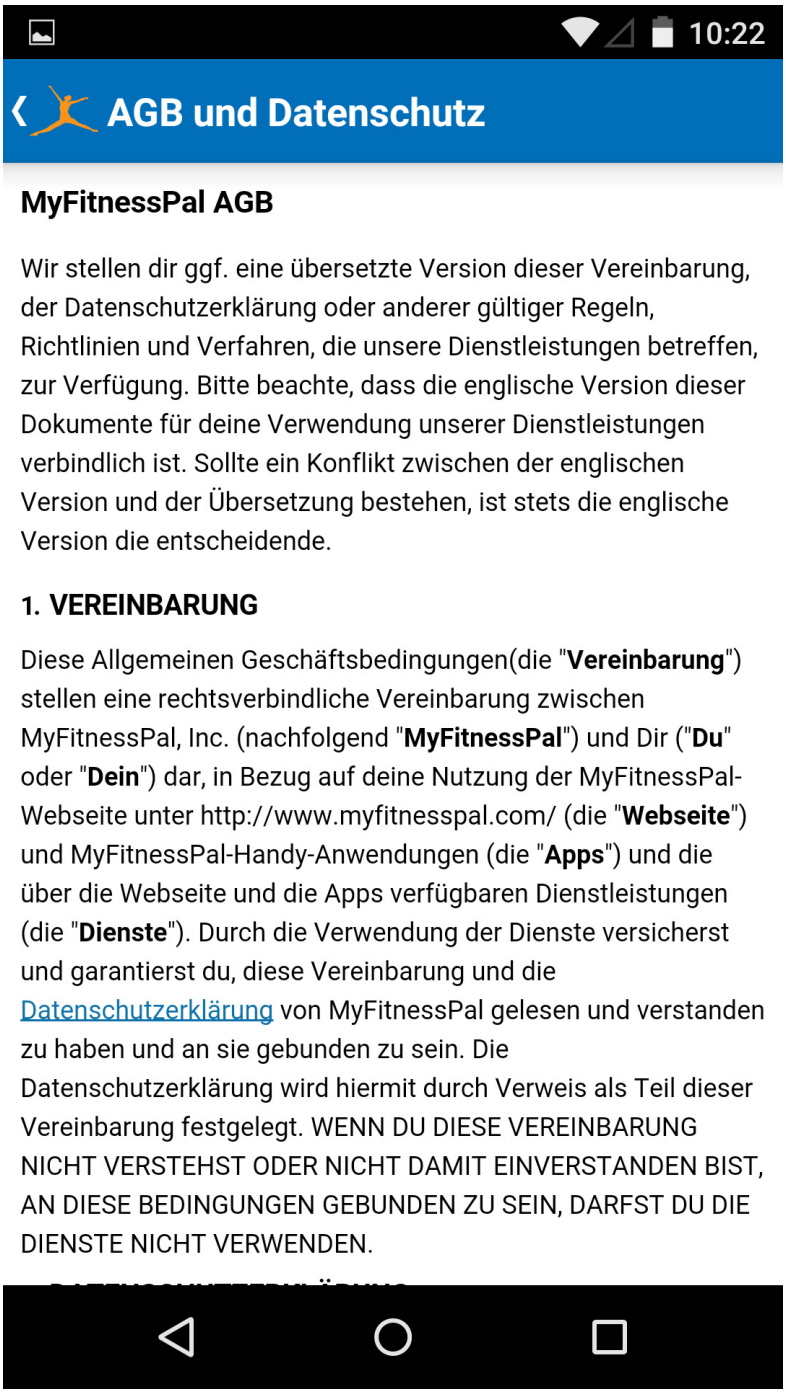


Abbildung 4.62: Kalorienzähler – MyFitnessPal - 7 - Datenschutzbestimmungen
Kalorienzähler – MyFitnessPal [75]

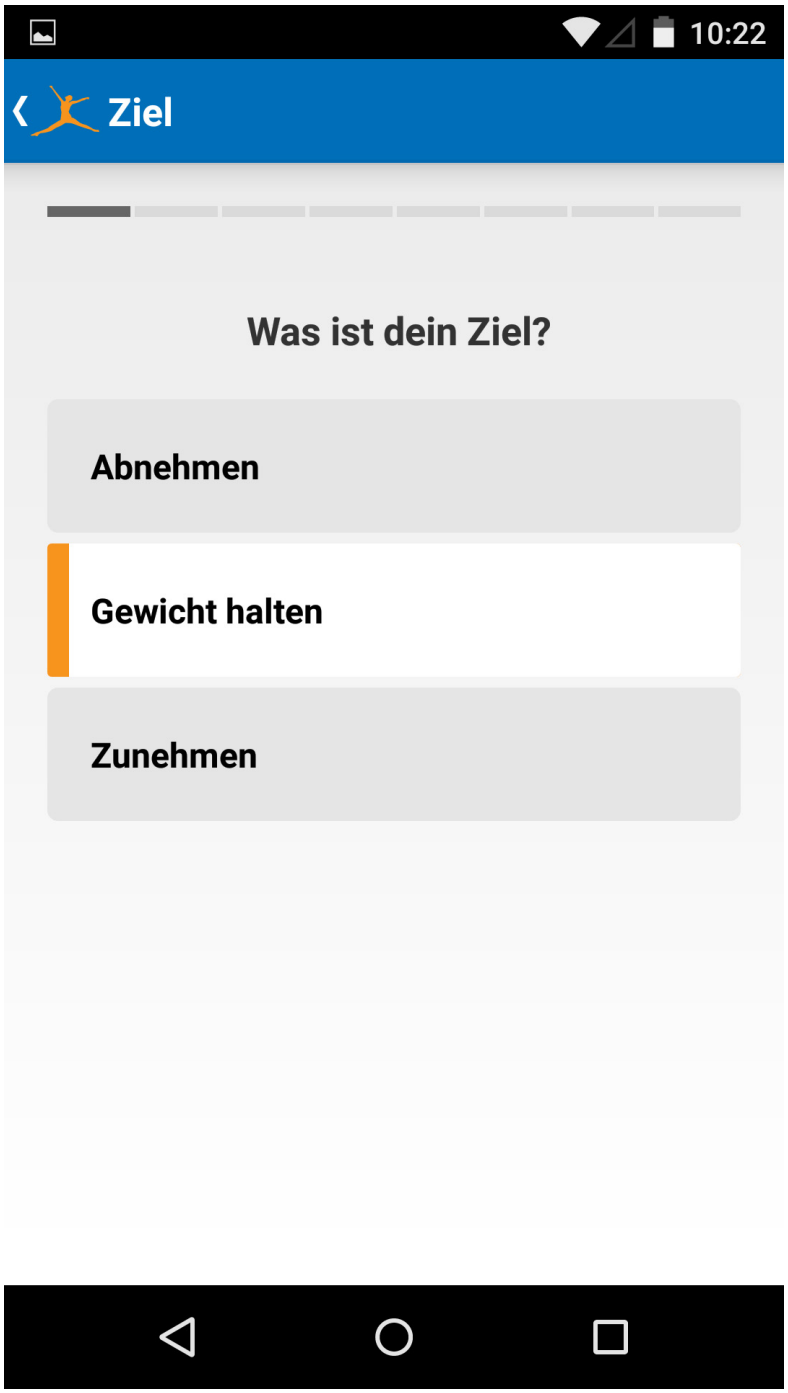


Abbildung 4.63: Kalorienzähler – MyFitnessPal - 8 - Einrichtung
Kalorienzähler – MyFitnessPal [75]

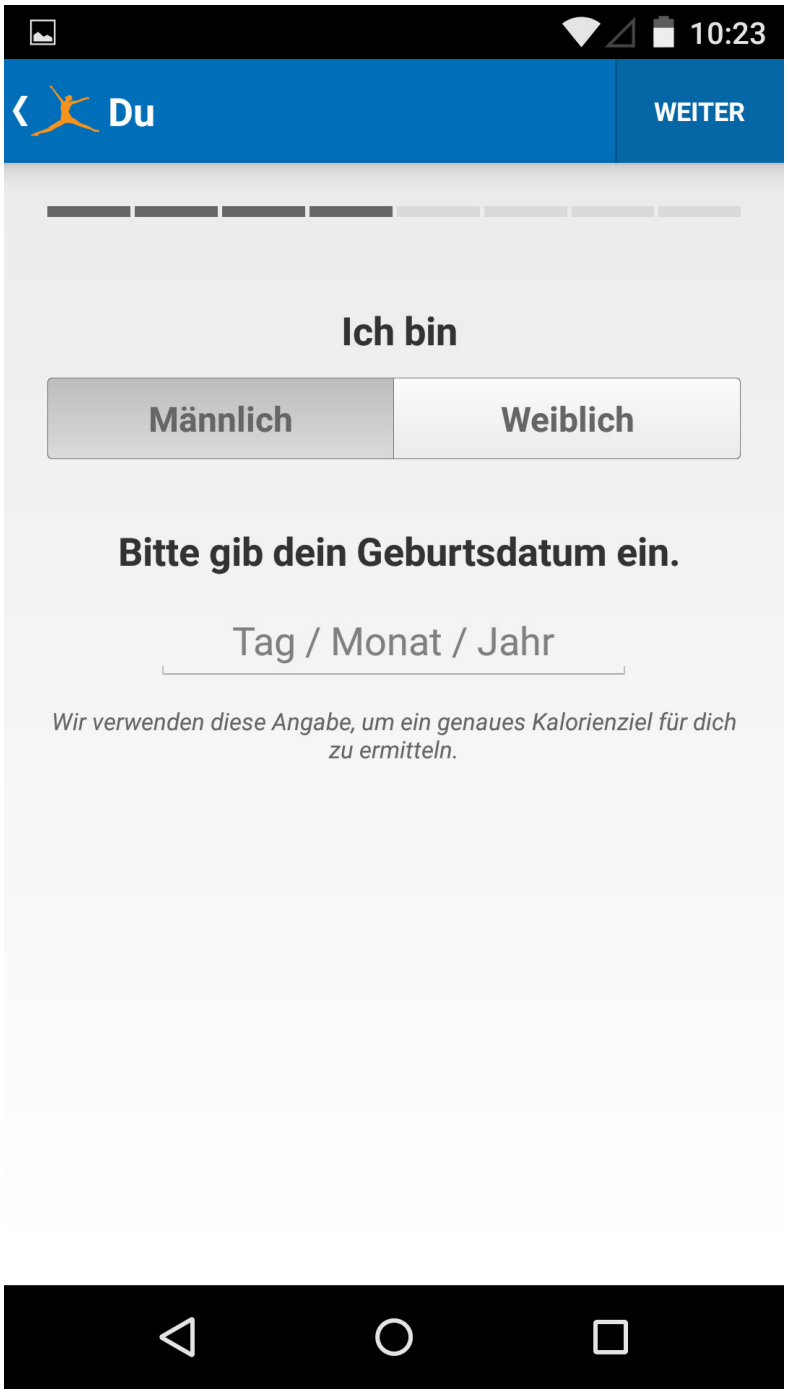


Abbildung 4.64: Kalorienzähler – MyFitnessPal - 9 - Einrichtung
Kalorienzähler – MyFitnessPal [75]

Abbildung 4.65: Kalorienzähler – MyFitnessPal - 10 - Einrichtung
Kalorienzähler – MyFitnessPal [75]

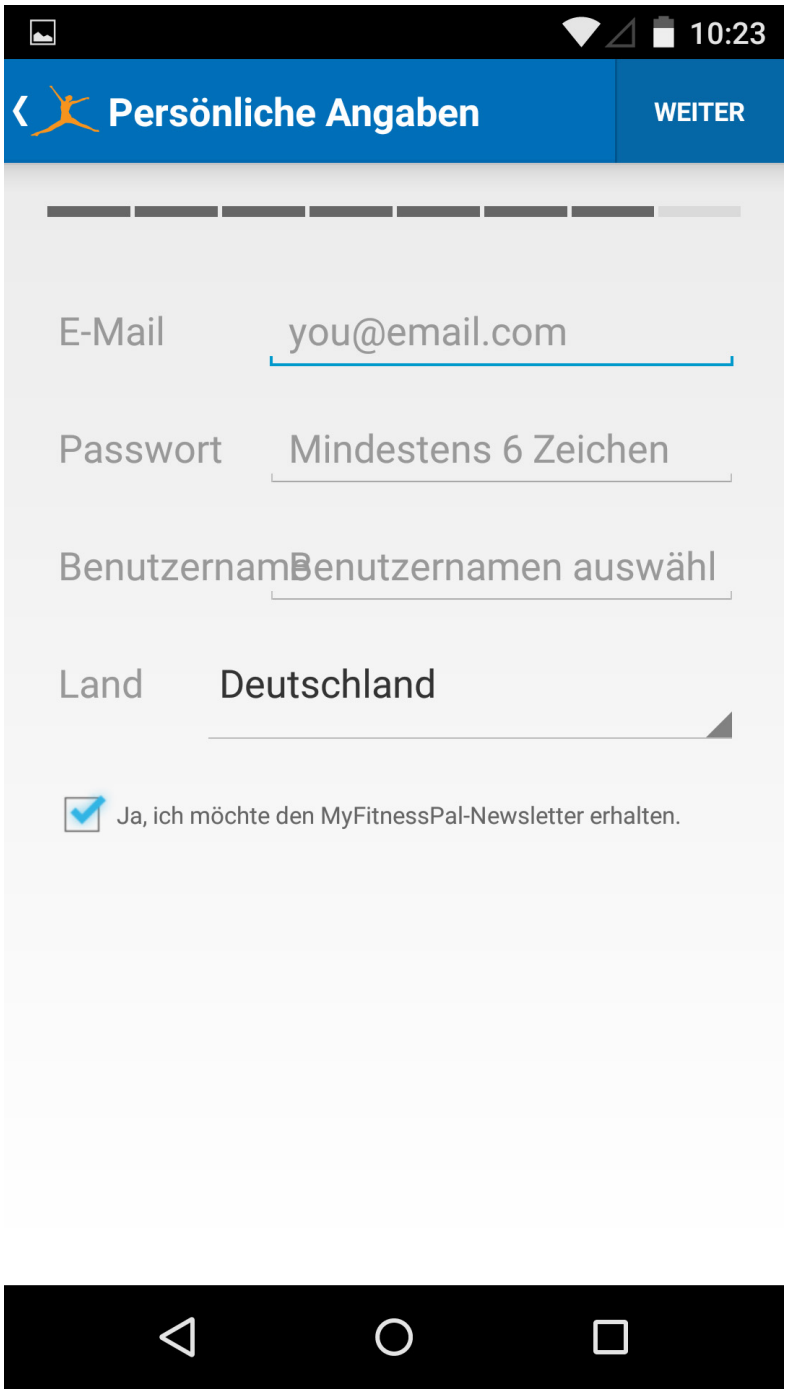


Abbildung 4.66: Kalorienzähler – MyFitnessPal - 11 - Einrichtung
Kalorienzähler – MyFitnessPal [75]

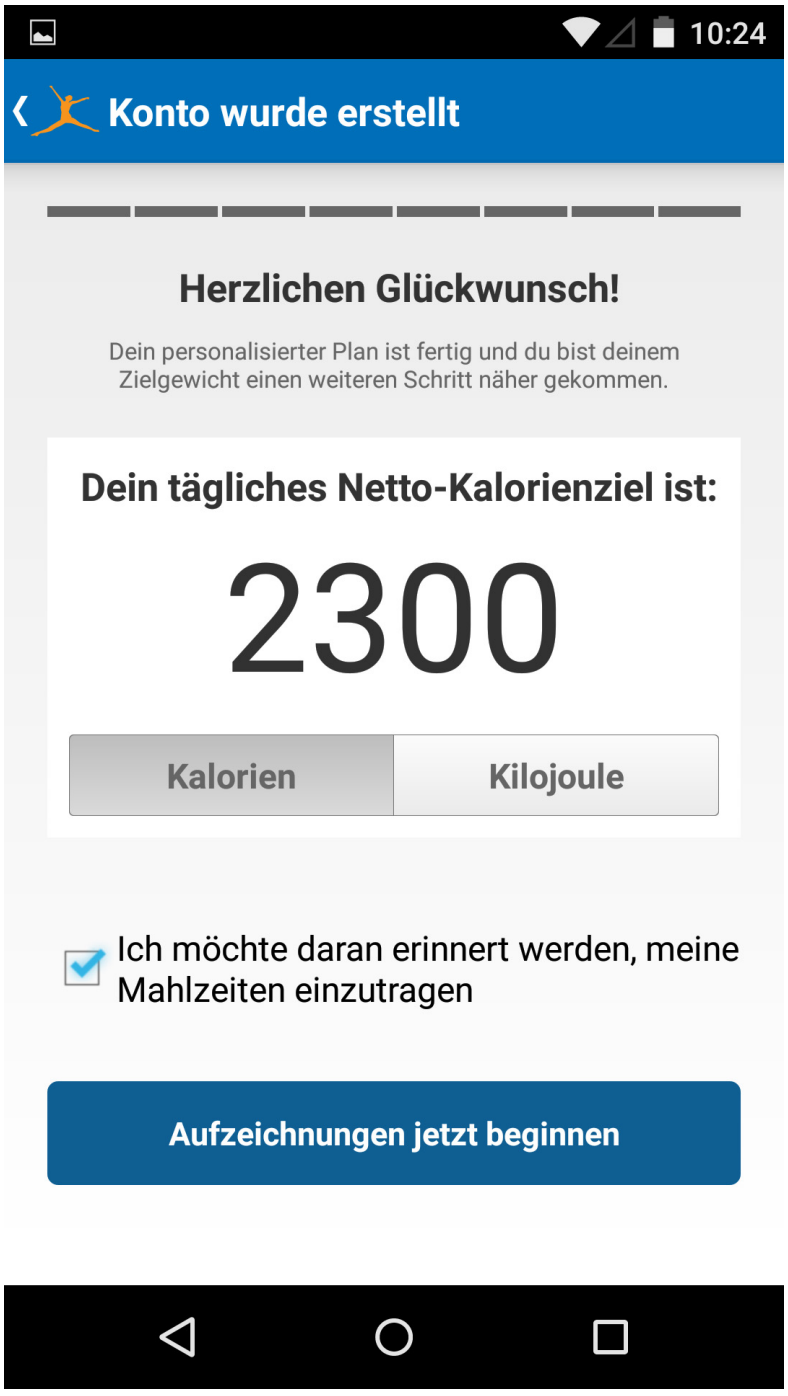


Abbildung 4.67: Kalorienzähler – MyFitnessPal - 12 - Einrichtung
Kalorienzähler – MyFitnessPal [75]

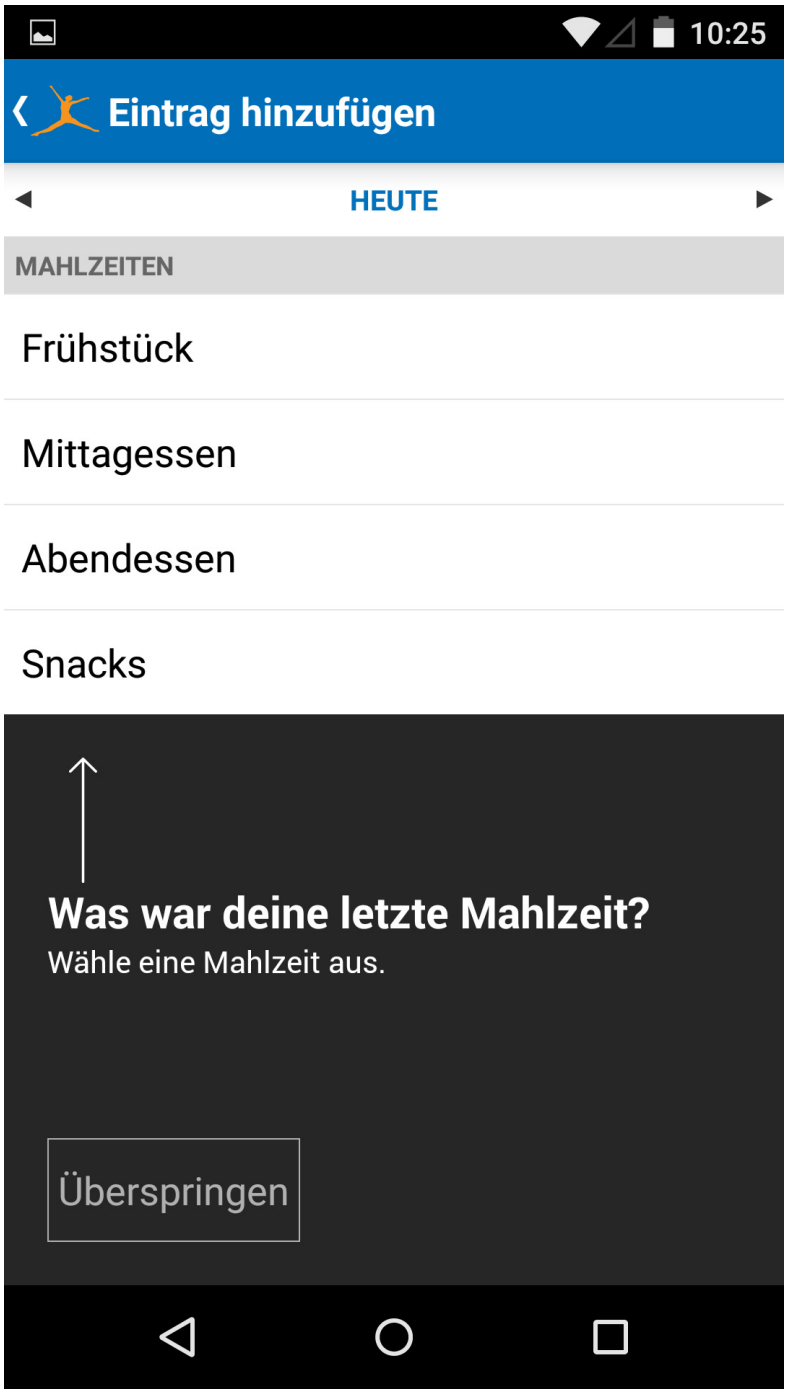


Abbildung 4.68: Kalorienzähler – MyFitnessPal - 13 - Funktionen - Eintrag hinzufügen
Kalorienzähler – MyFitnessPal [75]

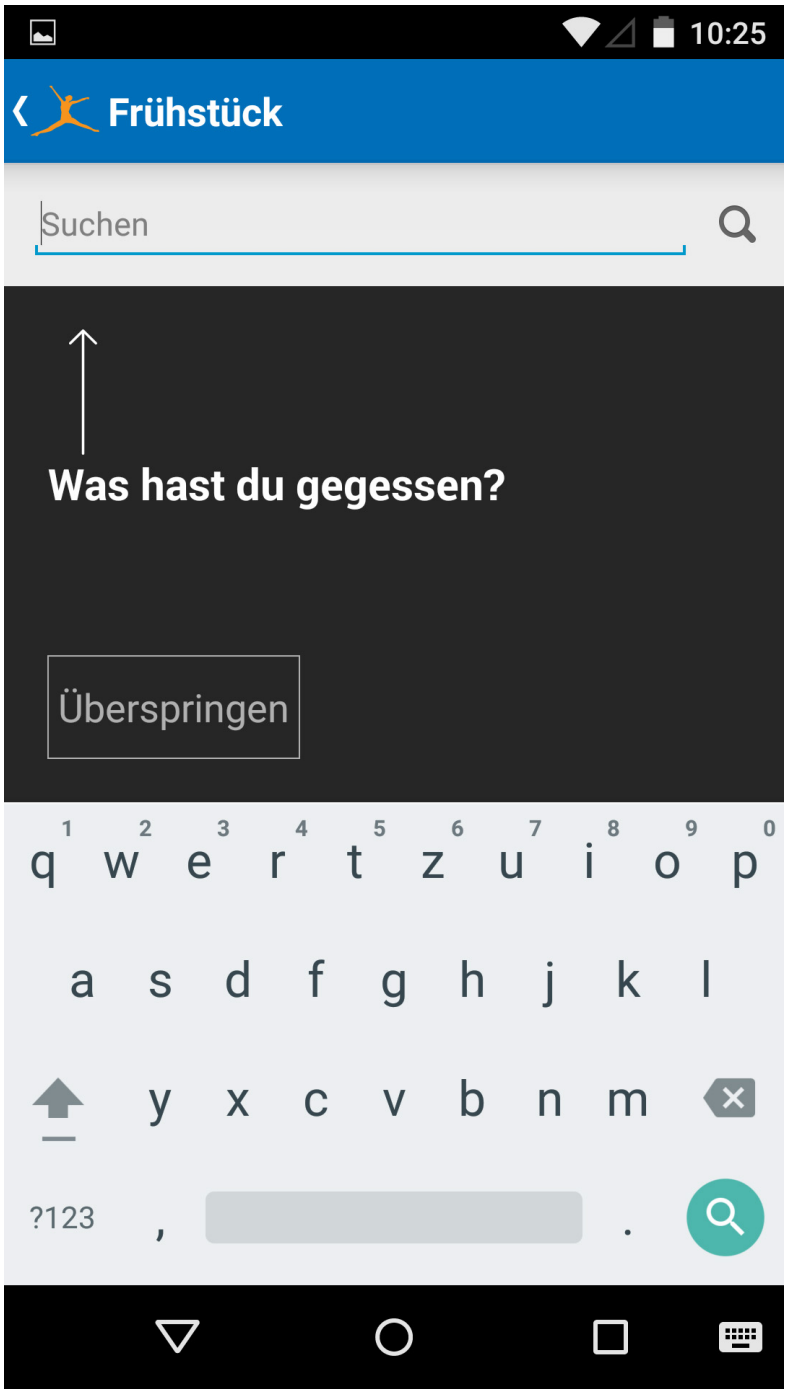


Abbildung 4.69: Kalorienzähler – MyFitnessPal - 14 - Funktionen - Eintrag hinzufügen
Kalorienzähler – MyFitnessPal [75]

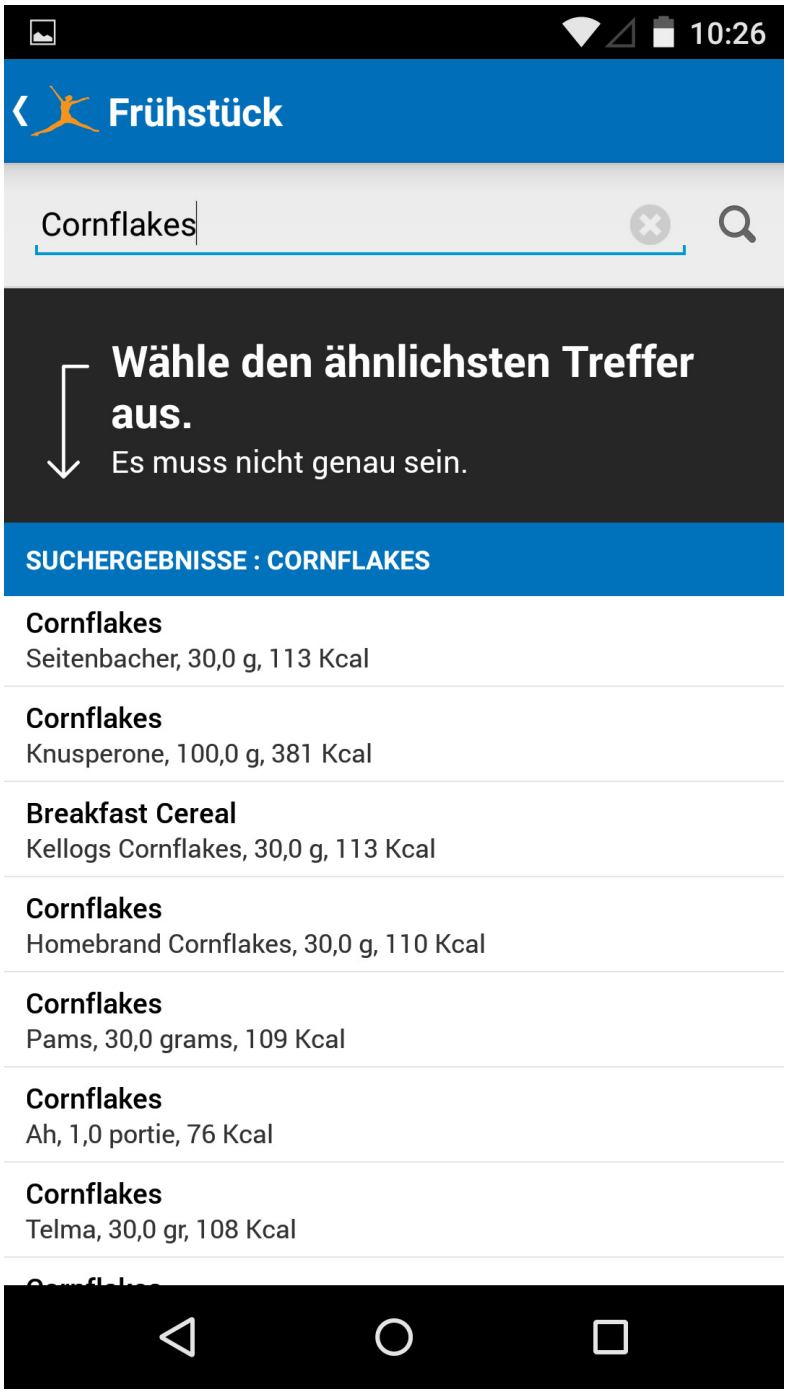


Abbildung 4.70: Kalorienzähler – MyFitnessPal - 15 - Funktionen - Eintrag hinzufügen
Kalorienzähler – MyFitnessPal [75]

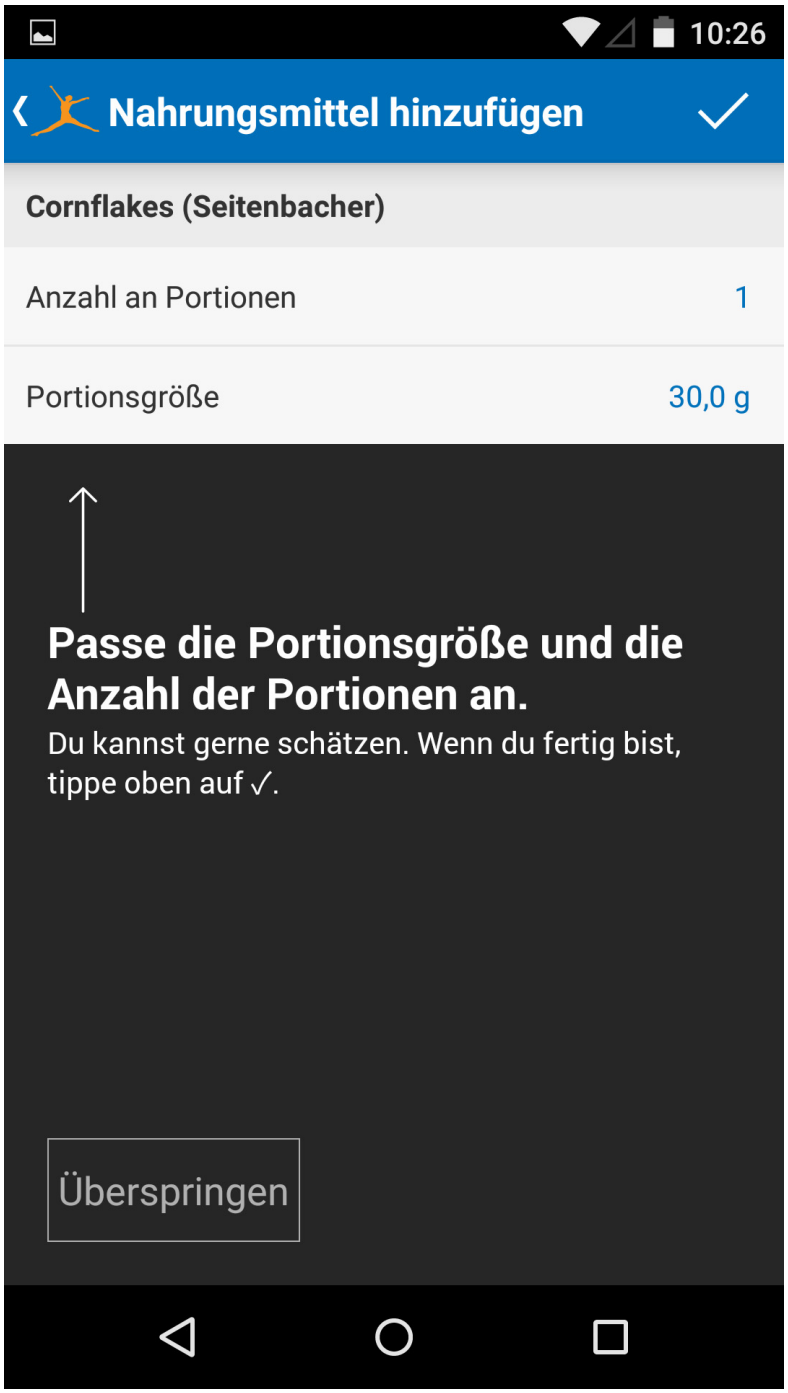


Abbildung 4.71: Kalorienzähler – MyFitnessPal - 16 - Funktionen - Eintrag hinzufügen
Kalorienzähler – MyFitnessPal [75]

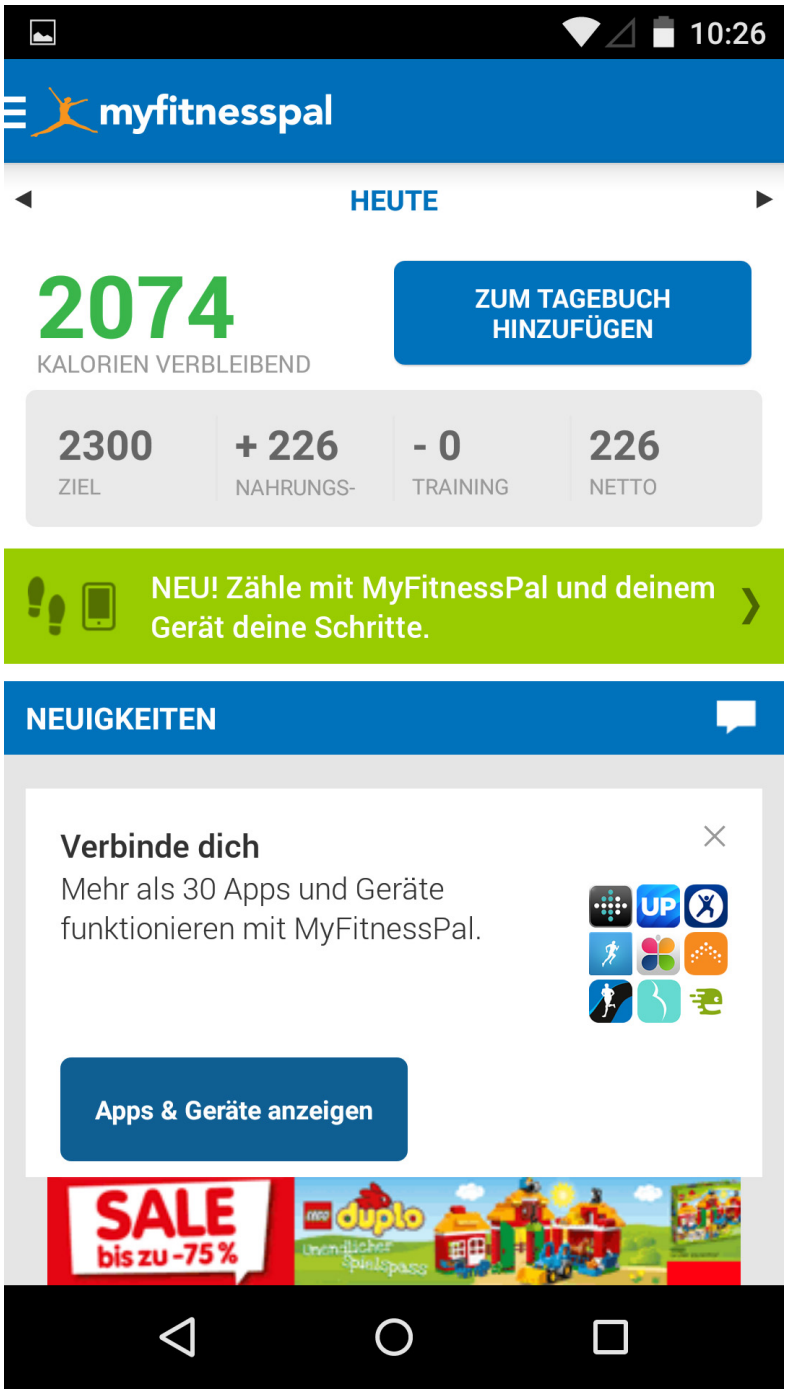


Abbildung 4.72: Kalorienzähler – MyFitnessPal - 17 - Funktionen - Start
Kalorienzähler – MyFitnessPal [75]

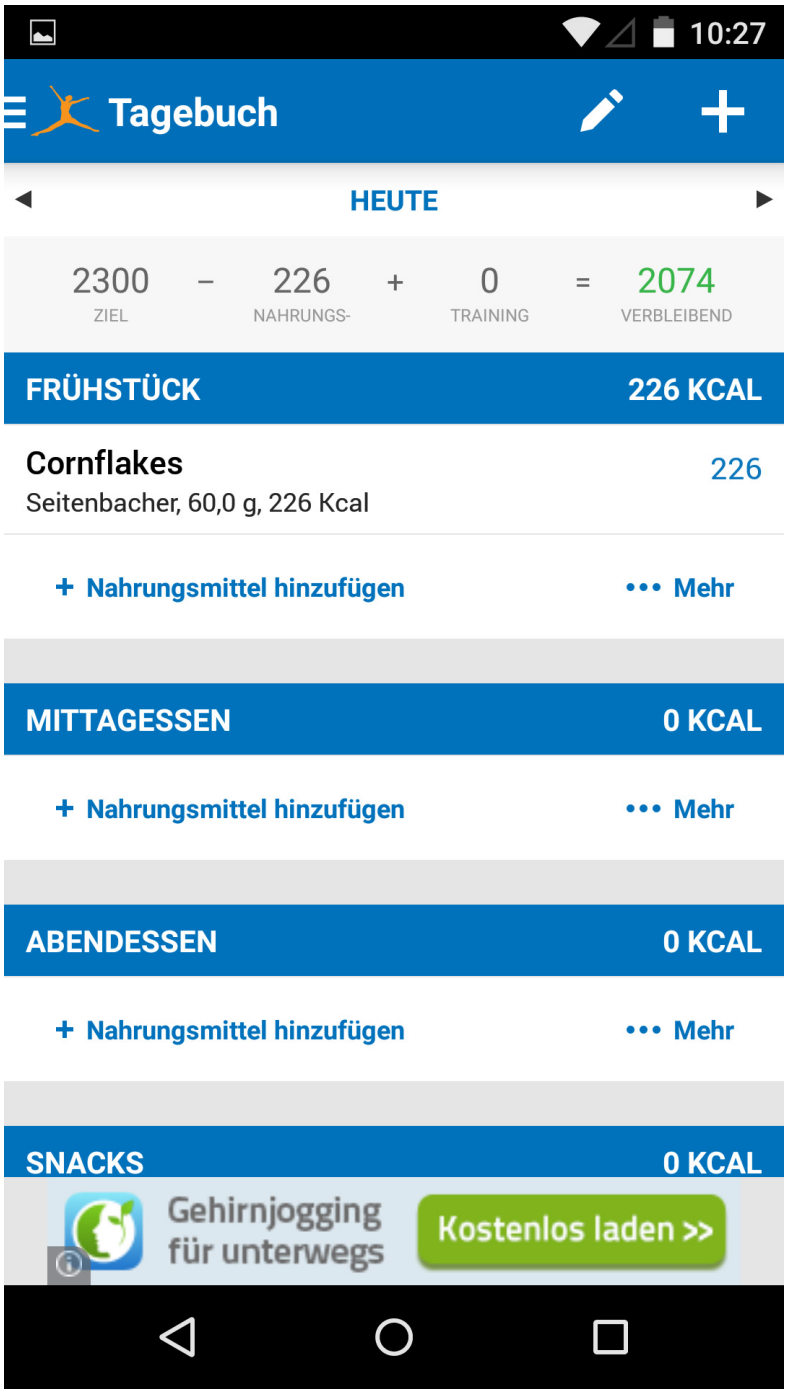
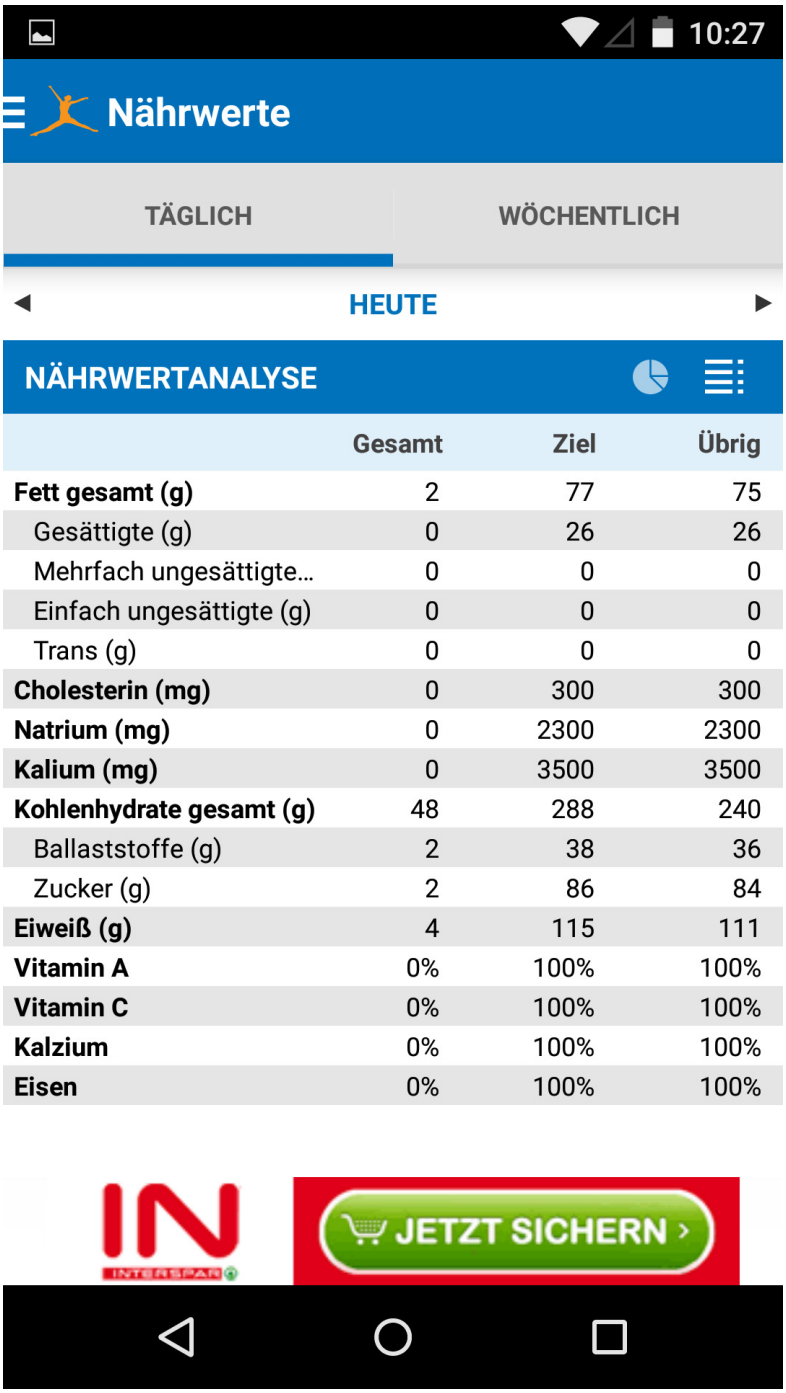


Abbildung 4.73: Kalorienzähler – MyFitnessPal - 18 - Funktionen - Tagebuch
Kalorienzähler – MyFitnessPal [75]



	Gesamt	Ziel	Übrig
Fett gesamt (g)	2	77	75
Gesättigte (g)	0	26	26
Mehrfach ungesättigte...	0	0	0
Einfach ungesättigte (g)	0	0	0
Trans (g)	0	0	0
Cholesterin (mg)	0	300	300
Natrium (mg)	0	2300	2300
Kalium (mg)	0	3500	3500
Kohlenhydrate gesamt (g)	48	288	240
Ballaststoffe (g)	2	38	36
Zucker (g)	2	86	84
Eiweiß (g)	4	115	111
Vitamin A	0%	100%	100%
Vitamin C	0%	100%	100%
Kalzium	0%	100%	100%
Eisen	0%	100%	100%

Abbildung 4.74: Kalorienzähler – MyFitnessPal - 19 - Funktionen - Nährwerte
Kalorienzähler – MyFitnessPal [75]

Abbildung 4.75: Kalorienzähler – MyFitnessPal - 20 - Funktionen - Meine Rezepte
Kalorienzähler – MyFitnessPal [75]

Abbildung 4.76: Kalorienzähler – MyFitnessPal - 21 - Funktionen - Blog
Kalorienzähler – MyFitnessPal [75]

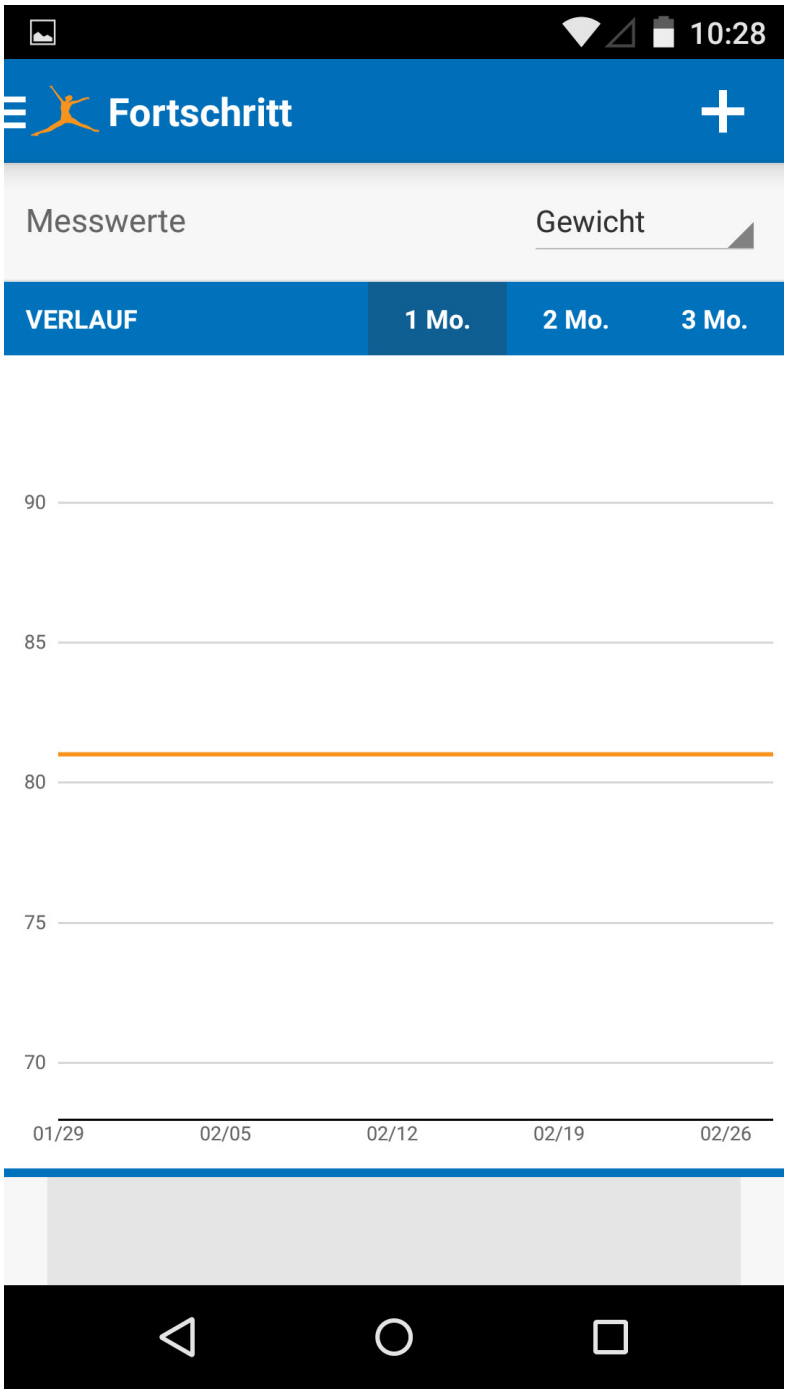


Abbildung 4.77: Kalorienzähler – MyFitnessPal - 22 - Funktionen - Fortschritt
Kalorienzähler – MyFitnessPal [75]

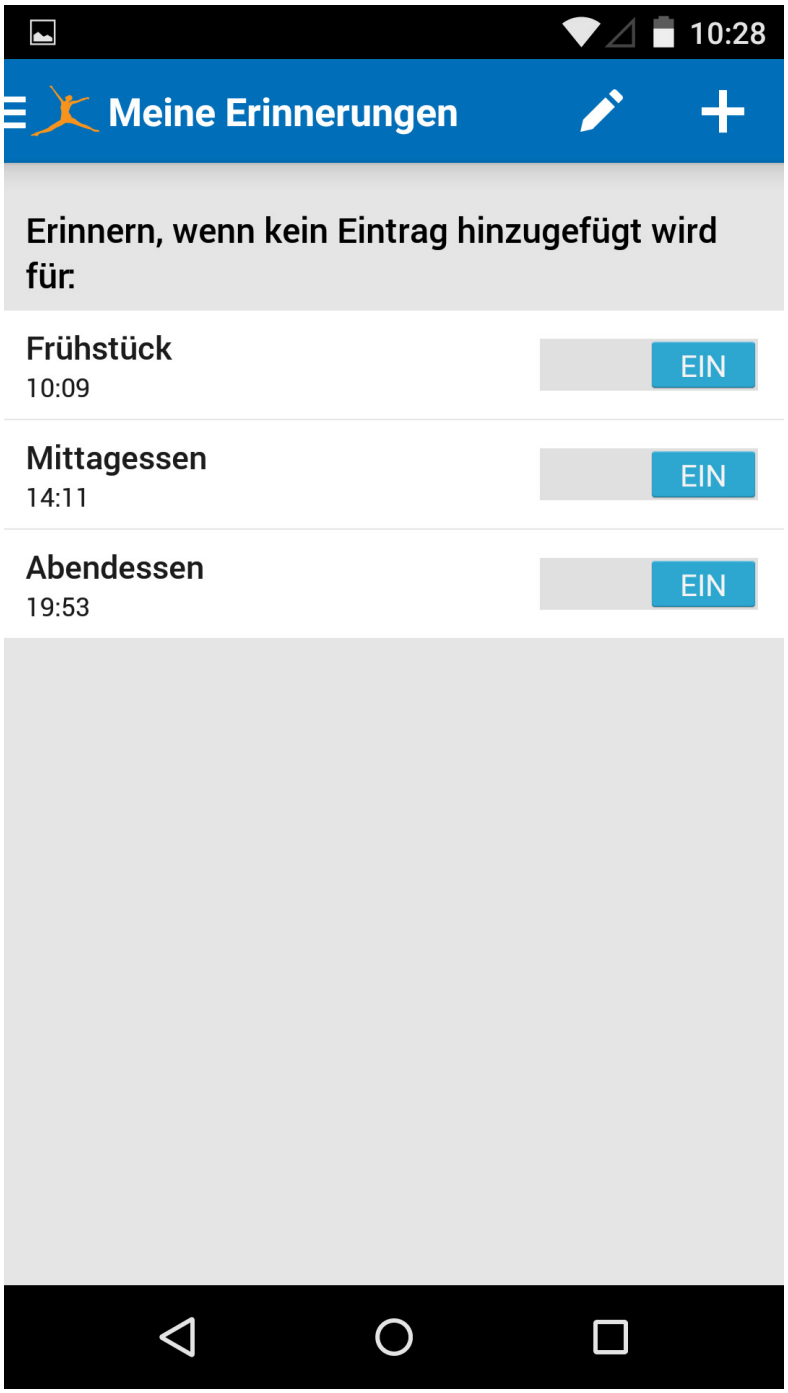


Abbildung 4.78: Kalorienzähler – MyFitnessPal - 23 - Funktionen - Meine Erinnerungen
Kalorienzähler – MyFitnessPal [75]

Abbildung 4.79: Kalorienzähler – MyFitnessPal - 24 - Funktionen - Ziele
Kalorienzähler – MyFitnessPal [75]

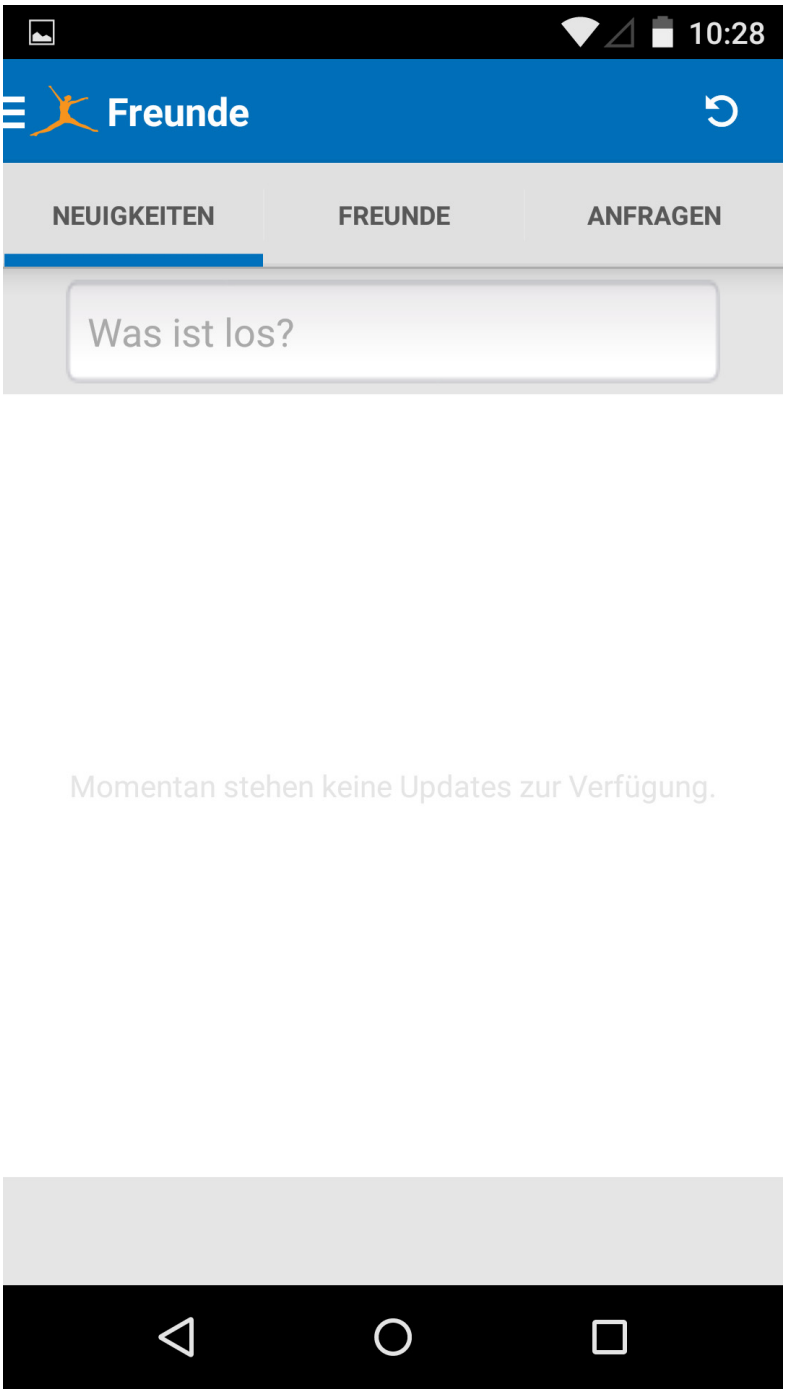


Abbildung 4.80: Kalorienzähler – MyFitnessPal - 25 - Funktionen - Freunde
Kalorienzähler – MyFitnessPal [75]

Abbildung 4.81: Kalorienzähler – MyFitnessPal - 26 - Funktionen - Nachrichten
Kalorienzähler – MyFitnessPal [75]

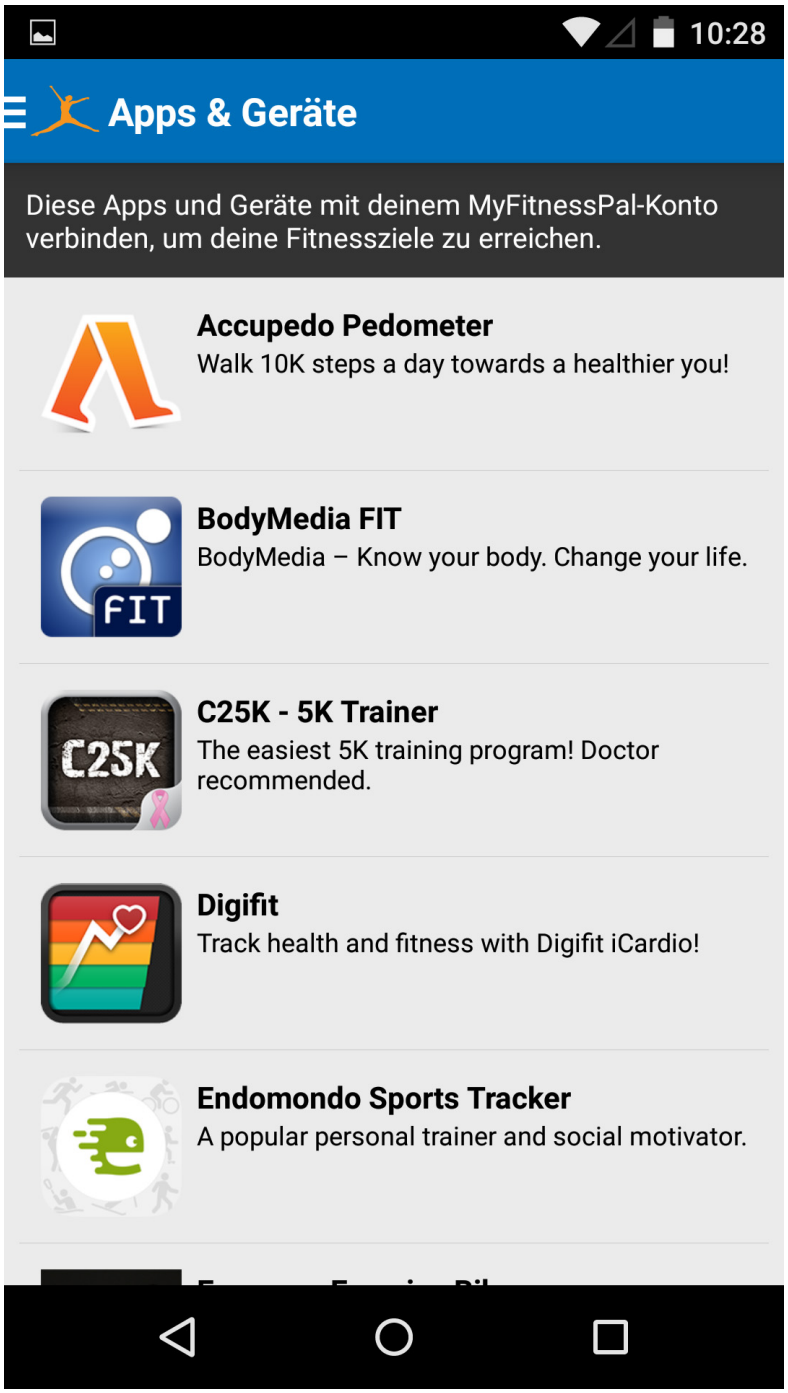


Abbildung 4.82: Kalorienzähler – MyFitnessPal - 27 - Funktionen - Apps & Geräte
Kalorienzähler – MyFitnessPal [75]

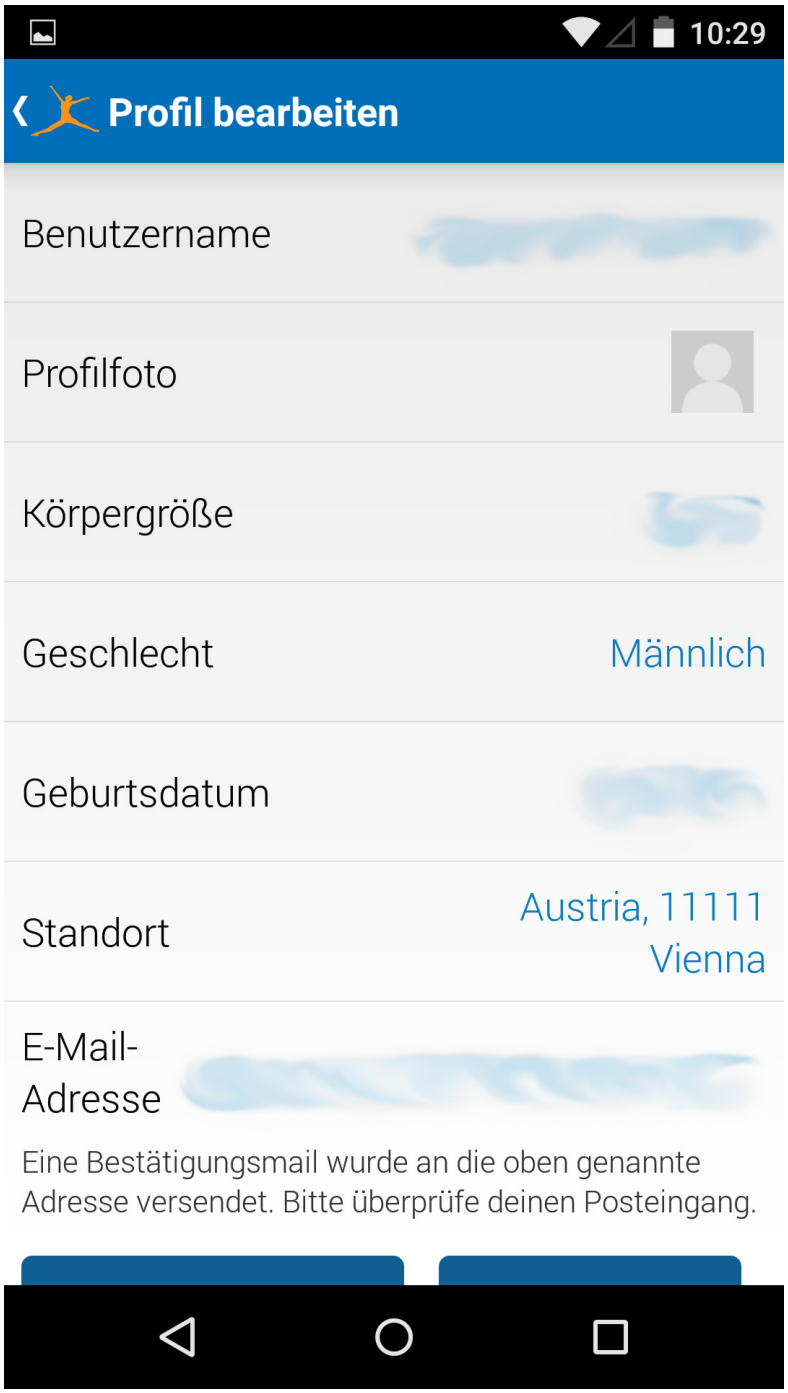


Abbildung 4.83: Kalorienzähler – MyFitnessPal - 28 - Privatsphäre
Kalorienzähler – MyFitnessPal [75]

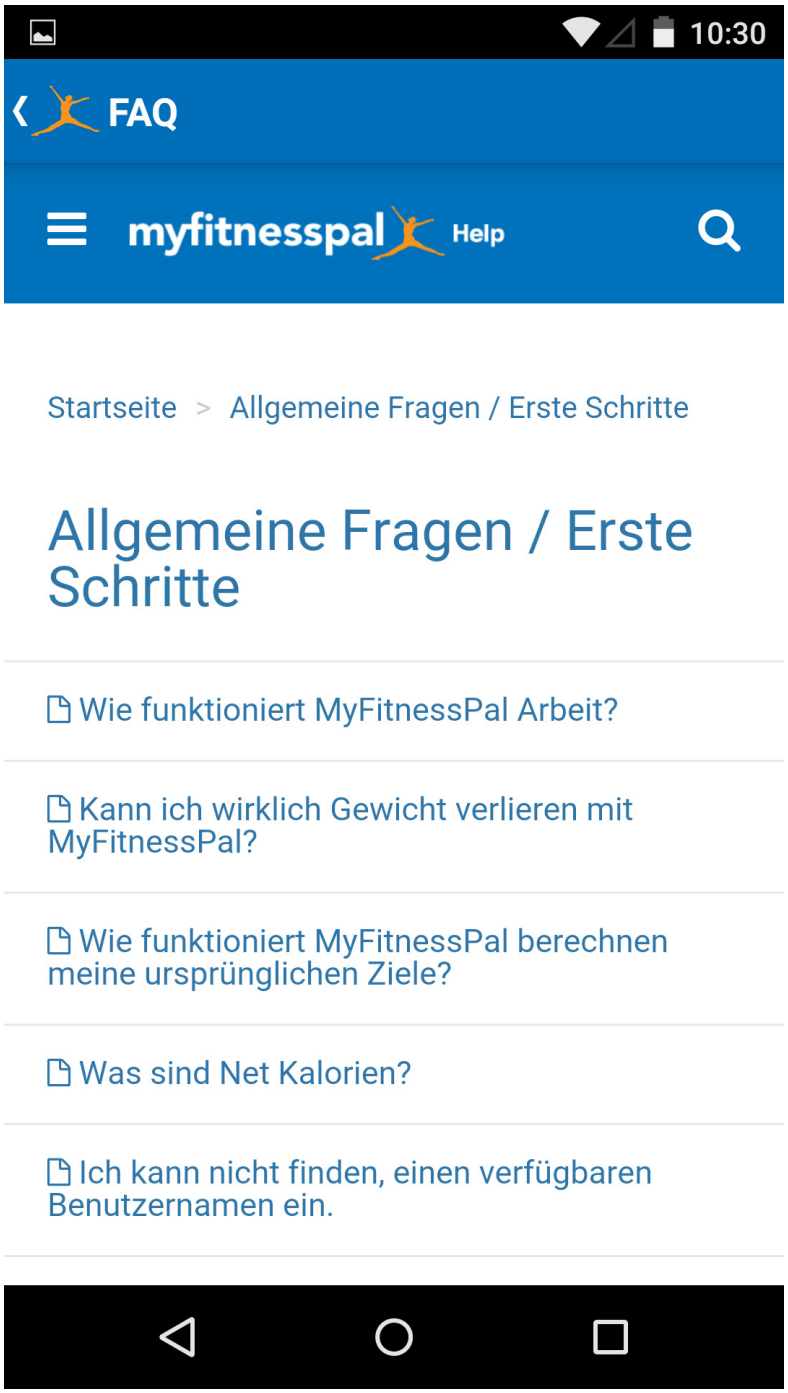


Abbildung 4.84: Kalorienzähler – MyFitnessPal - 29 - FAQ
Kalorienzähler – MyFitnessPal [75]

KAPITEL 5

Gegenüberstellung der Anwendungen

In diesem Kapitel wird eine direkte Gegenüberstellung der fünf exemplarisch getesten Apps in Form einer Tabelle mit definierten Fragen gezeigt, um einen Überblick der Situation zu erlangen. Die Fragestellung zu den einzelnen Punkten wurde explizit dahingehend gewählt, dass eine positive Antwort, ergo ein „JA“, datenschutzrechtliche Bedenken oder Risiken ausdrücken soll. Somit ist es nachfolgend leichter, mit einem Blick die Situation hinsichtlich des Datenschutzes pro Produkt zu erfassen.

Tabelle 5.1: Gegenüberstellung der Anwendungen

	Runtastic	**Google Fit**	**FitNotes**	**Endomondo**	**MyFitnessPal**
Vertragspartner schwer oder unklar erkennbar?	NEIN	NEIN	-	JA	JA
Firmensitz außerhalb EU?	NEIN	JA	-	NEIN	JA
Verwendung eines Benutzerkontos möglich?	JA	JA	NEIN	JA	JA
Benutzerkonto für Verwendung erforderlich?	NEIN	JA	-	JA	JA
Synchronisieren der Daten in Cloud?	JA	JA	-	JA	JA
Synchronisation verpflichtend?	NEIN	JA	-	JA	JA
Datentransfer in Drittstaat?	NEIN	JA	-	NEIN	JA
Personenbezogene Daten gesammelt?	JA	JA	NEIN	JA	JA
Sensible Daten gesammelt?	JA	JA	NEIN	JA	JA
Gesundheitsdaten gesammelt?	JA	JA	NEIN	JA	JA
Datenschutzbestimmungen schwer auffindbar?	NEIN	NEIN	-	NEIN	JA

Tabelle 5.1 - *Fortsetzung auf der nächsten Seite*

Tabelle 5.1 - *Fortsetzung der vorherigen Seite*

	Runtastic	**Google Fit**	**FitNotes**	**Endomondo**	**MyFitnessPal**
Datenschutzbestimmungen schwer verständlich?	NEIN	NEIN	-	JA	NEIN
Verwendung ohne explizite Zustimmung zu Bestimmungen möglich?	JA	NEIN	-	JA	JA
Weitergabe der Daten an Dritte möglich?	NEIN	JA	-	JA	JA

KAPITEL 6

Ergebnisse

Anhand der Tabelle 5.1 ist leicht erkennbar, dass bei der App Kalorienzähler - MyFitnessPal beinahe alle Fragen bejaht werden müssen. Dies bedeutet, dass im Zusammenhang mit dieser App erhebliche Datenschutzbedenken bestehen. Dicht dahinter liegen Google Fit und Endomondo, wobei Endomondo, trotz seines Firmensitzes innerhalb der EU, mit 11 von 14 positiven Antworten im Vergleich zu 10 von 14 ein wenig schlechter abschneidet als die App aus dem Unternehmen Google. Runtastic aus Österreich verhält sich in diesem Bezug deutlich besser, wenngleich auch keinesfalls fehlerfrei. Lediglich die App FitNotes schnitt komplett unbedenklich ab. Dies ist allerdings aufgrund jeglichen Fehlens einer Datenübertragung an externe Server nicht weiter verwunderlich. Somit kann resümiert werden, dass drei der fünf getesteten Apps große bis sehr große datenschutzrechtliche Bedenken auslösen.

KAPITEL 7

Zusammenfassung und Ausblick

Die aktuelle Rechtslage im Bereich des Datenschutzes ist in Europa derzeit weder für die Wirtschaft noch für den Verbraucher befriedigend. Für beide Seiten stellt sich ein länderspezifisches inhomogenes Feld an Vorschriften dar, welches wenig Rechtssicherheit bietet. Auf Seiten der Unternehmen fehlen Konzernprivilegien zur Übertragung der Daten innerhalb des Unternehmens sowie eindeutige einheitliche Rechtsvorschriften innerhalb des gesamten Europäischen Wirtschaftsraumes. Der Kunde bzw. die Privatperson ist größtenteils überfordert und oftmals vollkommen hilflos sowie uninformiert. Die technologische Entwicklung ist sowohl für den Gesetzgeber als auch für die Privatperson zu schnell erfolgt und die laufenden Veränderungen verschärfen die Situation. Die Thematik ist wesentlich zu umfangreich und komplex, um für die Allgemeinheit leicht erfassbar zu sein. Zusätzlich ist das Verständnis für persönlichen Datenschutz noch längst nicht im Bewusstsein des Einzelnen angekommen. Dies ist der beinahe augenscheinlichen Überrumpelung durch die sprungartige Entwicklung von Internet, Smartphones und dergleichen geschuldet. Dazu kommt, dass viele Entwicklungen in dieser Branche in den Vereinigten Staaten von Amerika entstehen und sich durch die Grenzenlosigkeit des Internets auf der ganzen Welt innerhalb von Augenblicken ausbreiten können. Freilich ergibt sich durch das grundsätzlich anders geartete Verständnis der USA betreffend Datenschutz eine unüberwindbar scheinende Differenz zwischen Amerika und Europa. [1] Dies spiegeln auch die Tests in Kapitel 4 wieder, in denen die Apps aus den USA deutlich hinter die aus der EU zurückfallen. Allerdings muss auch die teilweise überraschend schlechte Einhaltung von Datenschutzregulierungen der europäischen Produkte erwähnt werden. [2] In diesem Bereich ist dringender Nachholbedarf festzustellen. Ein definitiv nicht zu vernachlässigender Punkt ist die Datenübertragung in datenschutzrechtlich unsichere Staaten, sogenannte Drittstaaten. Dies ist rein nach europäischem Recht grundsätzlich nur mit Ausnahmeregelungen möglich, allerdings ist die Verfolgung und Sanktionierung kaum durchführbar. [3]

[1] siehe Kapitel 2
[2] siehe Kapitel 4, Kapitel 5 und Kapitel 6
[3] siehe Kapitel 2.4.1

Ein großer Hoffnungsträger scheint die neue EU-Datenschutzgrundverordnung zu sein, welcher bescheinigt wird, viele dieser Probleme zu lösen. Leider wird auch in diesem Kontext bereits seit einiger Zeit, lange vor der Verabschiedung, herbe Kritik laut. [4]

[4] siehe Kapitel 2.2.2

Literatur

Wissenschaftliche Literatur

[1] Stephen B. Adams. “Growing where you are planted: Exogenous firms and the seeding of Silicon Valley”. In: *Research Policy* 40.3 (2011), S. 368 –379. ISSN: 0048-7333. DOI: http://dx.doi.org/10.1016/j.respol.2010.12.002. URL: http://www.sciencedirect.com/science/article/pii/S0048733310002532.

[2] Jan Philipp Albrecht. “Starker EU-Datenschutz wäre Standortvorteil”. German. In: *Datenschutz und Datensicherheit - DuD* 37.10 (2013), S. 655–657. ISSN: 1614-0702. DOI: 10.1007/s11623-013-0270-3. URL: http://dx.doi.org/10.1007/s11623-013-0270-3.

[7] Gerald Auer. *Erschließung des ländlichen Raums durch Breitband-Internet*. Dipl.-Arb., Techn. Univ. Wien, Österreich, 2010.

[10] Lukas Bauer und Sebastian Reimer [Hrsg.] *Handbuch Datenschutzrecht; [Videoüberwachung, E-Government, Arbeitsrecht, Steuerrecht, Unternehmenskauf, Sicherheitspolizei]*. Wien: Facultas Verl., 2009. ISBN: 978-3-7089-0509-9.

[12] Eric Bodden u. a. “Schutzmaßnahmen gegen datenschutz-unfreundliche Smartphone-Apps”. German. In: *Datenschutz und Datensicherheit - DuD* 37.11 (2013), S. 720–725. ISSN: 1614-0702. DOI: 10.1007/s11623-013-0300-1. URL: http://dx.doi.org/10.1007/s11623-013-0300-1.

[15] Phillip W. Brunst. *Anonymität im Internet - rechtliche und tatsächliche Rahmenbedingungen; zum Spannungsfeld zwischen einem Recht auf Anonymität bei der elektronischen Kommunikation und den Möglichkeiten zur Identifizierung und Strafverfolgung*. Schriftenreihe des Max-Planck-Instituts für ausländisches und internationales Strafrecht : Reihe S, Strafrechtliche Forschungsberichte ; 117. Zugl.: Erlangen-Nürnberg, Univ., Diss., 2009. Berlin: Duncker und Humblot, 2009. ISBN: 978-3-428-13179-2; 978-3-86113-854-9.

[27] Gerald Dietl. *Mobile Computing - Innovationen und Trends für Hardware und Software*. Wien, Österreich, 2008.

[32] Jeffrey Erman, Alexandre Gerber und Subhabrata Sen. “HTTP in the home: it is not just about PCs”. In: HomeNets ’10 (2010), S. 43–48. DOI: 10.1145/1851307.1851319. URL: http://doi.acm.org/10.1145/1851307.1851319.

[35] Thomas A. Friedrich. “International: EU-Datenschutzrecht soll vereinheitlicht werden”. In: *Versicherungswirtschaft, 2012, Vol.67(17), p.1266* (2012). ISSN: 0042-4358.

[37] Hartmut Gehring u. a. “Zukunftstrend „Medical Apps“”. German. In: *Bundesgesundheitsblatt - Gesundheitsforschung - Gesundheitsschutz* 57.12 (2014), S. 1402–1410. ISSN: 1436-9990. DOI: 10.1007/s00103-014-2061-x. URL: http://dx.doi.org/10.1007/s00103-014-2061-x.

[38] Ivo Geis. “Datenschutzrecht in der internationalen Netzgesellschaft”. In: *Datenschutz-Berater, 2012(9), p.188* (2012). ISSN: 0170-7256.

[40] Thomas Giesen. “Für ein verfassungsgemäßes Datenschutzrecht in Europa: Wann beginnt die EU, sich auf ihre freiheitlichen Prinzipien zu besinnen?” In: *Computer und Recht, 2014, Vol.30(8), pp.550-556* (2014).

[44] Wolfgang Graf. *Datenschutzrecht im Überblick*. 2., überarb. Aufl. Manual. Wien: Facultas.WUV, 2010. ISBN: 978-3-7089-0596-9.

[45] Sabine Grapentin. “Haftung und anwendbares Recht im internationalen Datenverkehr: EU-Standardvertragsklauseln und Binding Corporate Rules; Computer und Recht”. In: *Computer und Recht, 2011, Vol.27(2), pp.102-107* (2011). ISSN: 0179-1990.

[47] Christopher Götz. “Grenzüberschreitende Datenübermittlung im Konzern”. German. In: *Datenschutz und Datensicherheit - DuD* 37.10 (2013), S. 631–637. ISSN: 1614-0702. DOI: 10.1007/s11623-013-0266-z. URL: http://dx.doi.org/10.1007/s11623-013-0266-z.

[48] Marit Hansen. “Datenschutz nach dem Summer of Snowden”. German. In: *Datenschutz und Datensicherheit - DuD* 38.7 (2014), S. 439–444. ISSN: 1614-0702. DOI: 10.1007/s11623-014-0203-9. URL: http://dx.doi.org/10.1007/s11623-014-0203-9.

[49] Simone Gräfin von Hardenberg. “Individualisierte Medizin in den USA”. German. In: *Datenschutz und Datensicherheit - DuD* 38.9 (2014), S. 619–622. ISSN: 1614-0702. DOI: 10.1007/s11623-014-0240-4. URL: http://dx.doi.org/10.1007/s11623-014-0240-4.

[52] Jens Heider. “Die Gretchenfrage: Wie halten Sie’s mit der App-Sicherheit?” German. In: *Datenschutz und Datensicherheit - DuD* 38.1 (2014), S. 15–19. ISSN: 1614-0702. DOI: 10.1007/s11623-014-0005-0. URL: http://dx.doi.org/10.1007/s11623-014-0005-0.

[53] Jörg Hladjk. “EU-Datenschutzrecht und Geolocation-Services”. In: *Datenschutz-Berater, 2011(7-8), p.9* (2011). ISSN: 0170-7256.

[55] Andreas Höpken und Helmut Neumann. *Datenschutz in der Arztpraxis; ein Leitfaden für den Umgang mit Patientendaten*. 2. Aufl. Frechen: Datakontext, 2008. ISBN: 978-3-89577-521-5.

[56] Niko Härting. “Datenschutzreform in Europa: Einigung im EU-Parlament: Kritische Anmerkungen; Computer und Recht”. In: *Computer und Recht, 2013, Vol.29 (11), pp.715-721* (2013). ISSN: 0179-1990.

[73] Dietmar Jahnel, Alfred Schramm und Elisabeth Staudegger [Hrsg.] *Informatikrecht*. Springers Kurzlehrbücher der Rechtswissenschaft. Wien [u.a.]: Springer, 2000. ISBN: 3-211-83279-3.

[74] Dietmar Jahnel, Stefan Siegwart und Natalie Fercher [Hrsg.] *Aktuelle Fragen des Datenschutzrechts; [Datensicherheit ; Datengeheimnis ; manuelle Dateien ; Videoüberwachung ; Whistleblowing u.v.m.]* Wien: Facultas.WUV, 2007. ISBN: 978-3-7089-0057-5.

[76] Margot Kellner. *Europol - das Spannungsverhältnis zwischen Sicherheit und Grundrechten*. Wien, Univ., Diss. 2007.

[77] Rainer Knyrim. *Datenschutzrecht; Praxishandbuch für richtiges Registrieren, Verarbeiten, Übermitteln, Zustimmen, Outsourcen, Werben uvm*. 2., vollst. überarb. Aufl. Wien: Manz, 2012. ISBN: 978-3-214-00687-7.

[78] Michael Kort. "Datenschutzrecht in der Europäischen Union: de lege lata und de lege ferenda". In: *Der Betrieb, 2012, Vol.(18), p.1020* (). ISSN: 0005-9935.

[79] Philipp Kramer. "Licht und Schatten im künftigen EU-Datenschutzrecht". In: *Datenschutz-Berater, 2012(3), p.57* (2012). ISSN: 0170-7256.

[82] Viktor Mayer-Schönberger [Hrsg.] und Ernst O. Brandl. *Datenschutzgesetz; Grundsätze und europarechtliche Rahmenbedingungen ; Gesetzestext mit Materialien ; Datenschutz-Verordnungen und Richtlinien im Anhang*. 2., überarb. Aufl. Fachbuch Recht. Früher u.d.T. Datenschutzgesetz 2000 / Bearb. von Viktor Mayer-Schönberger. Wien: Linde, 2006. ISBN: 3-7073-0869-3.

[85] Flemming Moos. *Datenschutzrecht; schnell erfasst*. Recht - schnell erfasst. Berlin [u.a.]: Springer, 2006. ISBN: 978-3-540-23689-4; 3-540-23689-9.

[87] o.A. "Datenschutzrecht: Neue Leitlinien für EU-Unternehmen bei der Nutzung der Cloud". In: *Europäische Zeitschrift für Wirtschaftsrecht, 2014, Vol.(14), p.525* (2014). ISSN: 0937-7204.

[88] o.A. "Ein neues Datenschutzrecht für Europa". In: *Zeitschrift für Rechtspolitik, 2012(07), p.193* (2012). ISSN: 0514-6496.

[89] o.A. "Leitfaden für mehr App-Sicherheit im Geschäftsumfeld". German. In: *Datenschutz und Datensicherheit - DuD* 38.7 (2014), S. 501–501. ISSN: 1614-0702. DOI: 10.1007/s11623-014-0227-1. URL: http://dx.doi.org/10.1007/s11623-014-0227-1.

[90] o.A. "LG Frankfurt: Unzulässigkeit von App-Store-AGB". German. In: *Datenschutz und Datensicherheit - DuD* 37.12 (2013), S. 810–812. ISSN: 1614-0702. DOI: 10.1007/s11623-013-0334-4. URL: http://dx.doi.org/10.1007/s11623-013-0334-4.

[91] o.A. "Sealed Cloud schließt IT-Sicherheitslücke "Mensch"". German. In: *Datenschutz und Datensicherheit - DuD* 37.5 (2013), S. 333. ISSN: 1614-0702. DOI: 10.1007/s11623-013-0130-1.

[92] o.A. "Tätigkeitsvorausschau des EDSB für 2014: Datenschutz im Herzen der EU-Politik". German. In: *Datenschutz und Datensicherheit - DuD* 38.3 (2014), S. 146–146. ISSN: 1614-0702. DOI: 10.1007/s11623-014-0064-2. URL: http://dx.doi.org/10.1007/s11623-014-0064-2.

[93] Matthias Orthwein und Katrin Anna Rücker. “Kann Europa von Kalifornien Datenschutz lernen?” German. In: *Datenschutz und Datensicherheit - DuD* 38.9 (2014), S. 613–618. ISSN: 1614-0702. DOI: 10.1007/s11623-014-0239-x. URL: http://dx.doi.org/10.1007/s11623-014-0239-x.

[95] Hans Jürgen Pollirer, Ernst M. Weiss und Rainer Knyrim. *Datenschutzgesetz 2000; (DSG 2000) ; samt ausführlichen Erläuterungen ; [idF der DSG-Novelle 2010]; DSG*. Manzsche Gesetzausgaben : Sonderausgabe ; 115. Nebent. DSG; Gilt als Sonder-Erg.-Lfg. 9a zu Datenschutzrecht. Wien: Manz, 2010. ISBN: 978-3-214-13401-3; 978-3-214-13403-7; 978-3-214-13402-0.

[100] Helmut Reimer. “Merkel: Acht-Punkte-Programm für einen europäischen und internationalen Datenschutz”. German. In: *Datenschutz und Datensicherheit - DuD* 37.10 (2013), S. 675–675. ISSN: 1614-0702. DOI: 10.1007/s11623-013-0276-x. URL: http://dx.doi.org/10.1007/s11623-013-0276-x.

[107] Alexander Roßnagel, Silke Jandt und Philipp Richter. “Die Zulässigkeit der Übertragung personenbezogener Daten in die USA im Kontext der NSA-Überwachung”. German. In: *Datenschutz und Datensicherheit - DuD* 38.8 (2014), S. 545–551. ISSN: 1614-0702. DOI: 10.1007/s11623-014-0181-y. URL: http://dx.doi.org/10.1007/s11623-014-0181-y.

[110] Lennart Schüßler und Oliver Zöll. “EU-Datenschutz-Grundverordnung und Beschäftigtendatenschutz”. German. In: *Datenschutz und Datensicherheit - DuD* 37.10 (2013), S. 639–643. ISSN: 1614-0702. DOI: 10.1007/s11623-013-0267-y. URL: http://dx.doi.org/10.1007/s11623-013-0267-y.

[111] Jochen Schneider und Niko Härting. “Datenschutz in Europa – Plädoyer für einen Neubeginn: Zehn „Navigationsempfehlungen“, damit das EU-Datenschutzrecht internettauglich und effektiv wird”. In: *Computer und Recht, 2014, Vol.30(5), pp.306-312* (2014). ISSN: 0179-1990.

[113] Axel Spies und Oliver Stutz. “Microsoft als Initialzünder für mehr Datenschutz in den USA?” German. In: *Datenschutz und Datensicherheit - DuD* 30.3 (2006), S. 170–176. ISSN: 1614-0702. DOI: 10.1007/s02045-006-0048-z. URL: http://dx.doi.org/10.1007/s02045-006-0048-z.

[118] Bettina Temath. *Kulturelle Parameter in der Werbung: Deutsche und US-amerikanische Automobilanzeigen im Vergleich*. VS Verlag für Sozialwissenschaften, 2010. ISBN: 978-3531926353. URL: https://books.google.at/books?id=t10fBAAAQBAJ.

[121] Marie-Theres Tinnefeld und Benedikt Buchner. “Rechtliche und technische Rettungsanker für Privatheit und Datenschutz”. German. In: *Datenschutz und Datensicherheit - DuD* 38.9 (2014), S. 581–582. ISSN: 1614-0702. DOI: 10.1007/s11623-014-0231-5. URL: http://dx.doi.org/10.1007/s11623-014-0231-5.

[122] Marie-Theres Tinnefeld, Eugen Ehmann und Rainer W. Gerling. *Einführung in das Datenschutzrecht; Datenschutz und Informationsfreiheit in europäischer Sicht*. 4., völlig neu bearb. u. erw. Aufl. München ; Wien: Oldenbourg, © 2005 [erschienen 2004]; 2004. ISBN: 3-486-27303-5.

[123] Fred Turner. “Exhibition: Shots of Silicon Valley”. In: *Nature, 2008, Vol.451(7182), p.1054* (). ISSN: 0028-0836.

[124] Jens Chr. Hammersen und Ulrich Eisenried. “Datenübermittlung in Nicht-EU-Staaten: rechtliche Probleme”. In: *Bank und Markt, 2013, Vol.(11), p.21* (). ISSN: 1433-5204.

[127] Friederike Voskamp, Dennis-Kenji Kipker und Richard Yamato. “Grenzüberschreitende Datenschutzregulierung im Pazifik-Raum”. German. In: *Datenschutz und Datensicherheit - DuD* 37.7 (2013), S. 452–456. ISSN: 1614-0702. DOI: 10.1007/s11623-013-0177-z. URL: http://dx.doi.org/10.1007/s11623-013-0177-z.

[128] Markus Wagner. *Das Safe-Harbor Modell; Datenschutzbestimmungen in der Relation EU-USA*. Parallelt. [Übers. des Autors] The Safe-Harbor model - Privacy in relation between the EU and the USA; Wien, Techn. Univ., Dipl.-Arb. 2011.

[131] Thilo Weichert. “Big Data, Gesundheit und der Datenschutz”. German. In: *Datenschutz und Datensicherheit - DuD* 38.12 (2014), S. 831–838. ISSN: 1614-0702. DOI: 10.1007/s11623-014-0328-x. URL: http://dx.doi.org/10.1007/s11623-014-0328-x.

[132] Thilo Weichert. “Freihandelsabkommen contra Datenschutz?” German. In: *Datenschutz und Datensicherheit - DuD* 38.12 (2014), S. 850–856. ISSN: 1614-0702. DOI: 10.1007/s11623-014-0331-2. URL: http://dx.doi.org/10.1007/s11623-014-0331-2.

[134] Mirko Wieczorek. “Der räumliche Anwendungsbereich der EU-Datenschutz Grundverordnung”. German. In: *Datenschutz und Datensicherheit - DuD* 37.10 (2013), S. 644–649. ISSN: 1614-0702. DOI: 10.1007/s11623-013-0268-x. URL: http://dx.doi.org/10.1007/s11623-013-0268-x.

[135] Jarunee Wonglimpiyarat. “The dynamic economic engine at Silicon Valley and US Government programmes in financing innovations”. In: *Technovation* 26.9 (2006), S. 1081–1089. ISSN: 0166-4972. DOI: http://dx.doi.org/10.1016/j.technovation.2005.09.005. URL: http://www.sciencedirect.com/science/article/pii/S0166497205001215.

Rechtsquellen

[11] *Bill of Rights*. 1791. URL: http://www.archives.gov/exhibits/charters/bill_of_rights.html.

[14] *Breach Notification Law*. 2003. URL: http://www.leginfo.ca.gov/pub/01-02/bill/sen/sb_1351-1400/sb_1386_bill_20020926_chaptered.pdf.

[22] *Charta der Grundrechte der Europäischen Union, Fassung vom 18.12.2000*. 2000. URL: http://www.europarl.europa.eu/charter/pdf/text_de.pdf.

[23] *Children's Online Privacy Protection Act of 1998*. 1998. URL: http://www.law.cornell.edu/uscode/text/15/6501.

[24] *Constitution of the United States*. 1788. URL: http://www.archives.gov/exhibits/charters/constitution.html.

[25] *Datenschutzgesetz 2000, Fassung vom 04.11.2014*. 2014. URL: http://www.ris.bka.gv.at/GeltendeFassung.wxe?Abfrage=bundesnormen&Gesetzesnummer=10001597&FassungVom=2014-11-04.

[26] *Die Europäische Menschenrechtskonvention, Fassung vom 01.06.2010*. 2010. URL: http://www.echr.coe.int/Documents/Convention_DEU.pdf.

[28] *Drivers Privacy Protection Act of 1994*. 1994. URL: http://www.law.cornell.edu/uscode/text/18/2721.

[29] *E-Commerce-Gesetz, Fassung vom 04.11.2014*. 2014. URL: https://www.ris.bka.gv.at/GeltendeFassung.wxe?Abfrage=Bundesnormen&Gesetzesnummer=20001703&FassungVom=2014-11-04.

[33] *Fair Credit Reporting Act of 1970*. 1970. URL: http://www.gpo.gov/fdsys/pkg/STATUTE-84/pdf/STATUTE-84-Pg1114-2.pdf.

[39] *Genetic Information Nondiscrimination Act of 2008*. 2008. URL: http://www.gpo.gov/fdsys/pkg/PLAW-110publ233/pdf/PLAW-110publ233.pdf.

[51] *Health Insurance Portability and Accountability Act of 1996*. 1996. URL: http://www.gpo.gov/fdsys/pkg/PLAW-104publ191/html/PLAW-104publ191.htm.

[84] *Mitteilung der Kommission an das Europäische Parlament und den Rat über die Verbesserung des Datenschutzes durch Technologien zum Schutz der Privatsphäre, Fassung vom 02.05.2007*. 2007. URL: http://eur-lex.europa.eu/legal-content/DE/TXT/PDF/?uri=CELEX:52007DC0228&from=DE.

[97] *Privacy Act of 1974*. 1974. URL: http://www.gpo.gov/fdsys/pkg/STATUTE-88/pdf/STATUTE-88-Pg1896.pdf.

[98] *Privacy Protection Act of 1980*. 1980. URL: http://www.law.cornell.edu/uscode/text/42/2000aa.

[103] *Richtlinie 2002/58/EG des Europäischen Parlaments und des Rates vom 12. Juli 2002 über die Verarbeitung personenbezogener Daten und den Schutz der Privatsphäre in der elektronischen Kommunikation, Fassung vom 12.07.2002*. 2002. URL: http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2002:201:0037:0047:de:PDF.

[104] *Richtlinie 95/46/EG des Europäischen Parlaments und des Rates vom 24. Oktober 1995 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten und zum freien Datenverkehr, Fassung vom 24.10.1995*. 1995. URL: http://eur-lex.europa.eu/legal-content/DE/TXT/PDF/?uri=CELEX:31995L0046&from=DE.

[105] *Richtlinie 97/66/EG des Europäischen Parlaments und des Rates vom 15. Dezember 1997 über die Verarbeitung personenbezogener Daten und den Schutz der Privatsphäre im Bereich der Telekommunikation, Fassung vom 15.12.1997*. 1997. URL: http://eur-lex.europa.eu/legal-content/DE/TXT/PDF/?uri=CELEX:31997L0066&from=DE.

[106] *Right to Financial Privacy Act of 1978*. 1978. URL: http://www.gpo.gov/fdsys/pkg/STATUTE-92/pdf/STATUTE-92-Pg3641.pdf.

[112] *Shine the Light Law*. 2003. URL: http://www.leginfo.ca.gov/cgi-bin/displaycode?section=civ&group=01001-02000&file=1798.80-1798.84.

[116] *Telekommunikationsgesetz 2003, Fassung vom 08.06.2015*. 2015. URL: https://www.ris.bka.gv.at/GeltendeFassung.wxe?Abfrage=Bundesnormen&Gesetzesnummer=20002849&FassungVom=2015-06-08.

[117] *Telephone Consumer Protection Act of 1991*. 1991. URL: http://www.law.cornell.edu/uscode/text/47/227.

[125] *Urteil des Gerichtshofs (Dritte Kammer), 24. November 2011, Verarbeitung personenbezogener Daten – Richtlinie 95/46/EG – Art. 7 Buchst. f – Unmittelbare Wirkung*. 2011. URL: http://curia.europa.eu/juris/document/document.jsf?docid=115205&doclang=de.

[126] *Vorschlag für eine Verordnung des Europäischen Parlaments und des Rates zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten und zum freien Datenverkehr, Fassung vom 25.01.2012*. 2012. URL: http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2012:0011:FIN:DE:PDF.

Online Referenzen

[3] Ron Amadeo. *The history of Android*. 16. Juni 2014. URL: http://arstechnica.com/gadgets/2014/06/building-android-a-40000-word-history-of-googles-mobile-os/ (besucht am 07. 06. 2015).

[4] App Annie. *App Annie Index – Market Q1 2014: Revenue Soars in the United States and China*. URL: http://blog.appannie.com/app-annie-index-market-q1-2014/ (besucht am 20. 02. 2015).

[5] App Annie. *App Annie Index – Market Q2 2013: Google Play Exceeds iOS App Store in App Downloads by 10% in Q2 2013*. URL: http://blog.appannie.com/app-annie-index-market-q2-2013/ (besucht am 20. 02. 2015).

[6] appfigures. *App Stores Growth Accelerates in 2014*. 13. Jan. 2015. URL: http://blog.appfigures.com/app-stores-growth-accelerates-in-2014/ (besucht am 07. 06. 2015).

[8] Android Authority. *15 best Android fitness apps and workout apps*. 18. Nov. 2014. URL: http://www.androidauthority.com/best-android-fitness-apps-and-workout-apps-567999/ (besucht am 22. 02. 2015).

[9] Richard Baguley. *The Gadget We Miss: The Calculator Watch*. 22. Aug. 2013. URL: https://medium.com/people-gadgets/the-gadget-we-miss-the-calculator-watch-e37b006cd53a (besucht am 07. 06. 2015).

[13] Julie Bort. *The History Of The Tablet, An Idea Steve Jobs Stole And Turned Into A Game-Changer*. 2. Juni 2013. URL: http://www.businessinsider.com/history-of-the-tablet-2013-5?op=1&IR=T (besucht am 07. 06. 2015).

[16] Electronic Privacy Information Center. *Children's Online Privacy Protection Act (COPPA)*. URL: https://epic.org/privacy/kids/ (besucht am 29. 01. 2015).

[17] Electronic Privacy Information Center. *Telemarketing and the Telephone Consumer Protection Act (TCPA)*. URL: https://epic.org/privacy/telemarketing/ (besucht am 29. 01. 2015).

[18] Electronic Privacy Information Center. *The Drivers Privacy Protection Act (DPPA) and the Privacy of Your State Motor Vehicle Record*. URL: https://epic.org/privacy/drivers/ (besucht am 28. 01. 2015).

[19] Electronic Privacy Information Center. *The Fair Credit Reporting Act (FCRA) and the Privacy of Your Credit Report*. URL: https://epic.org/privacy/fcra/ (besucht am 28. 01. 2015).

[20] Electronic Privacy Information Center. *The Privacy Protection Act of 1980*. URL: https://epic.org/privacy/ppa/ (besucht am 28. 01. 2015).

[21] Electronic Privacy Information Center. *The Right to Financial Privacy Act*. URL: https://www.epic.org/privacy/rfpa/ (besucht am 28. 01. 2015).

[30] Ben Elgin. *Google Buys Android for Its Mobile Arsenal*. 16. Aug. 205. URL: http://www.webcitation.org/5wk7sIvVb (besucht am 07. 06. 2015).

[31] *Endomondo Running Cycling Walk*. URL: https://play.google.com/store/apps/details?id=com.endomondo.android (besucht am 28. 02. 2015).

[34] *FitNotes - Gym Workout Log*. URL: https://play.google.com/store/apps/details?id=com.github.jamesgay.fitnotes (besucht am 26. 02. 2015).

[36] Futurezone. *Anonymous veröffentlicht tausende WKO-Daten*. 4. Okt. 2011. URL: http://futurezone.at/netzpolitik/anonymous-veroeffentlicht-tausende-wko-daten/24.571.950 (besucht am 29. 01. 2015).

[41] Jason Gilbert. *iPhone App Privacy: Path, Facebook, Twitter And Apple Under Scrutiny For Address Book Controversy*. 15. Feb. 2012. URL: http://www.huffingtonpost.com/2012/02/15/iphone-privacy-app-path-facebook-twitter-apple_n_1279497.html (besucht am 28. 04. 2013).

[42] Google. *Google Nexus 5*. URL: http://www.google.at/nexus/5/ (besucht am 22. 02. 2015).

[43] *Google Fit*. URL: https://play.google.com/store/apps/details?id=com.google.android.apps.fitness (besucht am 25. 02. 2015).

[46] GSMArena. *iPhone*. URL: http://www.gsmarena.com/apple_iphone-1827.php (besucht am 07. 06. 2015).

[50] Adam Hartung. *The Reason Why Google Glass, Amazon Fire Phone and Segway All Failed*. 15. Feb. 2015. URL: http://www.forbes.com/sites/adamhartung/2015/02/12/the-reason-why-google-glass-amazon-firephone-and-segway-all-failed/ (besucht am 07. 06. 2015).

[54] Marc Hoffmann. *Apple HealthKit in US-Krankenhäuser immer öfter eingesetzt*. 5. Feb. 2015. URL: http://www.pocketpc.ch/magazin/news/apple-healthkit-us-krankenhaeuser-immer-oefter-eingesetzt-20330/ (besucht am 06. 04. 2015).

[57] IDC. *Smartphone Market Share*. URL: http://www.idc.com/prodserv/smartphone-os-market-share.jsp (besucht am 18. 02. 2015).

[58] IDC. *Tablet Market Share*. 14. Juli 2014. URL: http://www.idc.com/getdoc.jsp?containerId=prUS25008314 (besucht am 18. 02. 2015).

[59] ITWissen. *Android*. URL: http://www.itwissen.info/definition/lexikon/Android.html (besucht am 07. 06. 2015).

[60] ITWissen. *BlackBerry*. URL: http://www.itwissen.info/definition/lexikon/BlackBerry-BlackBerry.html (besucht am 07. 06. 2015).

[61] ITWissen. *Fitness-Tracker*. URL: http://www.itwissen.info/definition/lexikon/Fitness-Tracker-fitness-tracker.html (besucht am 07. 06. 2015).

[62] ITWissen. *Intelligente Kleidung*. URL: http://www.itwissen.info/definition/lexikon/Intelligente-Kleidung-smart-clothes.html (besucht am 07. 06. 2015).

[63] ITWissen. *Intelligentes Armband*. URL: http://www.itwissen.info/definition/lexikon/Intelligentes-Armband-smart-bracelet.html (besucht am 07. 06. 2015).

[64] ITWissen. *iOS*. URL: http://www.itwissen.info/definition/lexikon/iPhone-OS.html (besucht am 07. 06. 2015).

[65] ITWissen. *iPad*. URL: http://www.itwissen.info/definition/lexikon/iPad-iPad.html (besucht am 07. 06. 2015).

[66] ITWissen. *iPhone*. URL: http://www.itwissen.info/definition/lexikon/iPhone-iPhone.html (besucht am 07. 06. 2015).

[67] ITWissen. *Smart Glasses*. URL: http://www.itwissen.info/definition/lexikon/smart-glasses-Datenbrille.html (besucht am 07. 06. 2015).

[68] ITWissen. *Smart Wearables*. URL: http://www.itwissen.info/definition/lexikon/Smart-Wearables-smart-wearables.html (besucht am 07. 06. 2015).

[69] ITWissen. *Smartphone*. URL: http://www.itwissen.info/definition/lexikon/Smartphone-smart-phone.html (besucht am 07. 06. 2015).

[70] ITWissen. *Smartwatch*. URL: http://www.itwissen.info/definition/lexikon/smartwatch-Computeruhr.html (besucht am 07. 06. 2015).

[71] ITWissen. *Tablet*. URL: http://www.itwissen.info/definition/lexikon/Tafel-PC-tablet-PC.html (besucht am 07. 06. 2015).

[72] ITWissen. *Windows Phone*. URL: http://www.itwissen.info/definition/lexikon/Windows-Phone-Windows-Phone.html (besucht am 07. 06. 2015).

[75] *Kalorienzähler – MyFitnessPal*. URL: https://play.google.com/store/apps/details?id=com.myfitnesspal.android (besucht am 28. 02. 2015).

[80] Stephen Lawson. *Android Market Needs More Filters, T-Mobile Says*. 17. März 2009. URL: http://www.pcworld.com/article/161410/article.html (besucht am 07. 06. 2015).

[81] Taylor Martin. *The evolution of the smartphone*. 28. Juli 2014. URL: http://pocketnow.com/2014/07/28/the-evolution-of-the-smartphone (besucht am 07. 06. 2015).

[83] *Microsoft Corp.* URL: https://www.microsoft.com (besucht am 07. 06. 2015).

[86] Smartwach News. *Top 5 Activity Trackers Of 2014*. 5. März 2013. URL: http://www.smartwatchnews.org/top-5-activity-trackers/ (besucht am 20. 02. 2015).

[94] PCMag. *Fitness Tracker*. URL: http://www.pcmag.com/encyclopedia/term/67469/fitness-tracker (besucht am 07. 06. 2015).

[96] Die Presse. *Generali: App soll Gesundheit der Kunden überwachen*. 22. Nov. 2014. URL: http://diepresse.com/home/wirtschaft/international/4600895/Generali_App-soll-Gesundheit-der-Kunden-uberwachen?xtor=CS1-15 (besucht am 04. 04. 2015).

[99] Lydia Ramsey. *Stick-On Tattoo Measures Blood Sugar Without Needles*. 20. Jan. 2015. URL: http://www.popsci.com/temporary-tattoos-could-monitor-diabetes-less-invasively?src=SOC&dom=gp (besucht am 06. 04. 2015).

[101] Reuters. *Microsoft Corp.* URL: http://in.reuters.com/finance/stocks/overview?symbol=MSFT.O (besucht am 07. 06. 2015).

[102] Reuters. *Samsung Electronics Co. Ltd.* URL: http://in.reuters.com/finance/stocks/companyProfile?symbol=005930.KS (besucht am 07. 06. 2015).

[108] *Runtastic*. URL: https://play.google.com/store/apps/details?id=com.runtastic.android (besucht am 23. 02. 2015).

[109] *Samsung Electronics Co. Ltd.* URL: http://www.samsung.com (besucht am 07. 06. 2015).

[114] Bundeskanzleramt Österreich. *Datenschutz - Allgemeine Informationen*. 1. Jan. 2014. URL: https://www.help.gv.at/Portal.Node/hlpd/public/content/244/Seite.2440300.html (besucht am 14. 12. 2014).

[115] Swide. *Wearable tech and the top 5 smart watches at IFA 2014*. 26. Sep. 2014. URL: http://www.swide.com/art-culture/top-5-smart-watches-2014-including-android-wear-and-moto-360/2014/09/26 (besucht am 20. 02. 2015).

[119] The Economic Times. *Apple rules global tablet market with 22.3% share*. 14. Nov. 2014. URL: http://articles.economictimes.indiatimes.com/2014-11-14/news/56092831_1_tablet-market-market-share-strategy-analytics (besucht am 07. 06. 2015).

[120] The Economic Times. *Google's Android eating Apple's market share*. 31. Jan. 2011. URL: http://articles.economictimes.indiatimes.com/2014-11-14/news/56092831_1_tablet-market-market-share-strategy-analytics (besucht am 07. 06. 2015).

[129] Christina Warren. *Google Play Hits 1 Million Apps*. 24. Juli 2013. URL: http://mashable.com/2013/07/24/google-play-1-million/ (besucht am 07. 06. 2015).

[130] The Next Web. *Facebook changes default privacy setting of new users' posts from Public to Friends*. 22. Mai 2014. URL: http://thenextweb.com/facebook/2014/05/22/facebook-changes-default-privacy-setting-new-users-posts-public-friends/ (besucht am 13. 01. 2015).

[133] Zack Whittaker. *WhatsApp privacy practices under scrutiny*. 28. Jan. 2013. URL: http://news.cnet.com/8301-1009_3-57566245-83/whatsapp-privacy-practices-under-scrutiny/ (besucht am 28. 04. 2013).

[136] Diego Wyllie. *Tresorit – Cloud Storage mit Ende-zu-Ende-Verschlüsselung*. 20. Okt. 2014. URL: http://www.computerwoche.de/a/tresorit-cloud-storage-mit-ende-zu-ende-verschluesselung,3069128 (besucht am 04. 04. 2015).

[137] Rose Yao. *Early Success Stories: Fitness and Open Graph*. 29. Aug. 2012. URL: https://developers.facebook.com/blog/post/2012/08/29/early-success-stories--fitness-and-open-graph/ (besucht am 28. 04. 2013).

Abbildungsverzeichnis

Tabellenverzeichnis

Abkürzungen

BCR Binding Corporate Rules. 32

DSG Datenschutzgesetz. 4–6, 8, 9, 11

DSRL Datenschutzrichtlinie. 1, 10–14, 17, 26, 28, 29, 32

ECG E-Commerce-Gesetz. 4

EMRK Europäische Menschenrechtskonvention. 10

EU Europäische Union. 4, 5, 14, 16, 24–26, 28, 30–32, 91, 93, 150, 151

FTC Federal Trade Commission. 24

GHz Gigahertz. 51

ISP Internet Service Provider. 9

MHz Megahertz. 51

o.A. ohne Autor. 4, 10, 26, 32–34

RIM Research In Motion Limited. 35

TKG Telekommunikationsgesetz. 9

USA United States of America. 4, 18, 20, 22–24, 26, 29, 31, 43, 70, 91, 93, 115, 151