Fakultät für Wirtschaftswissenschaften

Diplomarbeit

Datenschutz im Internet der Dinge im Verbraucherbereich

Abschlussarbeit zur Erlangung des Grades

Diplom (FH)

in Wirtschaftsinformatik

der Hochschule Wismar

eingereicht von:	Viktor Seemann
	geboren am 14. März 1982 in Burnoe
	Studiengang Wirtschaftsinformatik
Matrikelnummer:	123551
Erstgutachterin:	Prof. Dr. Karl Wolfhart Nitsch
Zweitgutachter:	Prof. Dr. Sabine Schumann

Rostock, den 28. Juni 2019

Widmung

Diese Diplomarbeit widme ich meinem Vater, der mich jederzeit bestmöglich unterstützt hat, den Abschluss dieser Arbeit aber nicht mehr erleben konnte.

INHALTSVERZEICHNIS

I. ABBILDUNGSVERZEICHNIS

II. TABELLENVERZEICHNIS

III. ABKÜRZUNGSVERZEICHNIS

AGB	Allgemeine Geschäftsbedingungen
BDSG	Bundesdatenschutzgesetz
BRD	Bundesrepublik Deutschland
BVerfG	Bundesverfassungsgericht
CCS	Connected Car Services
CPU	Central Processing Unit
DSK	Datenschutzbehörden des Bundes und der Länder
EMRK	Europäische Menschenrechtskonvention
ePV	ePrivacy-Verordnung
EU-DSGVO	EU-Datenschutz-Grundverordnung
GG	Grundgesetz
GRCh	Grundrechtecharta
IoT	Internet of Things (Internet der Dinge)
LPWAN	Low Power Wide Area Network
NRW	Nordrhein-Westfalen
PC	Personal Computer
PCI-DSS	Payment Card Industry Data Security Standard
SSL	Secure Sockets Layer
TKG	Telekommunikationsgesetz
TKV	Telekommunikations-Kundenschutzverordnung
TMG	Telemediengesetz
TSL	Transport Layer Security

1 EINLEITUNG UND PROBLEMSTELLUNG

1.1 Motivation und Zielsetzung

Ununterbrochen vernetzte intelligente Geräte im privaten Umfeld der Menschen sollen das Leben der Nutzer erleichtern. Zur Erleichterung ihres Einsatzes, sind viele dieser Geräte in der Lage, selbstständig und ohne Eingreifen des Menschen, direkt miteinander zu kommunizieren und Daten auszutauschen. Die weitgehend autonome Organisation dieser smarten Geräte im Internet der Dinge macht es dem einzelnen Menschen kaum noch möglich, den Überblick darüber zu behalten, welche seiner Daten aufgenommen, verarbeitet oder sogar weitergeleitet werden.

Einige dieser Geräte sammeln Daten der Nutzer und leiten sie zur Verarbeitung an Rechenzentren der Hersteller dieser Geräte oder Serviceanbieter weiter. Dazu zählen digitale Assistenten wie Google Home oder Amazon Echo und tragbare Computersysteme (Wearables) wie Smartwatches oder Fitnessarmbänder. Digitale Assistenzsysteme sind im Jahr 2019 in der Lage menschliche Stimmen zu erkennen, um den Sprachbefehlen der Nutzer Folge leisten zu können. Jedoch werden neben beabsichtigten Befehlen der Nutzer auch andere Unterhaltungen aufgezeichnet. Welcher Anteil davon zur Verarbeitung an die Server der Anbieter weitergeleitet wird, ist den Nutzern in dem Moment unbekannt. Wearables werden direkt am Körper getragen und sammeln mit Hilfe verschiedener Sensoren Daten, die nach Artikel 9 der EU Datenschutz-Grundverordnung (DSGVO) zu den besonderen Kategorien der personenbezogenen Daten zählen. In den meisten Fällen werden diese Informationen mit den Servern der Hersteller der Geräte oder Anbieter der dazugehörigen Apps synchronisiert. Wie diese Daten verwendet oder verwertet werden, darüber werden die Nutzer nur in seltenen Fällen ausreichend informiert. Stichproben durch Datenschutzbehörden aus Bund und Ländern zeigen, dass Anbieter gesetzliche Anforderungen missachten. Nutzer werden nicht oder nur mangelhaft darüber informiert, welche ihrer sensiblen Gesundheitsdaten von wem und zu welchem Zweck gespeichert werden. Gesammelte Daten können oftmals nicht gelöscht werden. Das Portal datensicherheit.de schreibt zum Beispiel: *„Oft würden die durch die Geräte erhobenen Gesundheitsdaten durch externe Dritte verarbeitet. Aufgrund der unklaren Regelungen zur Datenverarbeitung entglitten diese Daten dabei der Kontrolle durch die Nutzer.“* (datensicherheit.de, 2016)

Für die unklaren Regelungen zur Datenverarbeitung sorgen neben der stets fortlaufenden Entwicklung der Technik auch unterschiedliche Datenschutzgesetze. Trotz der im Jahr 2016 in Kraft getretenen EU Datenschutz-Grundverordnung gibt es weiterhin zusätzliche nationale Regelungen und Gesetze zum Datenschutz.

So weiß zum Beispiel der Nutzer in Deutschland bei vielen, insbesondere bei den im Ausland erworbenen, Geräten nicht, inwieweit ihre personenbezogenen Daten nach den deutschen Datenschutzregelungen verarbeitet werden.

Um den Nutzern mehr Handlungssicherheit bieten zu können, wird in dieser Arbeit der Frage nachgegangen, inwieweit die Datenschutzregelungen der Hersteller von den gesetzlichen Bestimmungen abweichen und inwieweit die Geräte, als Teilnehmer im Internet der Dinge, nach diesen Regelungen arbeiten. Da Gefahren für den Datenschutz auch aus dem Nutzerverhalten resultieren können, wird des Weiteren untersucht, wie weit die Datenschutzproblematik den Nutzern bekannt ist, welchen Stellenwert der Datenschutz für sie hat und welchen Anteil sie für den Schutz eigener Daten beitragen können.

1.2 Relevanz des Datenschutzes im Internet der Dinge

Das Internet der Dinge befindet sich im Jahr 2019, wie auch in den Jahren davor, im stetigen Wachstum. Bis zum Jahr 2020 soll es rund 13 Milliarden vernetzte Geräte in diesem Bereich geben. (Statista, 2018) Um die Geräte möglichst klein, günstig und energiesparsam herstellen zu können, werden sie mit leistungsschwacher Rechenhardware ausgestattet. Damit die Datensicherheit auf der technischen Seite gewährleistet werden kann, wird aber Leistung benötigt, um zum Beispiel Verschlüsselungsalgorithmen berechnen zu können. Bis zum Jahr 2018 gab es keine ausreichend wirkungsvolle gesetzliche Vorgaben für die Hersteller, um sichere Hardware herzustellen. So wurde die stetig steigende Anzahl der schlecht abgesicherten Geräte im Internet der Dinge zu einem immer größeren Sicherheitsrisiko. Im Jahr 2016 wurden hunderttausende Geräte im Internet der Dinge gekapert und zu einem Botnetz[1] zusammengeschlossen. Dieses Botnetz wurde für eine Reihe schwerwiegender DDoS-Angriffe[2] genutzt. (heise.de, 2018) Bei Geräten, die personenbezogene Daten verarbeiten, könnte die schwache Absicherung dazu führen, dass sensible Daten der Menschen dem Einflussbereich dieser entzogen werden. Die technische Umsetzung der Geräte ist nicht das einzige Risiko für die Datensicherheit. Auch das Verhalten der Nutzer kann zu schwerwiegenden Datenmissbräuchen führen.

Die Politik hat diesen Umstand erkannt und ihn für so wichtig eingestuft, dass im Artikel 25 der EU Datenschutz-Grundverordnung, die Verantwortlichen[3] für die Technikgestaltung dazu verpflichtet werden, schon bei der Entwicklung der Produkte, geeignete Maßnahmen, die Datensicherheit gewährleisten und Datenschutzrisiken minimieren, zu ergreifen. Um es dem Nutzer zu erleichtern, nicht mehr als die zur Verarbeitung notwenigen personenbezogenen Daten preiszugeben, dürfen per Voreinstellung nur diese verlangt werden.

[1] Botnetz: Eine Sammlung von mit Schadprogrammen infizierten Computern, die ein Angreifer aus der Ferne kontrollieren kann (Fischer D. , 2013)

[2] DDoS-Angriff: Versenden von sehr vielen Anfragen an eine Webressource, um ihre Kapazität zur Verarbeitung von Anfragen zu überlasten und so die Verfügbarkeit der Seite zu stören (kaspersky.de, 2018)

[3] Verantwortlicher: Laut Artikel 4 Absatz 7 DSGVO die natürliche oder juristische Person, Behörde, Einrichtung oder andere Stelle, die allein oder gemeinsam mit anderen über die Zwecke und Mittel der Verarbeitung von personenbezogenen Daten entscheidet. Im Folgenden wird der Verantwortliche im Bezug auf die Nutzung der Geräte oder Dienste im Internet der Dinge auch als Nutzer bezeichnet.

Auch der Mehrheit der Privatpersonen in Europa ist Datenschutz wichtig. Mehr als die Hälfte der Deutschen haben Sorgen um ihre Privatsphäre im Internet der Dinge. Es ist kein ausschließlich deutsches Phänomen. Mit 65 Prozent der besorgten Bürger liegt Deutschland auf dem zweiten Platz, dicht gefolgt von Großbritannien mit 63 Prozent. In Frankreich machen sich diesbezüglich mit 72 Prozent anteilig die meisten Bürger Sorgen. (Günter, 2017) Das zeigt, dass der Datenschutz im Internet der Dinge nicht nur in Deutschland ein wichtiges Thema ist.

1.3 Abgrenzung und Analyse der Aufgabenstellung

Das Internet der Dinge lässt sich grundsätzlich in zwei große Anwendungsbereiche unterteilen. Auf der einen Seite in den privaten Bereich der Menschen und auf der anderen Seite in den gewerblichen, beziehungsweise den industriellen Bereich. Der private Bereich umfasst hauptsächlich vernetzte Gegenstände, die den Alltag des Nutzers erleichtern sollen. Es sind zum Beispiel mobile Kleingeräte, die den Menschen im Alltag begleiten und seine Aktivitäts- und Gesundheitsdaten erfassen. Oder auch vernetzte Fahrzeuge, die die Navigation erleichtern und den Fahrkomfort erhöhen. Zu den ortsfesten Geräten im privaten Bereich des Internets der Dinge der Menschen gehören zum Beispiel Haushaltsgeräte, Unterhaltungselektronik oder auch Geräte zur Haushaltsautomation oder Energiemanagement. Im gewerblichen Bereich sind die Logistik und Warenwirtschaft die klassischen Einsatzbereiche des Internets der Dinge. In diesem Bereich werden zum Beispiel Radiowellen genutzt, um Waren berührungslos zu identifizieren und zu lokalisieren. In der Industrie lässt man Maschinen auf Grundlage des Internets der Dinge autonom miteinander kommunizieren (M2M)[4], um so Produktionsprozesse zu automatisieren und dadurch die Effizienz zu steigern und die Kosten zu senken. Die Produktionsmaschinen steuern dabei Fertigungsprozesse im cyber-physischen System[5]. In Deutschland wird diese Strategie unter der Bezeichnung Industrie 4.0 propagiert und von der Bundesregierung unterstützt. Im Ausland gibt es ähnliche Strategien. Jedoch ist der Begriff Industrie 4.0 außerhalb Deutschlands kaum bekannt. Als Synonym für Industrie 4.0. wird gerne der Begriff Industrial Internet of Things (IIOT) genutzt. Jedoch unterscheiden sich diese im Detail. Bei IIOT beschränkt man sich nicht nur auf den Fertigungsprozess, sondern schließt alle möglichen Faktoren der Wertschöpfung ein. *„Es ist quasi das Internet der Dinge angewandt auf alle denkbaren Wertschöpfungsprozesse.“* (Fischer T. , 2016)

Die Abbildung 1 zeigt, dass bis zum Jahr 2020 prognostiziert wird, dass nach der Anzahl der Geräte der Verbraucherbereich des Internets der Dinge größer bleiben wird als der gewerbliche Bereich. Auf Grund dieser Prognose befasst sich diese Arbeit mit dem größeren, also dem Verbraucherbereich, des Internets der Dinge. Ein weiteres Auswahlkriterium ist die Verfügbarkeit der Geräte für den Verfasser. Für den Verfasser ist es unmöglich alle existierenden Geräte, die im Internet der Dinge agieren, zu erfassen.

[4] M2M: Maschine-zu-Machine-Kommunikation, bei der Anlagen und Maschinen ohne menschlicher Auslöser Daten austauschen (elektronik-kompendium.de, 2018)
[5] Cyber-physisches System (CPS): Verbund mechanischer Komponenten über ein Netzwerk zur Steuerung und Kontrolle von komplexen Systemen und Infrastrukturen (Litzekl, 2017)

Deshalb werden in folgenden Kapiteln Geräte nach weiteren Kriterien ausgewählt und vertretend für ihren Bereich untersucht.

Häufig werden die Begriffe Datenschutz und Datensicherheit im Zusammenhang genannt. Aus Erfahrung des Verfassers kennen viele Leute die Unterschiede zwischen den beiden Begriffen nicht oder benutzen sie sogar als Synonym zueinander. Datenschutz befasst sich mit dem Schutz personenbezogener Daten[6]. Der Kernpunkt des Datenschutzes ist die informationelle Selbstbestimmung. Es ist das Recht des Einzelnen selbst über die Preisgabe und Verwendung seiner personenbezogenen Daten zu bestimmen und ist in der EU-Datenschutz-Verordnung verankert. In dieser Verordnung sind Regeln für den Umgang mit den personenbezogenen Daten festgelegt. Die rechtlichen Bestimmungen müssen auch mit Hilfe der Datensicherheit, also mit den technischen und organisatorischen Maßnahmen umgesetzt werden. In den Artikeln 5 und 32 der EU-Datenschutz-Grundverordnung sind Anhaltspunkte zu diesen Maßnahmen beschrieben. Datensicherheit im Allgemeinen befasst sich aber nicht nur mit personenbezogenen Daten, sondern allgemein mit allen Daten. Die Artikel 5 und 32 der EU-DSGVO bilden also eine Schnittmenge zwischen dem Datenschutz und der Datensicherheit. Diese Arbeit befasst sich mit dem Datenschutz im ausgewählten Bereich des Internets der Dinge und nur mit dem Anteil der Datensicherheit, aus der Schnittmenge mit dem Datenschutz.

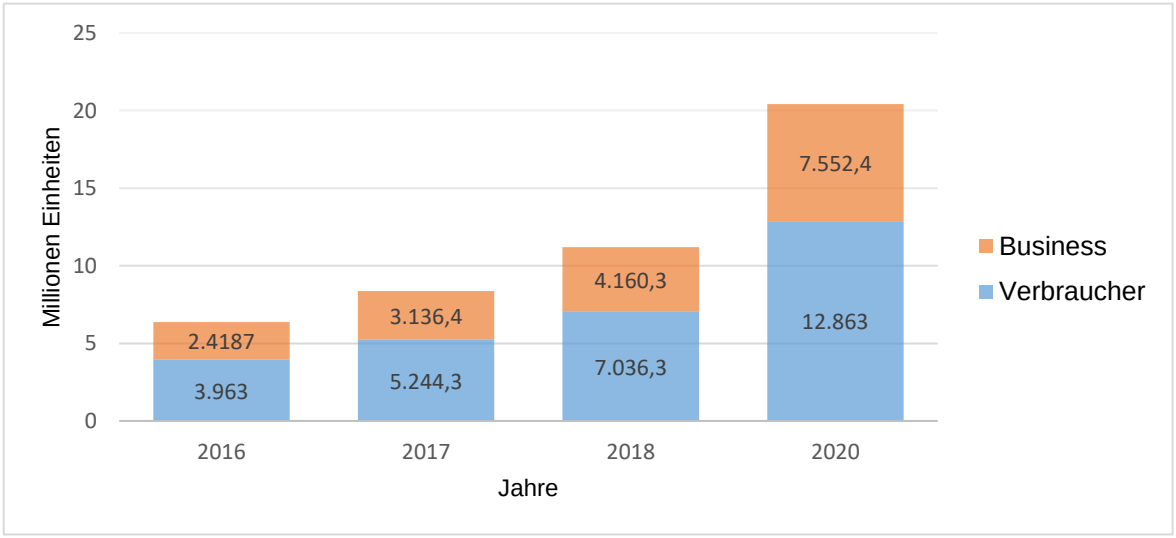


Abbildung 1: Anzahl der weltweit vernetzten Geräte im Internet der Dinge
Quelle: Eigene Darstellung in Anlehnung an Statista, 2018

[6] Personenbezogene Daten: Laut der EU-DSGVO Alle Informationen, die sich auf eine identifizierte oder identifizierbare natürliche Person beziehen.

2 THEORETISCHE GRUNDLAGEN

2.1 Internet der Dinge

2.1.1 Von einer Vision bis zur realen Allgegenwärtigkeit der Rechner

Der Begriff Internet of Things wurde erstmals im Jahr 1999 von Kevin Ashton, dem Mitbegründer und damaligen Leiter des Auto-ID-Centers am Massachusetts Institut of Technology (MIT), in einer Präsentation bei einem Konsumgüterhersteller erwähnt (Müller, 2016, S. 9).

Die grundsätzliche Idee vom Internet der Dinge hat ihren Ursprung noch einige Jahre davor. Im Jahr 1991 beschreibt Mark Weiser in seinem Aufsatz ‚The Computer for the 21st Century' seine Vision vom ubiquitous computing, also von der Allgegenwärtigkeit der Computer. Seiner Vision nach würden die Computer der Zukunft keine stationären Rechner mehr sein. Auch keine mobilen Computer, die man zum Strand, Dschungel oder Flughafen mitnehmen könnte. Denn selbst beim leistungsstärksten Notebook mit einem Zugang zum weltweiten Informationsnetzwerk konzentriert sich die Aufmerksamkeit auf eine einzige Box. Die Computer der Zukunft würden die stationären PCs ersetzen, indem sie den Alltag durchdringen und den Menschen helfen, ohne aufzufallen. Sie würden sich in Lichtschaltern, Thermostaten und Öfen befinden und im allgegenwärtigen Netzwerk miteinander kommunizieren. Sie würden also zu vernetzten intelligenten Gegenständen werden (Weiser, 1991). Damit beschreibt er schon damals Anwendungsgebiete des Smart Homes.

Während die Enzyklopädie der Wirtschaftsinformatik behauptet, dass die Forscher des MIT Media Labs das Konzept des Internets der Dinge prägten (Pipek, 2014), schreiben andere Autoren wie Stefan Müller in seinem Buch Internet of Things, dass es das damalige Auto-ID Center des MIT bzw. die nachfolgende Forschungsgruppe Auto-ID Labs zum Anfang des einundzwanzigsten Jahrhunderts war (Müller, 2016, S. 9). Den eigenen Angaben nach ist die Auto-ID Labs das weltweit führende Forschungsnetzwerk akademischer Laboratorien im Bereich des Internets der Dinge (Auto-ID Labs, 2018). Bereits Mitte der 2000er Jahre war der Begriff Internet der Dinge zu einem viel diskutierten Begriff geworden und im Jahr 2005 erschienen schon die ersten Bücher zu diesem Thema. Auch die Politik fing an, sich dafür zu interessieren. Im Jahr 2007 veranstaltete die EU-Kommission in Lissabon eine Konferenz unter dem Titel „on RFID – The next step to the Internet of Things" (Müller, 2016, S. 10)

Jedoch gibt es im Jahr 2018 immer noch keine einheitliche Definition für das Internet der Dinge. Die Suche nach diesem Begriff mittels der Suchmaschine Google, ergab am 06. November 2018 77.800.000 Ergebnisse. Die Suche nach der englischen Abkürzung IoT ergab 190.000.000 Ergebnisse und bei der Suche nach der vollen englischen Bezeichnung Internet of Things waren es sogar 1.800.000.000 Ergebnisse. Dem Verfasser ist aufgefallen, dass die Anzahl dieser Ergebnisse sehr schwankend ist. Auf zahlreichen Seiten im oberen Bereich der Suchergebnisse, konnte der Verfasser unterschiedliche Definitionen

lesen. Eine für den Verfasser gut formulierte Definition ist auf der Internetseite des Gabler Wirtschaftslexikons zu lesen. Die Autoren Richard Lackes und Markus Siepermann beschreiben in diesem Wirtschaftslexikon das Internet der Dinge folgendermaßen: *„Vernetzung von Gegenständen mit dem Internet, damit diese Gegenstände selbstständig über das Internet kommunizieren und so verschiedene Aufgaben für den Besitzer erledigen können. Der Anwendungsbereich erstreckt sich dabei von einer allg. Informationsversorgung über automatische Bestellungen bis hin zu Warn- und Notfallfunktionen“* (Lackes & Siepermann, 2018). Auch die Politik hat sich an der Definition des Internets der Dinge versucht. Der wissenschaftliche Dienst des Deutschen Bundestages beschreibt es als eine technische Vision, Objekte jeder Art, die mit einer eindeutigen Identität ausgestattet sind, miteinander zu vernetzen (Horvath, 2012). Die Vergabe der weltweit eindeutigen Identität für unvorstellbar große Anzahl der Geräte ist mit Hilfe des Internetprotokolls Version 6 (IPv6) möglich. IPv6 erlaubt eine 39-stellige Anzahl der Adressierungen. Diese vernetzten und mit künstlicher Intelligenz ausgestatteten Geräte werden als Smart Devices bzw. Smart Objects bezeichnet. Mit rund 11 Milliarden im Jahr 2018 und rund 20 Milliarden im Jahr 2020 vernetzter smarter Geräte und stetig steigender Anzahl (Statista, 2018) ist die Vision der Allgegenwärtigkeit der Rechner auf dem Weg in naher Zukunft wahr zu werden.

2.1.2 Technologien

„Das Internet und die Mikroprozessortechnik bilden die technischen Grundlagen des Internets der Dinge. Dank immer günstigerer, kleinerer und leistungsfähigerer Mikroprozessoren lassen sich Gegenstände mit relativ geringem Aufwand mit elektronischer Intelligenz ausstatten“ (Litzel, 2016). Sie werden in der Regel mit mindestens einer Kommunikationsschnittstelle ausgestattet. Die Geräte (Aktoren und Sensoren) können auf folgenden Wegen kommunizieren:

- Auf dem direkten Weg vom Gerät zu Gerät
- Auf dem direkten Weg zwischen dem Endgerät und dem Rechenzentrum bzw. der Cloud des Herstellers oder des Vertragspartners (Backend[7])
- Über ein Gateway[8] mit anderen Geräten oder mit dem Backend

Auf welchem Wege die Kommunikation stattfindet, hängt vom Produkttyp und dem Einsatzgebiet ab. Die Abbildung 3 zeigt eine typische Architektur des Internets der Dinge im privaten Umfeld der Menschen. Geräte wie Smartwatches können zum Beispiel mit Hilfe einer integrierter embedded SIM (eSIM)[9] direkt über das öffentliche Netz mit dem Backend Kommunizieren. Gleichzeitig besitzen diese Geräte auch die Fähigkeit im Nahbereich mit Hilfe der Technologien wie Bluetooth mit verbundenen Geräten wie Smartphones zu kommunizieren.

[7] Backend: Datenverarbeitende Seite des Systems. Zum Beispiel Rechenzentren der Serviceanbieter für Anwendungen im Internet der Dinge
[8] Gateway: Ein Gerät, dass eine Verbindung zwischen zwei unterschiedlichen Netzwerken herstellt
[9] eSIM: In ein Gerät fest eingebautes Teilnehmer-Identitätsmodul, das sich beliebig umprogrammieren lässt

Im Smart-Home-Bereich kommunizieren Geräte in der Regel über ein Gateway miteinander und mit dem Backend. Es gibt aber auch Netzwerktechnologien für das Smart Home, die es den Geräten erlauben direkt miteinander zu kommunizieren.

Für die Kommunikation über kurze Strecken werden zum Teil konventionelle Netzwerktechnologien wie das Ethernet für kabelgebundene (LAN) und das WiFi für die kabellose lokale (WLAN) verwendet. Analog dazu werden für weite Strecken konventionelle zellulare Netze[10] wie UMTS oder LTE verwendet.

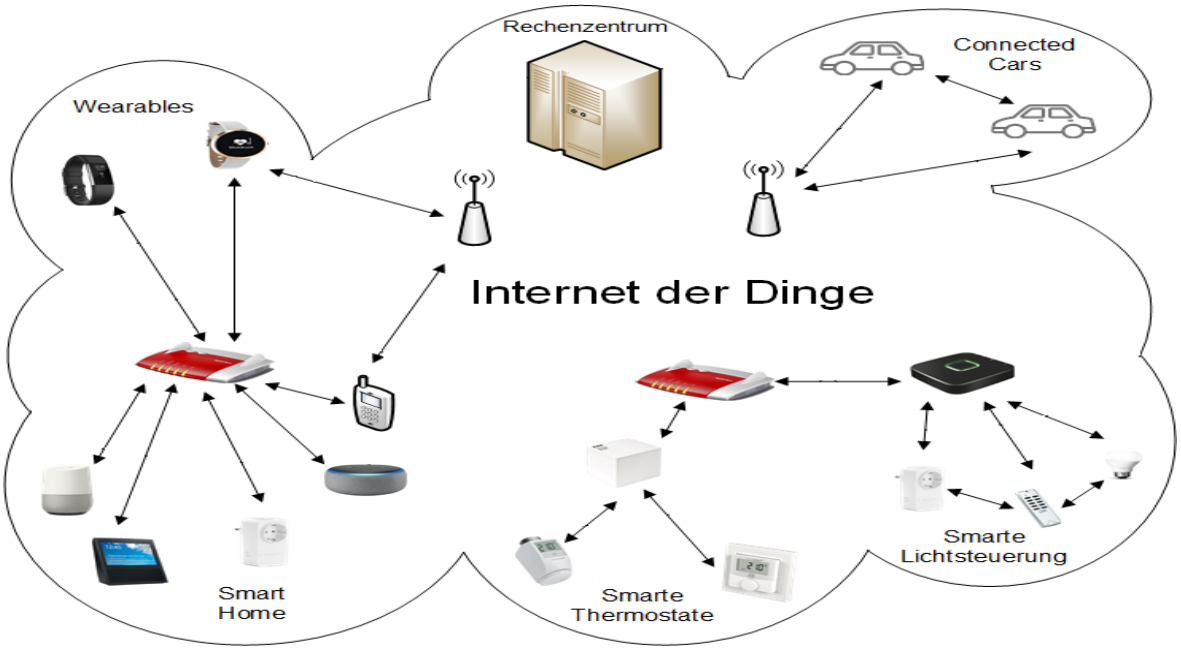


Abbildung 2: Architektur des Internets der Dinge
Quelle: Eigene Darstellung

Diese Technologien wurden für schnelle Übertragung sehr großer Datenmengen entworfen. Im Internet der Dinge übertragen die Geräte aber überwiegend kleine Datenmengen wie ausgelesene Daten der Sensoren, den aktuellen Zustand und Befehle zur Zustandsänderung. Da die miniaturisierten smarten Geräte häufig nicht an das Stromnetz angeschlossen sind, sollte die Übertragung möglichst wenig Energie verbrauchen, damit sie möglichst lange selbstständig, ohne Eingreifen des Menschen funktionieren können. Für diese Art der Kommunikation wären also Übertragungsverfahren, die auf geringe Datenmengen und geringen Energieverbrauch optimiert sind besser geeignet. Zusätzlich ist eine bessere Durchdringung von Gebäudewänden, vor allem im Bereich des Smart Homes, wichtig. So entstehen für das Internet der Dinge andere Anforderungen an die Übertragungstechnologien als beim Internet der Menschen. Um diesen Anforderungen gerecht zu werden, wurden einige konventionelle Übertragungstechnologien angepasst. Ein Beispiel im Bereich der Kurzstreckennetze ist Bluetooth.

[10] Zellulares Netz: Ein Mobilfunknetz, das in eine Vielzahl nebeneinanderliegenden Funkzellen eingeteilt ist (elektrosmoginfo.de, 2008)

Bluetooth besitzt ab der Version 4.0 den Protokollstapel Low Energy. Damit erfüllt er die Anforderungen an den geringen Stromverbrauch. Dieser Standard wird auch Bluetooth Low Energy oder Bluetooth smart genannt. Ab der Version 4.2 besitzt Bluetooth die Fähigkeit mit IPv6 umzugehen. Damit ist auch Bluetooth in der Lage eine sehr große Menge der Geräte im Internet der Dinge zu adressieren.

Im Weitstreckenbereich wurde der zellulare Mobilfunkstandard Long Term Evolution (LTE) von 3GPP[11] weiterentwickelt, um den Anforderungen des Internets der Dinge gerecht zu werden. Bei den neuen Standards, Long Term Evolution Machine Type Communications (LTE-M) und Narrow Band IoT (NB-IoT), wurden der Stromverbrauch gesenkt, die Bandbreite verringert und die Abdeckungsbreite erhöht. Diese Standards gehören zur Klasse des Low Power Wide Area Networks.

Low Power Wide Area Network (LPWAN) wird auch Low Power Network (LPN) genannt. Zu LPWAN zählen Netzwerkkonzepte, die die Anforderungen des Internets der Dinge erfüllen. Dazu zählen in erster Linie geringer Energieverbrauch, geringe Kosten und hohe Netzabdeckung. Das Webportal Elektronik-Kompendium.de schreibt, dass es bei den Low Power Funknetzen darum geht, eine große Anzahl der Teilnehmer in das Netz einzubinden. Dabei sind für die Kommunikation nur einfache Nachrichten vorgesehen. Damit die Funkmodule mit einer herkömmlichen Batterie mehrere Jahre auskommen, ist alles darauf ausgelegt, möglichst wenig Energie zu verbrauchen. Es sind zusätzliche Anforderungen wie geringe Anschaffungs- und Betriebskosten, geringe Anforderungen an die Hardware und sehr hohe Verfügbarkeit aufgelistet. Weil für Low Power Funknetze nur schmale Funkbänder und Frequenzbereiche mit günstigen Ausbreitungseigenschaften, hoher Reichweite und geringer Sendeleistung in Frage kommen, werden überwiegend Frequenzbereiche unter einem Gigahertz genutzt. In Europa werden häufig die lizenzfreien Frequenzbereiche 433 MHz und 868 MHz genutzt. (Elektronik Kompendium, 2018)

Zu den bereits beschriebenen Technologien, die auf Grundlage der konventionellen Übertragungsmethoden entwickelt wurden, stehen im Jahr 2019 weitere speziell für das Internet der Dinge neu entwickelte Übertragungstechnologien zur Verfügung. Es sind zum Teil freie Standards und zum Teil proprietäre[12] Lösungen. Einige Technologien befinden sich noch in der Entwicklung und zu einigen sind kaum oder widersprüchliche Informationen verfügbar. Die meisten sind nicht untereinander kompatibel. Um diesen Umstand zu verbessern, haben sich einige Technologieunternehmen wie Samsung, Intel, Microsoft, Qualcomm und Elektrolux zusammengeschlossen, um einheitliche Standards für das Internet der Dinge zu entwickeln.

Im Kurzstreckenbereich ist RFID eine alte und sehr weit verbreitete Technologie. Sie wird zur berührungslosen Identifikation eingesetzt. Ein häufiger Einsatzbereich ist die Warenidentifizierung. Dazu wird auf den Gegenstand ein Funketikett (Transponder) aufgebracht. Dieser Transponder enthält eine codierte Kennung. Ein Lesegerät kann den Transponder mit Hilfe von Radiowellen mit Strom versorgen und gleichzeitig die Kennung auslesen.

[11] 3GPP: weltweit kooperierende Gremien für die Standardisierung im Mobilfunk.
[12] Proprietär: herstellerspezifisch, nicht offen.

Es gibt auch aktive Transponder mit eigener Stromversorgung, die zum Beispiel bei größeren Entfernungen eingesetzt werden. Diese Technik wird auch häufig in der Logistik eingesetzt. RFID wird auch zur Identifizierung von Tieren, bei Eintrittskarten, Fahrkarten, Bezahlkarten oder Ausweisen eingesetzt. Ein im Jahr 2019 weit verbreiteter, auf RFID basierender Standard ist Near Field Communication (NFC), der zum kontaktlosen Austausch von Daten eingesetzt wird.

Weitere Standards wie ZigBee, Z-Wave und EnOcean konkurrieren vor allem im Smart-Home-Bereich miteinander. Sie sind auf geringen Energieverbrauch und zuverlässige Übertragung spezialisiert und verzichten dafür auf hohe Übertragungsraten. EnOcean geht sogar so weit, dass einige Sensoren und Schalter in der Lage sind aus dem Umfeld Energie zu gewinnen und dadurch batterielos zu arbeiten.

In der Abbildung 3 sieht man die einzelnen Übertragungsstandards und ihre Positionierung nach ihrer Bandbreite und Funkreichweite.

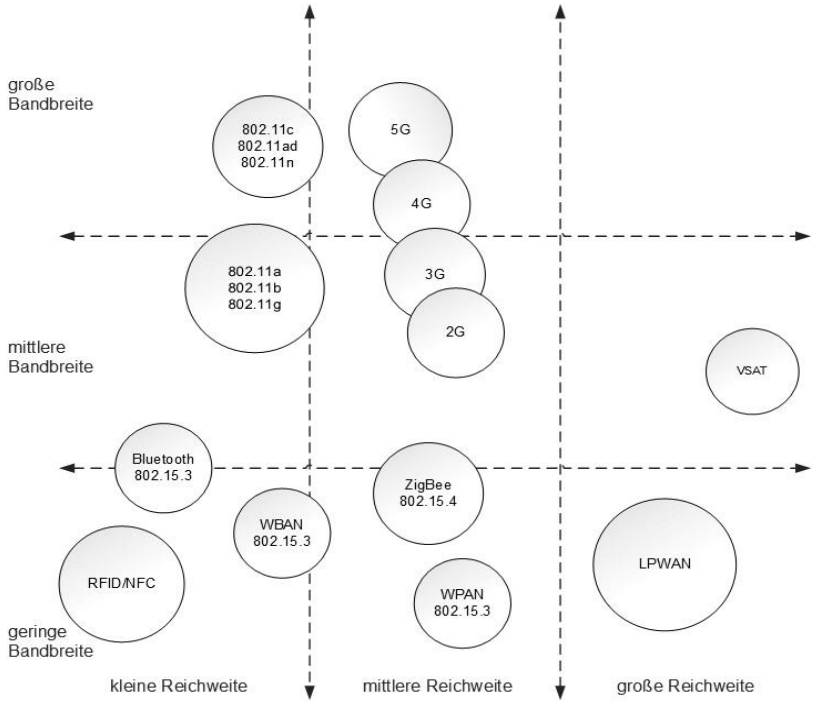


Abbildung 3: Übertragungsstandards nach Bandbreite und Funkreichweite
Quelle: Eigene Darstellung in Anlehnung an waviot.com, 2018

2.1.3 Anwendungsgebiete

Es existieren zahlreiche verschiedene Anwendungsgebiete des Internets der Dinge sowohl im privaten als auch im professionellen Umfeld.

Laut der Beschreibung von Nico Litzel auf BigData Insider, ist das Internet der Dinge auf der professionellen Seite in der Warenwirtschaft, der Autoindustrie und im Gesundheitswesen zu finden. Die Intelligenten Systeme überwachen zum Beispiel Transportwege, sorgen für Just-in-time-Lieferungen, lassen Fahrzeuge direkt mit den

Werkstätten kommunizieren oder überwachen medizinische Abläufe. Es kann auch zu einer Vermischung von privater und professioneller Anwendung kommen. Es können Daten von privat genutzten Geräten wie Wearables Versicherungsgesellschaften zur Verfügung gestellt werden. Diese können daraus persönliche Versicherungsrisiken berechnen. (Litzel, 2016)

Im privaten Bereich sind laut der Statistik des Online-Portals Statista die fünf häufigsten Anwendungsgebiete des Internets der Dinge Wearables, vernetzte Fernsehgeräte (TV-Screens), Netzwerklautsprecher (Network-Audio-Hardware), Smart Home und vernetzte Kraftfahrzeuge (Connected Cars). Die Abbildung 4 zeigt geschätzte anteilige Bestände an Verbraucher-IoT-Geräten in Deutschland. In dieser Arbeit werden diese fünf Bereiche vertretend für den gesamten privaten Bereich des Internets der Dinge behandelt. Nicht aufgelistete Sonderfälle werden nicht berücksichtigt.

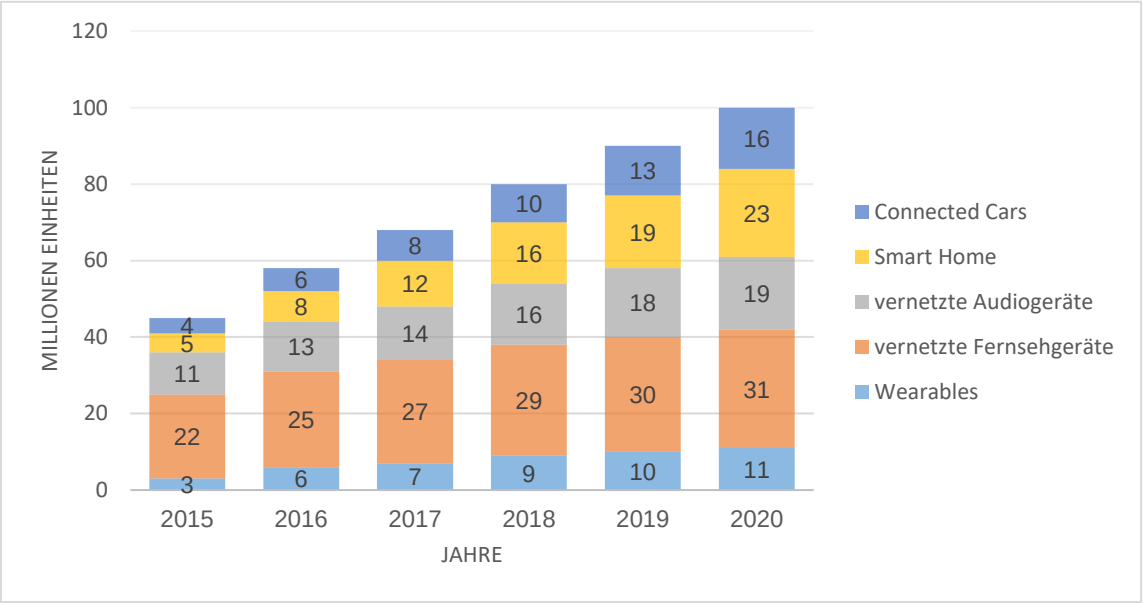


Abbildung 4: Bestand an Verbraucher-IoT-Geräten in Deutschland
Quelle: Eigene Darstellung in Anlehnung an Statista, 2018

Alle diese Anwendungsgebiete haben folgende Gemeinsamkeiten:

- Die Geräte weisen Sensoren auf,
- alle Geräte sind eindeutig identifizierbar,
- sie verarbeiten die erfassten Daten mit Hilfe der integrierten künstlichen Intelligenz,
- sie sind direkt oder indirekt, z.B. über ein Gateway, mit einem Backend verbunden. Dieses Backend kann eine Anwendung in einem Rechenzentrum oder in der Cloud sein. (Infotip Kompendium, 2018)

Es gibt aber auch zahlreiche Unterschiede zwischen den Anwendungsgebieten, die folgend einzeln beschrieben werden.

2.1.3.1 Wearables

Wearables sind mobile Computersysteme, die man direkt am Körper trägt. Im Jahr 2019 sind die Wearable-Geräte so klein, dass sie bei körperlichen Aktivitäten kaum noch störend wirken. Damit kommen sie den Visionen von Ubiquitous Computing und Pervasive Computing schon ziemlich nah. Wearables haben die Aufgabe den Menschen bei verschiedenen Aktivitäten zu unterstützen. Das tun sie indem sie mit Hilfe verschiedener Sensoren Daten erfassen, verarbeiten und dem Nutzer in unterschiedlichen Ausgabeformen präsentieren. Sie messen zum Beispiel physiologische Daten wie den Puls des Nutzers und sein Verhalten durch Schrittzähler oder GPS-Sensoren. Dadurch kann ein umfangreiches Profil des Nutzers erstellt werden. Das kann dem Nutzer helfen, sein Verhalten zu verbessern. An diesen Daten ist aber nicht nur der Nutzer selbst interessiert. Vor allem Krankenkassen zeigen sich sehr interessiert und fördern das Tragen von Fitness-Wearables, wenn sie im Gegenzug Zugriff auf die Gesundheitsdaten des Kunden erhalten. (Littmann, 2015)

Um die erfassten Daten nicht nur lokal verarbeiten und präsentieren zu können, sind Wearables in der Lage auf verschiedenen Wegen mit der Umwelt zu kommunizieren. Häufig werden die Daten mit der Cloud eines Dienstanbieters synchronisiert und dort verarbeitet. Häufig stehen folgende Kommunikationswege zur Verfügung:

- per Bluetooth vom Wearable zum Smartphone des Nutzers, das die Daten per Mobilfunk weiterschickt
- per WLAN vom Wearable zu einem Router, der mit dem Internet verbunden ist und die Daten weiterschickt
- oder bei Wearables mit integrierter eSIM direkt vom Wearable zum Dienstanbieter

Abbildung zeigt eine typische Netzwerkarchitektur der Wearables.

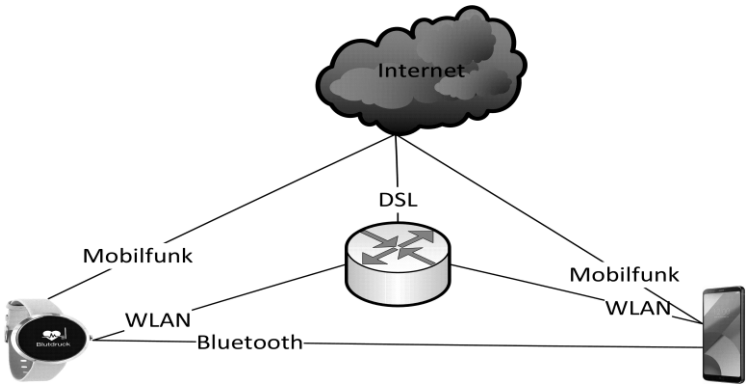


Abbildung 5: Netzwerkarchitektur der Wearables
Quelle: Eigene Darstellung

Wie in der Abbildung 6 zu sehen ist, dominieren Smartwatches und Fitness-Armbänder den Wearable-Markt. Gemeinsam haben sie die Kommunikationsmöglichkeiten per Bluetooth, WiFi oder Mobilfunknetz. Beide können Funktionalitäten des Smartphones erweitern, indem

sie zum Beispiel ankommende Nachrichten anzeigen oder Applikationen auf dem Smartphone steuern. Smartwatches haben in der Regel weniger Sensoren als Fitness-Armbänder. Sie haben dafür aber zusätzliche Funktionen. Als Betriebssystem werden bei den Smartwatches entweder das weit verbreitete Android-System (Wear OS) oder herstellerspezifische Lösungen eingesetzt. Smartwatches können das Aussehen eines klassischen Chronometers annehmen. Die Auswahl der Ziffernblätter ist in der Regel unbegrenzt. Mit Programmierkenntnissen kann auch der Nutzer selbst weitere Ziffernblätter entwickeln.

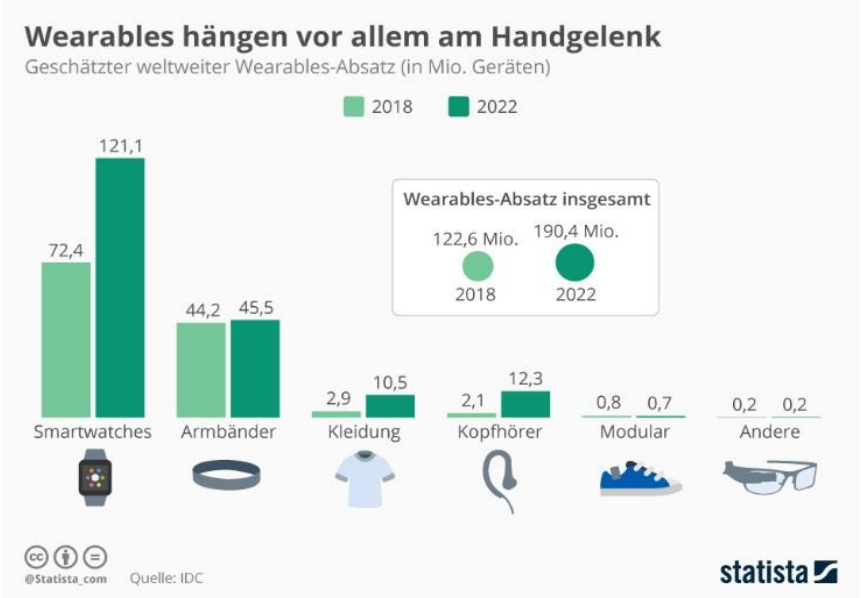


Abbildung 6: Absatz von Wearable-Arten
Quelle: statista.de

2.1.3.2 Vernetzte Fernsehgeräte

Vernetzte Fernsehgeräte erlauben den Nutzern eigene Mediendateien wie Videos, Musik oder Bilder vom eigenen Medienserver über das heimische Netzwerk abzurufen und es auf dem Fernsehgerät wiederzugeben. Wird das Fernsehgerät an das Internet angeschlossen, ist es möglich direkt mittels des Fernsehgerätes im Internet zu surfen oder Medieninhalte von Online-Videotheken abzurufen. Dies wird mittels der von Online-Streamingdiensten angebotenen Applikationen (Apps) möglich. Die Apps können aus den Vertriebsplattformen für Anwendungssoftware (App-Stores) bezogen werden. Als Betriebssystem setzen die Fernsehhersteller im Jahr 2019 noch unterschiedliche Lösungen ein. Einige Hersteller setzen auf das von Google entwickelte Betriebssystem Android TV. Dazu zählen Sony, Sharp und Philips. Andere Hersteller setzen auf andere Entwicklungen oder auf eigene Betriebssysteme. Der Marktführer im Jahr 2017 Samsung (20,2 Prozent) setzt auf das freie Betriebssystem Tizen, das wie auch Android auf Linux basiert. LG Electronics belegt den zweiten Platz in diesem Markt (12,1 Prozent) und setzt auf das eigene Betriebssystem webOS.

Laut der des Online-Portals Statista, waren bereits im Jahr 2016 über 20 Millionen der Fernsehgeräte in Deutschland vernetzt. Die Abbildung 7 zeigt, dass die Anzahl dabei stetig steigend ist. (Statista, 2018) Das Handelsblatt schreibt, dass im Jahr 2016 über die Hälfte der Fernsehgeräte in den deutschen Haushalten, sich mit dem Internet verbinden lassen. Davon sind 74 Prozent an das Internet angeschlossen. Wobei rund ein Drittel der Nutzer regelmäßig auf die angebotenen Inhalte zugreifen. (Handelsblatt, 2016)

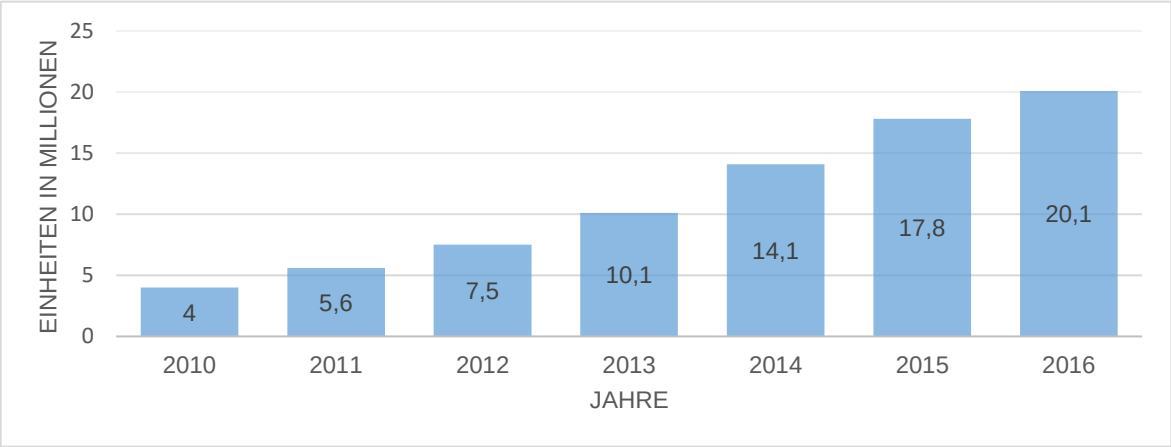


Abbildung 7: Haushalte mit aktiv vernetzten TV-Endgeräten in Deutschland
Quelle: Eigene Darstellung in Anlehnung an Statista, 2018

Da die smarten Fernsehgeräte nicht nur Inhalte aus dem Internet beziehen, sondern auch die Nutzereingaben über das Internet an die Anbieter senden, könnten die Nutzer identifizierbar werden. Die Nutzereingaben können auf folgenden Wegen erfolgen: Auf dem klassischen Weg per Infrarotfernbedienung, über das Heimnetzwerk mittels einer App, per Gestensteuerung oder Sprachsteuerung. Bei der Sprachsteuerung ist zu unterscheiden, ob die Aufnahme mittels eines Schlüsselworts oder eines Knopfdrucks erfolgt. Inwieweit diese Optionen abschaltbar sind, wird in späteren Kapiteln untersucht. Mit dem Internet sind Fernsehgeräte in der Regel über einen Router per LAN oder WLAN verbunden. Abbildung 8 zeigt eine typische Netzwerkarchitektur, an die ein Fernsehgerät angebunden ist.

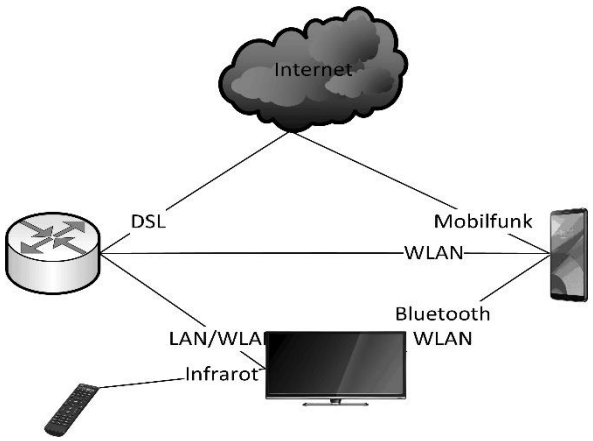


Abbildung 8: Netzwerkarchitektur eines vernetzten Fernsehgerätes
Quelle: Eigene Darstellung

2.1.3.3 Vernetzte Audiogeräte

Vernetzte Audiogeräte ermöglichen es Audioquellen ohne Verkabelung von anderen vernetzten Geräten abzuspielen. Die Übertragung findet dabei per Bluetooth oder WLAN statt. Per Bluetooth können Audioquellen direkt vom eigenen Gerät wie Smartphone zum Lautsprecher übertragen werden. Per WLAN gibt es mehr Möglichkeiten. Die Quelle kann sich auch auf dem eigenen Gerät befinden oder auch von einem Streaming-Anbieter aus dem Internet übertragen werden. Das Smartphone wird dabei nur als Steuergerät eingesetzt. Für die Übertragung per WLAN existieren mehrere untereinander konkurrierende Übertragungsprotokolle. Es gibt offene Lösungen wie Miracast und Digital Living Network Alliance (DLNA) sowie auch proprietäre wie AirPlay von Apple und Chromecast von Google. Die Systeme sind untereinander nicht kompatibel. Sie lassen sich also in der Regel nur mit Geräten desselben Herstellers erweitern. Einige werden direkt in das vorhandene WLAN eingebunden und übertragen Audiosignale auch über dieses Netzwerk. Einige Systeme werden über ein Gateway in das Heimnetzwerk eingebunden. Hersteller wie Samsung und Sonos bauen derartige Lautsprechersysteme. Der Nachteil derartiger Systeme ist, dass man ein zusätzliches Netzwerkgerät betreiben muss. Vorteilhaft ist aber, dass bei der Übertragung das WLAN nicht belastet wird.

Derartige reine Wiedergabegeräte sind bezüglich des Datenschutzes aus der Sicht des Verfassers unbedenklich. Es gibt aber auch Lautsprechersysteme mit eingebauten Mikrofonen, Videokameras und künstlicher Intelligenz. Damit werden Lautsprecher zu digitalen Sprachassistenten. Sie lauschen nach akustischen Aktivierungsbefehlen im Raum und nehmen anschließend Befehle entgegen. Dazu werden Unterhaltungen aufgenommen, zur Auswertung an die Rechenzentren der Anbieter geschickt, von dem sie dann einen Ausführungsbefehl erhalten. Im Jahr 2019 sind solche Systeme in der Lage online einzukaufen, Musik von Online-Streaming-Diensten abzurufen und Smart-Home-Geräte wie Licht oder Heizungsregelung zu steuern. Derartige Geräte werden in späteren Kapiteln ausführlich behandelt. Die Abbildung 9 zeigt eine typische Netzwerkarchitektur der smarten Sprachassistenten.

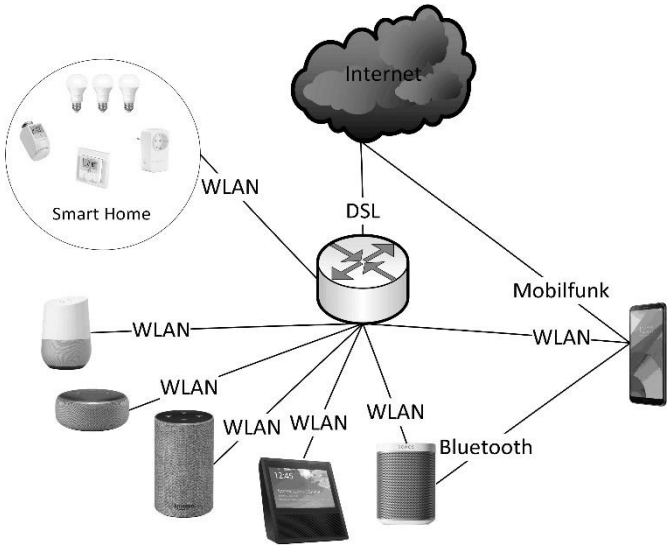


Abbildung 9: Netzwerkarchitektur der Sprachassistenten
Quelle: Eigene Darstellung

2.1.3.4 Vernetztes Auto

Die bekanntere Bezeichnung für das vernetzte Auto ist der englischsprachige Begriff Connected Car. Das belegt zum Beispiel die Suche nach den beiden Begriffen bei der Suchmaschine Google. Die Suche nach der Bezeichnung Connected Car ergab am 24.11.2018 rund 140 Mal so viele Ergebnisse als die Suche nach dem Begriff vernetztes Auto. Intern sind Fahrzeuge schon seit einiger Zeit vernetzt und mit zahlreichen Sensoren ausgestattet. Die durch die Sensoren ermittelten Daten werden im Speicher der Steuergeräte gespeichert und können mittels einer Schnittstelle des Fahrzeugdiagnosesystems ausgelesen werden. Die On-Board-Diagnose-Systeme (OBD) wurden 1988 ursprünglich für die Überwachung der Abgassysteme im Auto eingeführt. Dreißig Jahre später können bei einigen Fahrzeugmodellen nicht nur die Werkstätte, sondern auch die Nutzer selbst zahlreiche, in den Steuergeräten gespeicherten, Informationen auslesen. Mit Adaptern von OBD bzw. OBD2[13] zu Bluetooth oder USB, einem Smartphone und einer passenden Applikation kann der Nutzer auf eine sehr bequeme Weise nicht nur Statusinformationen und gespeicherte Fehlermeldungen selbst auslesen, sondern auch Steuergeräte des Autos umprogrammieren. Die Abbildung 10 zeigt Beispiele für OBD-Adapter, die eine Kommunikation mit dem Fahrzeug ermöglichen. Mittels der in Abbildung 11 gezeigten Applikation für Android-Geräte konnte der Verfasser bei einem BMW E60 LCI Informationen aus 20 Steuergeräten auslesen.

Abbildung 10: OBD2-Adapter
Quelle: Eigene Darstellung

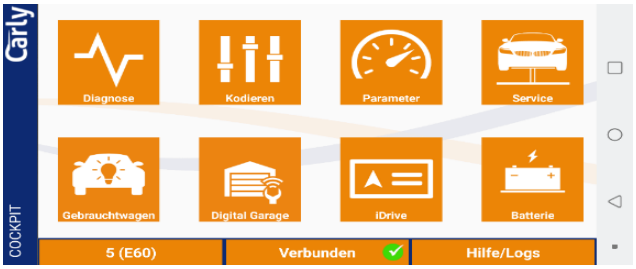


Abbildung 11: Benutzeroberfläche der Carly-App
Quelle: Eigene Darstellung

[13] OBD2: normierte Form des OBD

Für die fahrzeuginterne Kommunikation werden je nach Anwendungsart und Hersteller unterschiedliche Übertragungsmethoden verwendet. Das Webportal KUNBUS listet die Bussysteme CAN, LIN, FLEXRAY und MOST als die wichtigsten Kfz-Bussysteme auf. (KUNBUS GmbH, 2018)

Für die externe Kommunikation werden Mobilfunknetze wie LTE genutzt. In einigen Fahrzeugen, die über kein integriertes Mobilfunksystem verfügen, besteht die Möglichkeit das Kommunikationssystem des Fahrzeugs per WLAN oder Bluetooth mit einem Mobilfunkgerät wie Smartphone zu verbinden und darüber den Zugang zu externen Netzen zu erlangen.

Am 29. April 2015 verabschiedete das europäische Parlament und der Rat der Europäischen Union eine Verordnung, nach der alle neue Automodelle ab dem ersten April 2018 mit einem automatischen Notrufsystem Emergency Call (eCall) ausgestattet sein müssen. (EUR-Lex, 2018) Bei einem Unfall kann das System selbstständig automatisch einen Notruf absetzen. Der Notruf kann auch manuell von einem Insassen abgesetzt werden. Das System benötigt dafür eine Mobilfunkverbindung. Aus Erfahrung des Verfassers, ist Deutschland kein Mobilfunknetz im Jahr 2019 ohne Funklöcher. So kann das System also nicht flächendeckend funktionieren.

Die fünfte Generation des Mobilfunknetzes (5G) könnte diesen Umstand ändern. Im Jahr 2019 ist diese Technologie allerdings noch in der Entwicklungsphase. Das 5G-Netz ist eine der Grundlagen für das Funktionieren eines vernetzten Autos. Laut Christopher Rummel sagen die Forscher im Jahr 2018 voraus, dass das Auto in naher Zukunft 1 TB Daten pro Tag erzeugen wird. Diese Daten erzeugen hunderte IoT-Geräte verschiedener Hersteller, die miteinander kommunizieren. (Rummel, 2018) Mögliche Kommunikationsszenarien der vernetzten Autos sind Kommunikation des Autos mit der Infrastruktur (Car2Infrastructure), Kommunikation des Autos mit anderen Autos (Car2Car) und die Kommunikation des Autos mit verschiedenen Arten von Kommunikationspartnern (Car2X). Bei Car2Infrastructure kommunizieren Autos mit der umgebenen Infrastruktur wie zum Beispiel Ampeln, Parkplätzen, Messstationen für Verkehrsaufkommen und Überwachungskameras. Bei Car2Car kommunizieren Autos eigenständig miteinander, um Informationen wie Geschwindigkeit, Position oder Richtung auszutauschen. Bei Car2X kommunizieren Autos mittels Mobilfunknetzes über das Internet, um zum Beispiel Informationen aus einer Cloud abzurufen oder selbst gesammelte Informationen hochzuladen und damit anderen Verkehrsteilnehmern zur Verfügung zu stellen. (Adam, 2015)

Abbildung 12: Kommunikationsszenarien für vernetzte Autos
Quelle: Adam, 2015, modifiziert durch den Verfasser

2.1.3.5 Intelligentes Zuhause

Für das intelligente Zuhause gibt es auch keine allgemeingültige Definition. Geläufiger als die deutsche Bezeichnung Intelligentes Zuhause ist auch im deutschsprachigen Raum der englische Begriff Smart Home. So ergab eine Suche am 23. November 2018 mittels der Suchmaschine Google bei der Eingabe der Bezeichnung intelligentes Zuhause 7.660.000 Ergebnisse. Die Suche nach der Bezeichnung Smart Home ergab 2.900.000.000 Treffer. Einige Hersteller benutzen dafür auch andere, an das eigene Marketing angepasste, Bezeichnungen. Auf der Webseite des Dudenverlags duden.de ist die folgende Definition des Begriffes Smart Home zu finden: „Wohnumgebung, in der Beleuchtung, Heizung, Haushaltgeräte u. Ä. elektronisch, insbesondere mittels Smartphone, steuerbar sind“. (Duden, 2018) Dort findet man auch den Hinweis, dass es mehrere Schreibweisen für diesen Begriff gibt.

Die fehlende allgemeingültige Definition trägt dazu bei, dass es schwierig ist Smart Home von anderen Bereichen klar abzugrenzen. Die Grenzen zu einigen benachbarten Bereichen sind weich. So zum Beispiel zur Gebäudeautomation, die nach Recherchen des Verfassers teils als Synonym und teils als Vorgänger des Smart Homes beschrieben ist. Im Jahr 2017 wurden Smart-Home-Nutzer befragt, welche Anwendungen sie in diesem Bereich aktiv nutzen. Mit rund 60 Prozent ist Energiemanagement die am meisten genutzte Anwendung im Smart-Home. Dicht danach mit rund 56 Prozent kommt Entertainment. Komfort, Sicherheit und altersgerechte Assistenzsysteme liegen etwas abgeschlagen auf den Plätzen drei bis fünf. Aber auch diese Bereiche innerhalb des Smart Homes lassen sich nicht eindeutig abgrenzen, da die teilnehmenden Geräte mehrere Aufgaben erfüllen können. Die schon beschriebenen vernetzten Fernsehgeräte würde der Verfasser im ersten Moment dem Beriech der Unterhaltungselektronik zuordnen. Sobald das Fernsehgerät aber auch andere Geräte steuern kann, greift es zum Beispiel in den Bereich des Energiemanagements ein. Über einen Rückkanal einer HDMI-Verbindung ist es einem Fernsehgerät möglich angeschlossene Geräte auszuschalten. Die Fernsehgeräte der Marke Philips, die mit Ambilight ausgestattet sind, besitzen eine besondere Eigenschaft. Sie können die Philips Hue Lampen steuern. Diese gehören wiederum einerseits, mit der Fähigkeit Lichtstimmungen zu erzeugen, zur Unterhaltungselektronik und andererseits, durch die Lichtintensitätssteuerung, zum Energiemanagement. Die ebenfalls schon beschriebenen vernetzten Lautsprecher können reine Ausgabegeräte für akustische Signale sein oder gleichzeitig auch Eingaben verarbeiten. Damit gehören sie sowohl zur Unterhaltungselektronik sowie auch zur Kommunikation. Zu den Anwendungsbereichen des Smart Homes gehören ebenfalls auch vernetzte Haushaltsgeräte, Überwachungs- und Alarmsysteme, automatische oder fernsteuerbare Heizungsregelung und Management der Elektroenergie mit intelligenten Steckdosen oder Schaltern.

Zur Kommunikation werden Übertragungstechnologien genutzt, die im Kapitel 2.1.2 beschrieben wurden. Abbildung 14 zeigt, dass unterschiedliche Übertragungsprotokolle eingesetzt werden. Sie sind häufig untereinander nicht kompatibel. Einige Hersteller wie eQ-3 nutzen eigens entwickelte Übertragungsmethoden mit Frequenzen um 433 und 868 MHz. Andere wie Philips oder Bosch setzen das ZigBee-Protokoll ein und sind damit zumindest theoretisch miteinander kompatibel. Eingeschränkte Software-Unterstützung

macht es dem Nutzer trotzdem kaum möglich, die Systeme direkt miteinander kommunizieren zu lassen. Wie man es in der Abbildung auch sieht, sind Gateway als Vermittler notwendig, um unterschiedliche Systeme miteinander arbeiten zu lassen.

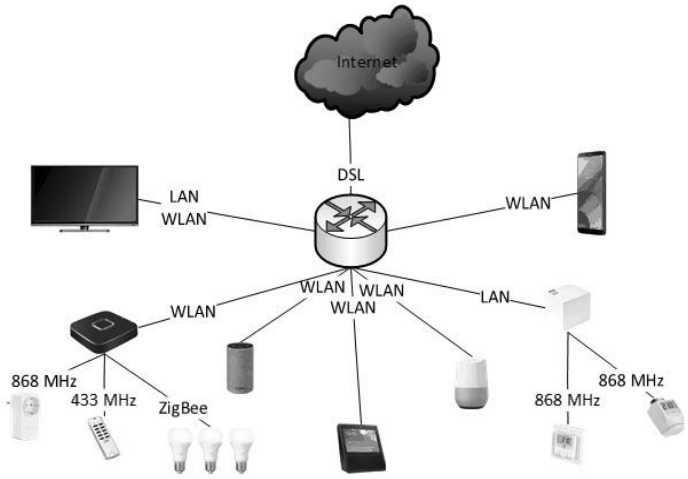


Abbildung 13: Smart-Home-Architektur
Quelle: Eigene Darstellung

2.2 Datenschutz in Deutschland und Europa

Wie für das Internet der Dinge, gibt es auch für den Datenschutz keine weltweit allgemeingültige Definition. Jedoch ist der Datenschutz in einigen Regionen und Ländern der Welt rechtlich geregelt. Die Betrachtungsweisen, Interpretationen und Ausmaße des Datenschutzes unterscheiden sich von Region zu Region. Während der Datenschutz in den Vereinigten Staaten von Amerika kaum rechtlich geregelt ist, genießt er in der Europäischen Union einen hohen Stellenwert. Diesen Stellenwert hat die Europäische Union in der Verordnung (EU) 2016/679 des europäischen Parlaments und des Rates vom 27. April 2016 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten, zum freien Datenverkehr und zur Aufhebung der Richtlinie 95/46/EG verankert. Wie man aus der Bezeichnung der Verordnung ersehen kann, wird der Datenschutz in der Europäischen Union nicht als Schutz der Daten selbst, sondern als Schutz der Menschen, deren personenbezogenen Daten verarbeitet werden, betrachtet. Ähnlich sehen es auch die Länder Schweiz und Liechtenstein. Der Zweck der Datenschutzgesetze beider Länder ist der Schutz der Persönlichkeit und der Grundrechte von Personen, über die Daten verarbeitet werden. Im österreichischen Datenschutzgesetz, welches die EU Datenschutz-Grundverordnung in Österreich ergänzt, wird beschrieben, dass jedermann einen Anspruch auf Geheimhaltung der ihn betreffenden personenbezogenen Daten hat, soweit ein schutzwürdiges Interesse daran besteht. In Deutschland regeln die EU Datenschutzverordnung und eigene Gesetze den Datenschutz. Neben den Datenschutzgesetzen, besteht in Deutschland sogar ein Grundrecht auf den Datenschutz bzw. auf die informationelle Selbstbestimmung. Dieses Recht wird im Grundgesetz nicht explizit erwähnt. Es wurde vom Bundesverfassungsgericht 1983 aus dem allgemeinen Persönlichkeitsrecht und dem Schutz der Menschenwürde abgeleitet.

2.2.1 Vom Eid des Hippokrates bis zum europäischen Datenschutzrecht

Bei der Recherche zur Geschichte des Datenschutzes, stieß der Autor häufig auf die Angabe des hessischen Datenschutzgesetzes oder des Volkszählungsurteils von 1983 als Ursprung des Datenschutzes. Das waren die Anfänge der Art des Datenschutzes, die man im Jahr 2019 kennt. Dem Kenntnisstand des Autors nach, liegt der Ursprung des Datenschutzes aber in der Antike. Der berühmteste Arzt des Altertums Hippokrates von Kos, der ca. 460 bis ca. 370 vor Christi gelebt haben soll, soll folgenden Wortlaut verfasst haben:

> *„Was ich bei der Behandlung sehe oder höre oder auch außerhalb der Behandlung im Leben der Menschen, werde ich, soweit man es nicht ausplaudern darf, verschweigen und solches als ein Geheimnis betrachten."* (Hippokrates, ca. 400 v.Chr.)

Damit schützte er die Daten seiner Patienten, die im Zeitalter der EU Datenschutz-Grundverordnung unter besondere Kategorien personenbezogener Daten fallen würden. Im Mittelalter wurde das Beichtgeheimnis im Kirchenrecht festgeschrieben. Tobias Glenz beschreibt in seinem Artikel auf katholisch.de das Beichtgeheimnis als eine der ältesten Datenschutzvorschriften der Welt. Es gilt bereits seit dem Vierten Laterankonzil 1215 verbindlich für die gesamte katholische Kirche. Dem Kirchenrecht nach ist es dem Beichtvater streng verboten, den Beichtenden auf irgendeine Weise und aus irgendwelchem Grund zu verraten. Eine Verletzung des Beichtgeheimnisses wird mit Exkommunikation[14] bestraft. (Glenz, 2017) In der frühen Neuzeit kam das Postgeheimnis als eine Art des Datenschutzes dazu. Die Motivation des Postgeheimnisses war aber weniger die Daten der Versender zu schützen, sondern eher das Vertrauen in die staatliche Post zu stärken. Als in den sechziger Jahren des zwanzigsten Jahrhunderts die Computertechnologie fortschritt, wurde damit die massenhafte automatisierte Datenverarbeitung durch die staatlichen Behörden ermöglicht. Dieser Umstand führte zur Diskussion über den Schutz der Bürger gegenüber der Datenmacht des Staates. Als Ergebnis entstand in Hessen 1970 das erste Datenschutzgesetz der Welt. 1977 folgte das Bundesdatenschutzgesetz (BDSG). Laut diesem Gesetz durften die Behörden nur dann personenbezogenen Daten der Bürger verarbeiten, wenn diese zur Aufgabenerfüllung der Behörde notwendig waren, wenn ein Gesetz es vorsah oder wenn der Bürger der Verarbeitung seiner Daten freiwillig zugestimmt hatte. Die private gewerbliche Verarbeitung der personenbezogenen Daten war erlaubt, wenn diese Verarbeitung dem berechtigten geschäftlichen Interesse diente und das Interesse des Schutzes der Daten des Betroffenen[15] nicht überwog. Bis 1981 führten auch andere Bundesländer der BRD Landesdatenschutzgesetze ein. Im Jahr 1983 war eine Volkszählung geplant, bei der neben der Kopfzählung auch eine Erhebung weiterer Daten über die Bürger geplant war. Als sich zahlreiche Betroffene dagegen wehrten, befasste sich das Bundesverfassungsgericht (BVerfG) dieser Angelegenheit. Im sogenannten Volkszählungsurteil erklärte das Bundesverfassungsgericht diese Volkszählung für verfassungswidrig. Das Gericht leitete aus dem allgemeinen Persönlichkeitsrecht, das in den ersten beiden Artikeln des Grundgesetzes definiert wird, das Recht auf informationelle Selbstbestimmung, welches

[14] Exkommunikation: Ausschluss aus der Gemeinschaft der Gläubigen aber nicht aus der Kirche.
[15] Betroffener: Person von der personenbezogene Daten Verarbeitet werden.

durch diese Volkszählung verletzt worden wäre. Damit wurde der Datenschutz zu einem Grundrecht in Deutschland. Daraus folgte, dass die Landesdatenschutzgesetze und das Bundesdatenschutzgesetz erneuert werden mussten. Im Jahr 1990 wurde das Bundesdatenschutzgesetz novelliert und in den ersten zwei Jahren nach der Wiedervereinigung Deutschlands verabschiedeten auch die neuen Bundesländer ihre Landesdatenschutzgesetze. Als Versuch den Datenschutz in der Europäischen Union zu harmonisieren, wurde 1995 die Richtlinie 95/46/EG zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten und zum freien Datenverkehr erlassen. In den folgenden Jahren wurde das Bundesdatenschutzgesetz mehrmals novelliert, um Vorgaben der europäischen Richtlinie in Deutschland zu erfüllen und um das Gesetz dem technischen Fortschritt anzupassen. Mit der Aufnahme in die Charta der Grundrechte der Europäischen Union im Jahr 2009 wurde der Datenschutz auch in Europa zu einem Grundrecht. Um die Richtlinie von 1995 an den Fortschritt anzupassen und um die Datenschutzvorschriften verbindlich zu machen, wurde nach jahrelanger Erarbeitungszeit die Datenschutz-Grundverordnung erlassen. Sie gilt seit dem 25. Mai 2018 unmittelbar und einheitlich in jedem Mitgliedsland der Europäischen Union und ersetzt die Richtlinie 95/46/EG.

2.2.2 Zusammenhänge der Gesetze und ihre Relevanz

Im Laufe der Geschichte des Datenschutzes entstanden zahlreiche Datenschutzgesetze. Einige wurden durch Spezialgesetze erweitert, einige wurden in Nachfolgegesetze integriert und einige wurden aktualisiert. Als Anwender ist es nur schwer zu erkennen, welches Gesetz in welchem Anwendungsfall greift. Dieser Abschnitt zeigt eine Übersicht der Datenschutzgesetze mit ihren Beziehungen zueinander und der Relevanz zum Thema dieser Arbeit.

2.2.2.1 Grundgesetz für die Bundesrepublik Deutschland

Das Recht auf die informationelle Selbstbestimmung ist eines der zentralen Begriffe im deutschen Datenschutzrecht. Es besagt, dass jeder selbst über die Preisgabe und Verwendung seiner personenbezogenen Daten bestimmen kann. Es ist ein Grundrecht in der Bundesrepublik Deutschland, obwohl es nicht explizit im Grundgesetz erwähnt wird. Es wurde vom Bundesverfassungsgericht im Jahr 1983 aus dem allgemeinen Persönlichkeitsrecht abgeleitet. Das Persönlichkeitsrecht ergibt sich wiederum aus dem Schutz der freien Entfaltung der Persönlichkeit aus dem Artikel 2 Absatz 1 GG in Verbindung mit dem Schutz der Menschenwürde aus dem Artikel 1 Absatz 1 GG. Somit spielt das Grundgesetz eine wichtige Rolle im deutschen Datenschutzrecht. Der Bundesgerichtshof argumentierte, dass mit dem Recht auf informationelle Selbstbestimmung, eine Gesellschaftsordnung und eine diese ermöglichende Rechtsordnung nicht vereinbar wären, in der die Bürger nicht mehr wissen können, wer was wann und bei welcher Gelegenheit über sie weiß. (BVerfG, 1983) Aber nicht nur die ersten 2 Artikel des Grundgesetzes sind im Datenschutzrecht relevant. Im Artikel 10 GG ist das Brief- Post- und Fernmeldegeheimnis beschrieben. Während die auf den Telekommunikationsendgeräten gespeicherten Daten durch das informationelle

Selbstbestimmungsrecht geschützt werden, schützt das Fernmeldegeheimnis alle Daten während der telekommunikativen Übertragungsphase. (Helfrich, 2018)

2.2.2.2 Europäische Menschenrechtskonvention

Die Europäische Menschenrechtskonvention (EMRK), die im Jahr 1950 in Rom unterzeichnet wurde und am 3. September 1953 in Kraft getreten ist, enthält einen Katalog von Grund- und Menschenrechten. Im Artikel 8 ist festgelegt, dass jede Person das Recht auf Achtung ihres Privat- und Familienlebens, ihrer Wohnung und ihrer Korrespondenz hat. Damit ist die Unverletzlichkeit der Wohnung, sowie die Gewährleistung eines Brief- und Telekommunikationsgeheimnisses gemeint. „Bestandteil des Rechts auf Achtung des Privatlebens ist auch das Recht auf informationelle Selbstbestimmung“ (menschenrechtskonvention.eu, kein Datum)

2.2.2.3 Charta der Grundrechte der Europäischen Union

Beeinflusst von der Menschenrechtskonvention wurde die Charta der Grundrechte der Europäischen Union (GRCh), die im Jahr 2000 proklamiert[16] wurde und im Jahr 2009 ihre Rechtskraft erlangte. So wurde Artikel 1 Absatz 1 EMRK im Artikel 7 der Grundrechtecharta fast eins zu eins wiederholt. Artikel 8 der Grundrechtecharta befasst sich direkt mit dem Schutz der personenbezogenen Daten. Im Absatz 1 heißt es, dass jede Person das Recht auf Schutz dieser Daten hat. Im zweiten Absatz werden Regeln für die Verarbeitung der personenbezogenen Daten sowie das Recht des Betroffenen auf Auskunft über die erhobenen Daten beschrieben. Schließlich wird im dritten Absatz beschrieben, dass die Einhaltung dieser Vorschrift von einer unabhängigen Stelle überwacht wird. Die Charta ist für alle Staaten der Europäischen Union, außer für das Vereinigte Königreich und Polen, bindend.

2.2.2.4 Datenschutzkonvention des Europarates

Rund zwei Jahrzehnte vor der Charta der Grundrechte der Europäischen Union einigte sich der Europarat auf das erste internationale Abkommen für den Schutz der personenbezogenen Daten. Am 28. Januar 1981 wurde die Europäische Datenschutzkonvention verabschiedet. Sie trat am 1. Oktober 1985 in Kraft. Die ausführliche und offizielle Bezeichnung dieses Abkommens lautet: Übereinkommen zum Schutz des Menschen bei der automatischen Verarbeitung personenbezogener Daten. Wie der Name schon verrät schützt dieses Abkommen personenbezogene Daten, die automatisch verarbeitet werden. Daten, die nicht automatisch verarbeitet werden, wie zum Beispiel Papierakten, fallen nicht unter den Schutz dieser Regelung. Die Motivation dieses Abkommens war, ein einheitliches Datenschutzniveau in den Unterzeichnerstaaten herzustellen und einen einfacheren Transfer zwischen diesen Staaten zu ermöglichen. Die Unterzeichnerstaaten wurden verpflichtet die Prinzipien der Konvention in nationales Recht umzusetzen. Die Konvention steht auch Staaten außerhalb Europas offen. Sie enthält

[16] Proklamieren: öffentlich, feierlich, amtlich verkünden

folgende Prinzipien, die sich so oder in abgewandelter Form auch in späteren Datenschutzgesetzen wiederfinden:

- Die Daten müssen nach Treu und Glauben und auf rechtmäßige Weise beschafft und verarbeitet werden.
- Verarbeitung der Daten darf nur zu dem Zweck, zu dem sie erhoben wurden erfolgen und diese Erhebung muss rechtmäßig sein.
- Die Daten müssen sachlich richtig sein und bei Notwendigkeit aktualisiert werden
- Der Betroffene hat jederzeit das Recht auf Auskunft über seine Daten

Die Konvention legt auch besondere Arten von Daten fest und schreibt einen erhöhten Schutz für diese vor.

2.2.2.5 Datenschutzrichtlinie der EG

Mitte der 90er Jahre einigten sich der Europarat und das Europäische Parlament auf die nächste Stufe des gemeinsamen Datenschutzes für europäische Staaten. Es wurde die Richtlinie 95/46/EG des Europäischen Parlaments und des Rates zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten und zum freien Verkehr verabschiedet. Die Mitgliedstaaten wurden verpflichtet die Vorgaben dieser Richtlinie in nationales Recht umzusetzen. Im Gegensatz zu der Datenschutzkonvention betrifft diese Richtlinie auch die nicht automatisierte Verarbeitung personenbezogener Daten, wenn sie in einer Datei[17] gespeichert sind oder gespeichert werden sollen. Die Richtlinie untersagt grundsätzlich die Erhebung und Verarbeitung personenbezogener Daten. Außer wenn folgende Voraussetzungen, die im Artikel 7 ausführlich beschrieben sind, bestehen:

- Die betroffene Person hat zweifelsfrei eingewilligt.
- Die Verarbeitung ist für die Vertragserfüllung notwendig.
- Die Verarbeitung ist notwendig, um rechtliche Verpflichtungen zu erfüllen
- Die Verarbeitung ist für die Wahrung lebenswichtiger Interessen des Betroffenen erforderlich
- Die Verarbeitung ist für das Wahrnehmen öffentlicher Interessen erforderlich

Artikel 8 der Richtlinie befasst sich mit der Verarbeitung besonderer Kategorien personenbezogener Daten. Im Gegensatz zu der Datenschutzkonvention ist in dieser Richtlinie die Verarbeitung dieser Art von Daten, wie auch die Verarbeitung anderer personenbezogenen Daten, grundsätzlich verboten. Auch für diese Daten sind Ausnahmefälle definiert, welche die Verarbeitung erlauben. Wie es auch schon bei der Datenschutzkonvention der Fall war, hat auch laut dieser Richtlinie der Betroffene ein Recht auf Auskunft über die Verarbeitung seiner Daten. Dazu können betroffene Personen einen

[17] Datei mit personenbezogenen Daten: Laut Richtlinie 95/46/EG jede strukturierte Sammlung personenbezogener Daten, die nach bestimmten Kriterien zugänglich sind, gleichgültig ob diese Sammlung zentral, dezentralisiert oder nach funktionalen oder geographischen Gesichtspunkten aufgeteilt geführt wird

Widerspruch gegen die Verarbeitung der Daten einlegen. Im Artikel 3 Absatz 2 ist festgelegt, dass diese Richtlinie keine Anwendung in folgenden Bereichen findet:

- Öffentliche Sicherheit
- Landesverteidigung
- Sicherheit des Staates
- strafrechtlicher Bereich
- Ausübung ausschließlich persönlicher oder familiärer Tätigkeiten einer natürlichen Person

2.2.2.6 Datenschutzrichtlinie für elektronische Kommunikation

Im Bereich der Telekommunikation wurde die Richtlinie 95/46/EG im Jahr 1997 durch die Richtlinie 97/66/EG des Europäischen Parlaments und des Rates ergänzt. Zusätzlich regelt sie laut Artikel 1 Absatz 2 den Schutz der berechtigten Interessen von Teilnehmern, bei denen es sich um juristische Personen handelt. Diese Richtlinie betrifft folgende Dienste:

- Öffentlich zugängliche Telekommunikationsdienste in öffentlichen Telekommunikationsnetzen,
- öffentliche digitale Mobilfunknetze,
- Teilnehmeranschlüsse, die an digitale Vermittlungsstellen angeschlossen sind und
- Teilnehmeranschlüsse, die an analoge Vermittlungsstellen angeschlossen sind, wenn es technisch machbar und verhältnismäßig ist.

Diese Richtlinie wurde im Jahr 2002 durch die Richtlinie 2002/58/EG des Europäischen Parlaments und des Rates über die Verarbeitung personenbezogener Daten und den Schutz der Privatsphäre in der elektronischen Kommunikation (Datenschutzrichtlinie für elektronische Kommunikation) ersetzt. Die Richtlinie 2002/58/EG ist auch noch nach dem Inkrafttreten der Datenschutzverordnung gültig und soll nach dem Stand vom Februar 2019 frühstens im Jahr 2020 durch die ePrivacy-Verordnung (ePV) ersetzt werden. (bvdw.org, 2019) Im Jahr 2009 wurde diese Richtlinie durch die Richtlinie 2009/136/EG ergänzt, die eine ausdrückliche Einwilligung der Nutzer von Webseiten verlangt, Cookies setzen zu dürfen. Die betroffenen Dienste in der Richtlinie 2002/58/EG heißen nun nicht mehr Telekommunikationsdienste, sondern elektronische Kommunikationsdienste. Die Richtlinie enthält mitunter Angaben zu der Betriebssicherheit dieser Dienste, der Vertraulichkeit der Kommunikation, der Anzeige von Rufnummern, der Anrufweiterleitung, zu den Einzelgebührennachweisen, Verkehrsdaten, Standortdaten, Teilnehmerverzeichnissen und unerbetenen Nachrichten. Wobei der Artikel 5, der die Vertraulichkeit der Kommunikation regelt, dem Autor am wichtigsten für das Thema dieser Arbeit erscheint. In diesem Artikel wird das Mithören, Abhören und Speichern sowie andere Arten des Abfangens oder Überwachens von Nachrichten und der damit verbundenen Verkehrsdaten durch andere Personen als die Nutzer untersagt, wenn diese nicht durch andere Regelungen dazu berechtigt ist. Da es keine Verordnung, sondern eine Richtlinie ist, liegt es an den betroffenen Staaten, diese Regelungen in nationale Gesetze umzusetzen.

2.2.2.7 ePrivacy-Verordnung

Da die Umsetzungen der Richtlinien in nationale Gesetze relativ unterschiedlich ausfallen, wird seit dem Jahr 2016 an einer Verordnung gearbeitet, die mit dem Inkrafttreten direkt in den Mitgliedstaaten gilt und somit ein höheres Niveau der Harmonisierung zwischen diesen Staaten bietet. Diese schon erwähnte ePrivacy-Verordnung wird gegenüber der Richtlinie 2002/58/EG auch dem technischen Stand der Technik angepasst. Die Verordnung wird folgende datenschutzrelevante Ziele haben:

- Unterbindung des Handels mit den Backdoors[18], indem die Anbieter nicht mehr dazu verpflichtet werden können, den Schutz den Nutzer zu untergraben.
- Verpflichtung der Anbieter die Daten der Nutzer nach dem Stand der Technik zu sichern und vor unbefugtem Zugriff zu schützen.
- Verbot des räumlichen Trackings[19] durch Anwendungen, die nicht aktiv genutzt werden. Erstellung unerwünschter Bewegungsprofile, die zu den personenbezogenen Daten zählen, soll dadurch erschwert werden.
- Weitgehende Einstellungsmöglichkeiten für den Nutzer beim Tracking. Sodass der Nutzer zum Beispiel das Tracking komplett deaktivieren kann.
- Verbot der Datenverarbeitung durch Online-Kommunikationsdienste wie WhatsApp oder Facebook, ohne einer ausdrücklichen Einverständniserklärung des Nutzers.
- Verpflichtung der Anbieter zu datenschutzfreundlichen Voreinstellungen. (datenschutz.org, kein Datum)

Die Abbildung 14 zeigt die wichtigsten Meilensteine bei der Erarbeitung dieser Verordnung. Wie es auf der Grafik zu erkennen ist, rechnet man im Jahr 2019, dass es nicht vor dem Jahr 2022 zur Anwendbarkeit dieser Verordnung kommt.

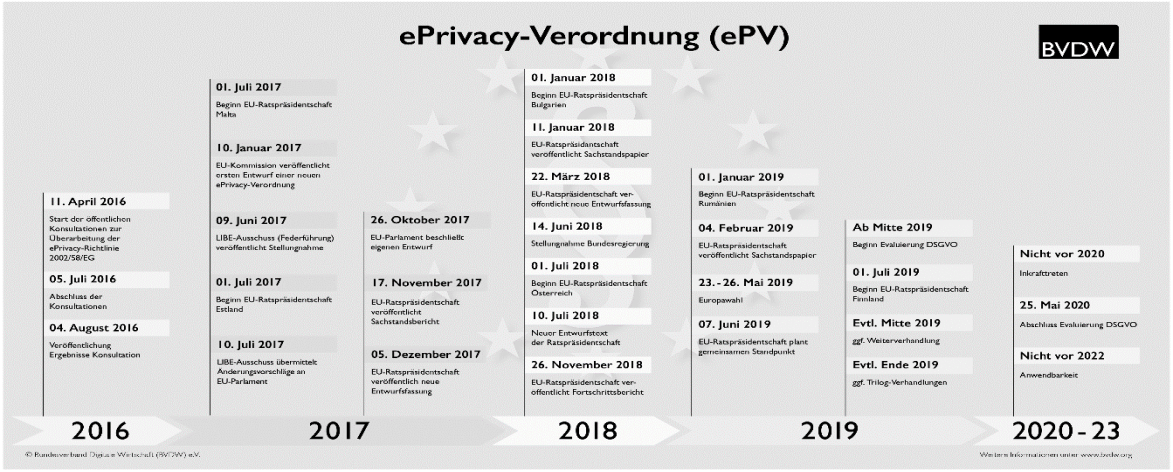


Abbildung 14: ePrivacy-Verordnung - ein Fahrplan zur Einführung
Quelle: bvdw.org, 2018, modifiziert durch den Verfasser

[18] Backdoor: „Eine Backdoor ist ein alternativer Zugang zu einer Software oder zu einem Hardwaresystem, der den normalen Zugriffsschutz umgeht. Mit einer Backdoor lassen sich Sicherheitsmechanismen der Hard- und Software umgehen.“ (Schmitz, 2018)

[19] Tracking: Protokollierung des Nutzerverhaltens. Beim Tracking auf Webseiten, wird zum Beispiel aufgezeichnet worauf der Nutzer klickt. Beim Geo-Tracking werden seine geografische Positionsdaten protokolliert.

2.2.2.8 Telekommunikationsgesetz

Mit dem Telekommunikationsgesetz (TKG) wurde im Jahr 2004 die Datenschutzrichtlinie für elektronische Kommunikation in das nationale Recht in Deutschland umgesetzt. Im Jahr 2007 wurden die Regelungen aus der Telekommunikations-Kundenschutzverordnung (TKV) in das Telekommunikationsgesetzt integriert. Die TKV wurde daraufhin aufgehoben. Die Hauptaufgabe des Telekommunikationsgesetzes ist es den Wettbewerb im Bereich der Telekommunikation zu regulieren. Die Abschnitte 1 und 2 vom Teil 7 dieses Gesetzes befassen sich mit dem Fernmeldegeheimnis und dem Datenschutz. Im Abschnitt 1 wird jeder Fernmeldediensteanbieter zur Geheimhaltung des Inhaltes der Kommunikation verpflichtet. Außerdem wird es den Dienstanbietern sowie auch anderen Funkteilnehmern verboten sich selbst oder andere über das erforderliche Maß hinaus über den Inhalt der Kommunikation in Kenntnis zu setzen. Es wird auch ein Verbot definiert, Telekommunikationsanlagen zu besitzen, herzustellen, zu vertreiben oder einzuführen, welche das heimliche Abhören ermöglichen. Für alle Verbote werden auch Ausnahmen beschrieben, auf die hier nicht weiter eingegangen wird. Geräte im Internet der Dinge kommunizieren teilweise auch über die in diesem Gesetz erfassten Telekommunikationsanschlüsse. Unter den durch das Fernmeldegeheimnis geschützten Daten können also auch personenbezogene Daten sein, die von diesen Geräten versendet werden.

Abschnitt 2 befasst sich mit dem Schutz personenbezogener Daten der Teilnehmer und Nutzer der Telekommunikation. Es werden auch juristische Personen und Personengesellschaften eingeschlossen. Da es sich hierbei um Vertrags-, Verkehrs- und andere Daten handelt, die direkt den Telekommunikationsanschluss betreffen, hat dieser Abschnitt nur indirekt eine Relevanz für den Datenschutz im Internet der Dinge.

2.2.2.9 Telemediengesetz

Während das Telekommunikationsgesetz sich mit den Übertragungsdienstleistungen befasst, befasst sich daneben das Telemediengesetz (TMG) mit allen anderen Informations- und Kommunikationsdiensten, die nicht von dem TKG oder dem Rundfunkstaatsvertrag bzw. den Pressegesetzen abgedeckt werden. Ausgenommen ist auch der Bereich der Besteuerung. Der Begriff Telemedien entstand aus den Begriffen Teledienste und Mediendienste, die ursprünglich in separaten Gesetzen behandelt wurden. Die Abgrenzung zwischen den Telediensten und Mediendiensten war häufig schwierig und umstritten. Um die Handhabung zu vereinfachen, wurden um Jahr 2007 die unterschiedlichen Gesetze, die sich mit den Telediensten und den Mediendiensten befassten, zusammengeführt. Wie man in der Abbildung sieht, entstand aus dem Teledienstegesetz, dem Teledienstedatenschutzgesetz und dem Mediendienste-Staatsvertrag das Telemediengesetz. Die alten Gesetze wurden anschließend außer Kraft gesetzt. Dienste, die Telemedien und gleichzeitig auch Telekommunikationsdienste sind, unterliegen den Regelungen des Telekommunikationsgesetzes sowie auch des Telemediengesetzes. Telemediendienste werden von den meisten Geräten im Internet der Dinge genutzt. Bei den vernetzten Fernsehgeräten sind es zum Beispiel Video-on-

Demand[20]-Angebote wie Amazon Prime Video oder Netflix. Sie sind mit rund 39 Prozent und rund 34 Prozent der Marktanteile die beiden Marktführer in Deutschland. (Loesche, 2017) Bei Wearables sind es Wetterdienst- oder Sportanwendungen. Im vernetzen Auto sind es Dienstleistungen der Hersteller oder der Verkehrsdatenanbieter. Bei den vernetzten Audiogeräten oder im intelligenten Zuhause sind es zum Beispiel Sprachassistenten.

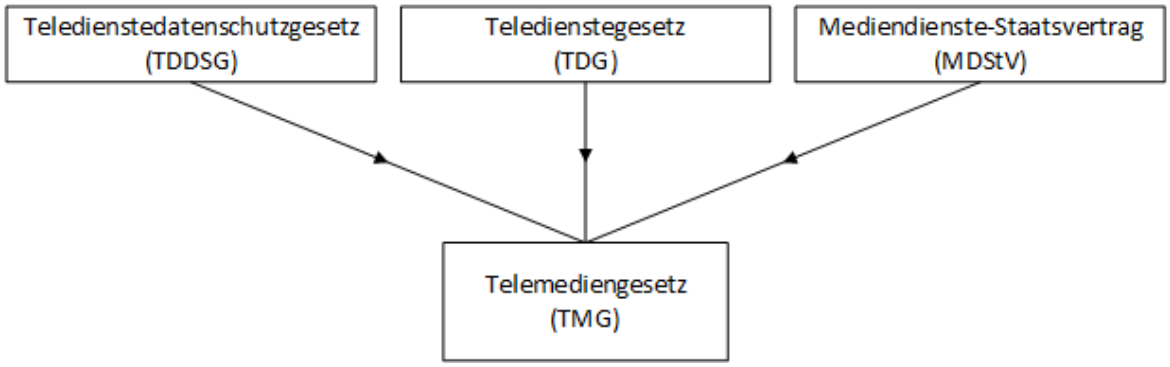


Abbildung 15: Telemediengesetz
Quelle: Eigene Darstellung

Der Datenschutz wird in den §§ 11 bis 15 TMG geregelt. Diese Paragraphen befassen sich mit dem Anbieter-Nutzer-Verhältnis, mit den Grundsätzen, Pflichten des Dienstanbieters, Bestands- und Nutzerdaten. Diese Bereiche werden in einer allgemeineren Form auch in der DSGVO geregelt. Auf der Konferenz der unabhängigen Datenschutzbehörden des Bundes und der Länder im April 2018 wurde geschlussfolgert, dass die Artikel 5, 6 und 25 der DSGVO als Rechtsgrundlage für die Verarbeitung personenbezogener Daten durch Dienstanbieter von Telemedien in Betracht kommen. (Datenschutzbehörden des Bundes und der Länder, 2018) Auf Grund des Anwendungsvorrangs der Datenschutz-Grundverordnung werden diese Bereiche im Folgenden auf der Grundlage der DSGVO behandelt.

2.2.2.10 Datenschutz-Grundverordnung und Bundesdatenschutzgesetz

Die EU-Datenschutz-Grundverordnung, die mit dem vollen Namen Verordnung (EU) 2016/679 des Europäischen Parlaments und des Rates vom 27. April 2016 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten, zum freien Datenverkehr und zur Aufhebung der Richtlinie 95/46/EG heißt, trat im Jahr 2016 in Kraft und gilt seit Mai 2018 unmittelbar in jedem Mitgliedsland der Europäischen Union. Da sie die Datenschutzrichtlinie aus dem Jahr 1995 ersetzt, müssen alle Gesetze, die diese Richtlinie umgesetzt hatten, aktualisiert werden. Das trifft vor allem auf das Bundesdatenschutzgesetz zu. Das Bundesdatenschutzgesetz setzte bis zu dem Zeitpunkt der Verbindlichkeit der Datenschutz-Grundverordnung die Richtlinie 95/46/EG in nationales Recht um. An diesem Zeitpunkt trat die angepasste Form des Bundesdatenschutzgesetzes

[20] Video-on-Demand: Abruf auf Anfrage von Videos per Streaming oder Download von einem Online-Anbieter.

in Kraft. Die Datenschutz-Grundverordnung enthält zahlreiche Öffnungsklauseln, mit denen die einzelnen Staaten die Datenschutzregelungen an ihre nationalen Besonderheiten anpassen können. Allerdings ist es den Staaten nicht erlaubt, die Bestimmungen der Datenschutz-Grundverordnung zu verstärken oder abzuschwächen. Die Bestimmungen dürfen nur spezialisiert werden. Diese Spezialisierung wurde in Deutschland mit der Novellierung des Bundesdatenschutzgesetzes umgesetzt. Das angepasste Bundesdatenschutzgesetz besteht aus 4 Teilen. Im ersten Teil sind gemeinsame Regelungen für die folgenden Bestimmungen festgelegt. Der zweite Teil enthält angepasste Durchführungsbestimmungen zu der Datenschutz-Grundverordnung. Der dritte befasst sich mit den Bestimmungen für die Verarbeitung personenbezogener Daten durch die für die Verhütung, Ermittlung, Aufdeckung, Verfolgung oder Ahndung von Straftaten oder Ordnungswidrigkeiten zuständigen öffentlichen Stellen. Damit setzt das BDSG die Richtlinie (EU) 2016/680 des Europäischen Parlaments und des Rates vom 27. April 2016 um. Diese Richtlinie trat als Ergänzung zu der Datenschutz-Grundverordnung für den Bereich der Polizei und der Justiz in Kraft. Im letzten Teil des BDSG werden Bestimmungen behandelt, die nicht in die Anwendungsbereiche der DS-GVO und der Richtlinie (EU) 2016/680 fallen.

Mit der Datenschutz-Grundverordnung hat sich das Datenschutzrecht im Vergleich zur Richtlinie 95/46/EG beziehungsweise der nationalen Umsetzung durch das Bundes-datenschutzgesetz nicht grundsätzlich verändert. Die Regelungen sind aber teilweise umfangreicher geworden. In manchen Bereichen wurden sie an den technischen Stand im Jahr 2016 angepasst und zum Teil konkretisiert und verschärft. Die Verordnung besteht aus 99 Artikeln, die auf 11 Kapitel aufgeteilt sind. Unverändert sind zum Beispiel folgende für den Datenschutz im Internet der Dinge relevante Bereiche geblieben:

- Geschützt werden Grundrechte und Grundfreiheiten und insbesondere die Privatsphäre natürlicher Personen bei der Verarbeitung personenbezogener Daten. Artikel 1 Absatz 2 DSGVO, Artikel 1 Absatz 1 Richtlinie 95/46/EG.
- Die Regelungen gelten für die ganz oder teilweise automatisierte Verarbeitung personenbezogener Daten sowie für die nichtautomatisierte Verarbeitung personenbezogener Daten, die in einem Dateisystem gespeichert sind oder gespeichert werden sollen. Nur aus dem Begriff Datei der Richtlinie ist in der Verordnung Dateisystem geworden. Artikel 2 Absatz 1 DSGVO, Artikel 3 Absatz 1 Richtlinie 95/46/EG
- Die Bestimmungen werden bei der Verarbeitung durch natürliche Personen zur Ausübung ausschließlich persönlicher oder familiärer Tätigkeiten nicht angewendet. (Artikel 2 Absatz 2 Buchstabe c DSGVO)
- Die Grundsätze der Verarbeitung der personenbezogenen Daten wurden in der DSGVO präzisiert, sind aber im Kern den Grundsätzen aus der Richtlinie gleichgeblieben. (Artikel 5 DSGVO, Artikel 6 Richtlinie 95/46/EG)
- Auch die Voraussetzungen für die Rechtmäßigkeit der Verarbeitung sind im Kern gleichgeblieben. Jedoch wurden Bedingungen für die Einwilligung in der DSGVO erweitert. (Artikel 6 DSGVO, Artikel 7 DSGVO, Artikel 7 Richtlinie 95/46/EG)

- Die Verarbeitung besonderer Kategorien[21] personenbezogener Daten ist grundsätzlich verboten. Für Ausnahmen von diesem Verbot sind strenge Voraussetzungen definiert. (Artikel 9 DSGVO, Artikel 8 Richtlinie 95/46/EG)

Zu den Neuerungen in der Datenschutz-Grundverordnung gehören, neben den erweiterten und präzisierten Grundsätzen für die Datenverarbeitung und erweiterten Rechten der Betroffenen, vor allem auch erweiterte Anforderungen an die Verantwortlichen. Den Datenschutzbestimmungen müssen sich alle Datenverarbeiter unterwerfen, die Leistungen in der Europäischen Union anbieten. Dies gilt unabhängig davon, wo der Dienstleister seinen Sitz hat und wo die Daten verarbeitet werden. Betroffen sind also auch nicht europäische Anbieter, die vernetzte Geräte oder Dienstleistungen in Europa anbieten, welche Daten sammeln und diese auf den Servern in Amerika oder Asien verarbeiten. Vorgaben für die Betreiber finden sich im Kapitel 4 der Datenschutz-Grundverordnung. Im schon erwähnten Artikel 25 DSGVO wird bestimmt, dass der Verantwortliche unter Berücksichtigung der Verhältnismäßigkeit geeignete technische und organisatorische Maßnahmen treffen muss, um Datenschutzgrundsätze umzusetzen. Das hat er nicht erst während der Verarbeitung, sondern schon zum Zeitpunkt der Festlegung der Mittel für die Verarbeitung umzusetzen. Im Absatz 2 wird der Anbieter verpflichtet diese Maßnahmen so umzusetzen, dass durch die Voreinstellung nur personenbezogene Daten verarbeitet werden, deren Verarbeitung für den jeweiligen bestimmten Verarbeitungszweck erforderlich ist. Im Artikel 32 werden technische und organisatorische Maßnahmen zur Gewährleistung der Sicherheit der Datenverarbeitung aufgezählt. Diese schließen neben der

- Pseudonymisierung und Verschlüsselung personenbezogener Daten auch
- Sicherstellung der Vertraulichkeit[22], Integrität[23], Verfügbarkeit[24] und Belastbarkeit[25] datenverarbeitender Systeme und Dienste ein.

Integrität und Vertraulichkeit gehören außerdem zu den Grundsätzen der Datenverarbeitung, die im Artikel 15 behandelt werden. Die oben genannten Maßnahmen sind nicht ausschließlich und können erweitert werden. Eine weitere wichtige Neuerung der Datenschutz-Grundverordnung ist die Anhebung der Bußgelder für Verstöße gegen die Verordnung. So wurden die maximalen Strafen von 300.000 Euro auf 2.000.000 Euro oder auf bis zu 4 Prozent des weltweiten Jahresumsatzes erhöht. Der maximale Bußgeldbetrag wird aus der größeren Zahl von den beiden ermittelt. Damit wurde ein Mittel geschaffen, das auch sehr große datenverarbeitende Unternehmen vor Datenschutzverstößen abschrecken kann. Die Bedingungen für die Verhängung von Geldbußen werden im Artikel

[21] Besondere Kategorien personenbezogener Daten: Nach Artikel 9 Absatz 1 DSGVO personenbezogener Daten, aus denen die rassische und ethnische Herkunft, politische Meinungen, religiöse oder weltanschauliche Überzeugungen oder die Gewerkschaftszugehörigkeit hervorgehen, sowie genetische Daten, biometrische Daten zur eindeutigen Identifizierung einer natürlichen Person, Gesundheitsdaten oder Daten zum Sexualleben oder der sexuellen Orientierung einer natürlichen Person.

[22] Vertraulichkeit: Schutz vor unbefugtem Mitlesen der Nachrichten beziehungsweise vor unbefugtem Einsehen der Informationen.

[23] Integrität: Schutz vor unbefugtem Verändern der Nachrichten beziehungsweise Informationen

[24] Verfügbarkeit: Möglichkeit jederzeit auf die Systeme beziehungsweise Daten zuzugreifen und sie wie vorgesehen zu nutzen.

[25] Belastbarkeit: Fähigkeit, Belastung oder Materialbeanspruchung auszuhalten (Duden, 2018)

83 DSGVO behandelt. Es wurden noch einige weitere Auflagen für die Verarbeiter verschärft, die im Kapitel 4 der DSGVO geregelt sind. Auf diese wird nicht weiter eingegangen, da sie für das Thema dieser Arbeit nur indirekt relevant sind. Die nach Ansicht des Autors wichtige Grundsätze des Datenschutzes sowie auch Rechte der Betroffenen werden in einem separaten Abschnitt behandelt.

2.2.2.11 Grafische Übersicht und weitere Datenschutzgesetze

Der Datenschutz wird in Deutschland noch von einigen weiteren Gesetzen geregelt. Dazu zählen Polizeigesetze, die von der Richtlinie (EU) 2016/680 beeinflusst werden. Die einzelnen Bundesländer haben ihre Landesdatenschutzgesetze. Diese regeln den Datenschutz in Landes- und Kommunalbehörden. Das Strafgesetzbuch enthält datenschutzrelevante Paragraphen, in denen zum Beispiel Verletzung der Vertraulichkeit des Wortes, Verletzung des höchstpersönlichen Lebensbereichs durch Bildaufnahmen oder die Verletzung des Briefgeheimnisses behandelt werden. Auch Kirchen haben datenschutzrechtliche Regeln in ihren Gesetzen. Weitere Gesetze wie das Strafgesetzbuch, die Strafprozessordnung, Beamtengesetze, Arbeitsrechtgesetze und Sozialgesetze werden indirekt vom Datenschutzrecht beeinflusst. Auf die zuletzt genannten Gesetze wird nicht weiter eingegangen, da sie eine zu geringe Relevanz für diese Arbeit besitzen.

In der Abbildung 16 stellt der Autor Datenschutzgesetze dar, die von ihm für diese Arbeit einbezogen wurden. Die Darstellung der Beziehungen zwischen den Gesetzen ist vereinfacht dargestellt, da bei einer detaillierteren Beziehungsdarstellung die Übersichtlichkeit verloren gehen würde.

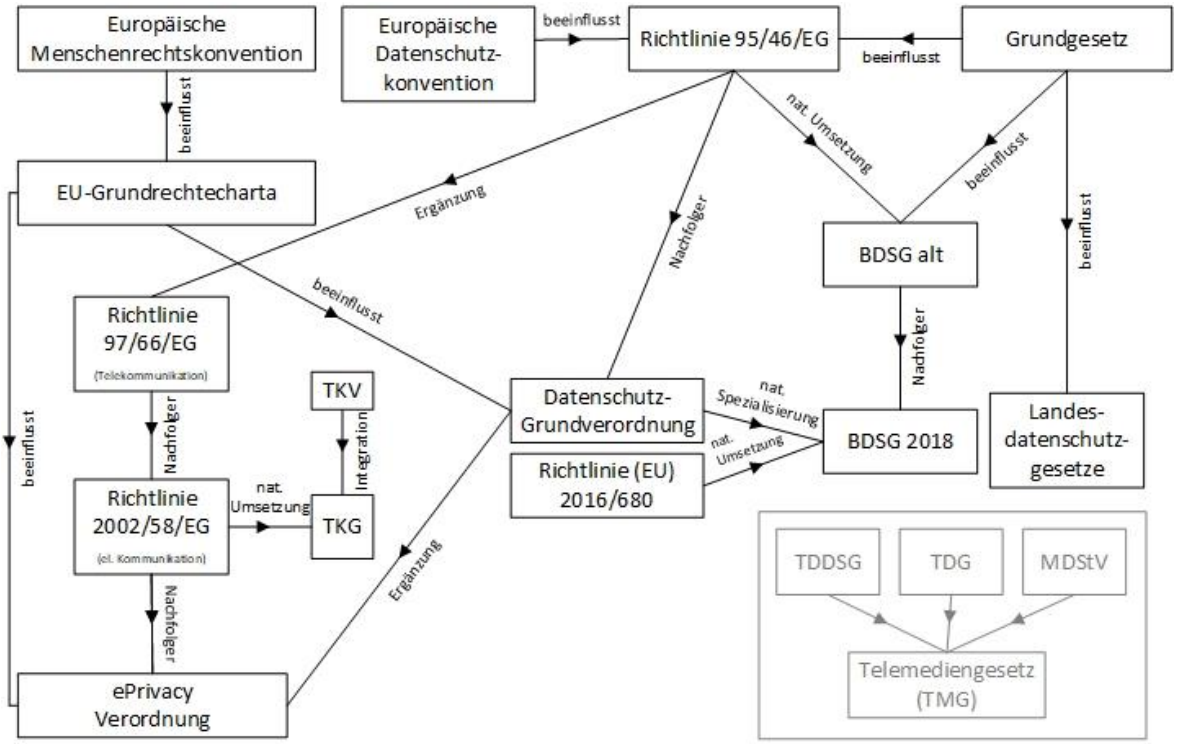


Abbildung 16: Datenschutzgesetze mit ihren gegenseitigen Beziehungen
Quelle: Eigene Darstellung

2.2.3 Datenschutzgrundsätze und Verbraucherrechte

Da die Datenschutz-Grundverordnung zum Teil den Datenschutz der Länder direkt bestimmt und zum anderen Teil nationale Gesetze beeinflusst, spielt sie eine zentrale Rolle im europäischen Datenschutzrecht. Deshalb befasst sich dieser Abschnitt mit den für diese Arbeit relevanten Datenschutzgrundsätzen und den Rechten der Verbraucher, die in der Datenschutzverordnung geregelt sind. Die in der DSGVO geregelten Grundsätze, Rechte der Verbraucher und Pflichten der Verantwortlichen werden im folgendem auch als Datenschutzprinzipien bezeichnet. Grundsätze werden im Kapitel 2 der DSGVO behandelt. Artikel 5 DSGVO besagt, dass personenbezogene Daten auf eine rechtmäßige Weise, nach Treu und Glauben und in einer für die Person nachvollziehbaren Weise verarbeitet werden müssen.

Der Ausdruck Treu und Glauben wird in der Datenschutz-Grundverordnung nicht weiter erläutert. Nach Recherchen des Autors kann man es als aufrichtig, ehrlich, fair oder verhältnismäßig ansehen.

Mit der Rechtmäßigkeit befasst sich Artikel 6 DSGVO. Die Rechtmäßigkeit wird unter Bedingungen gestellt, die in diesem Artikel aufgezählt werden. Aus der Erfahrung des Autors sind folgende zwei Bedingungen im Umgang mit den Geräten des Internets der Dinge im Verbraucherbereich anzutreffen:

- Die Datenverarbeitung ist für die Erfüllung des Vertrages oder für die Durchführung vorvertraglicher Maßnahmen erforderlich oder
- der Nutzer willigt die Verarbeitung seiner Daten ein.

Für die Einwilligung werden wiederum Bedingungen gestellt, mit denen sich der Artikel 7 DSGVO befasst. Die Bedingung bedarf keiner Schriftform. Da der Verantwortliche aber nachweisen muss, dass der Betroffene eingewilligt hat, ist aus der Sicht des Verantwortlichen eine schriftliche Einwilligung vorzuziehen. Wenn die schriftliche Einwilligung für mehrere Verarbeitungszwecke erfolgt, dann müssen diese nach Absatz 2 dieses Artikels klar voneinander zu unterscheiden sein. Die Einwilligung muss freiwillig erteilt worden sein. Um das möglichst sicher zu stellen, darf der Verarbeiter eine Dienstleistung nicht verweigern, wenn der Nutzer die Verarbeitung der Daten abgelehnt hat, die für die Erfüllung dieser Dienstleistung selbst nicht erforderlich sind. Große Dienstleister, auf deren Dienste Nutzer nur schwer verzichten können, weil sie auf ihrem Gebiet quasi alternativlos sind, können mit dieser Vorschrift die Betroffenen nicht mehr zwingen, mehr als nur die benötigten Daten preiszugeben. Die Betroffenen können ihre Einwilligung jederzeit widerrufen. Der Widerruf muss so einfach wie die Erteilung der Einwilligung sein.

Der dritte Grundsatz im Artikel 5 Buchstabe a DSGVO ist die Transparenz. Mit der Transparenz befassen sich Artikel 12 bis 15 der Datenschutz-Grundverordnung. Artikel 13 besagt, dass der Verantwortliche zum Zeitpunkt der Erhebung der personenbezogenen Daten dem Betroffenen Informationen zur Erhebung mitteilen muss. Anschließend sind Inhaltspunkte aufgelistet, die je nach Art der Verarbeitung mindestens in der Mitteilung

enthalten sein müssen. Artikel 14 DSGVO befasst sich mit demselben Vorgehen, wenn die personenbezogenen Daten nicht bei der betroffenen Person erhoben werden. Laut Artikel 15 hat der Betroffene das Recht eine Bestätigung vom Verantwortlichen darüber zu verlangen, ob er personenbezogene Daten von ihm verarbeitet. Im Falle einer Verarbeitung hat er das Recht auf weitere Informationen darüber. Im Artikel 12 ist geregelt, dass der Verantwortliche diese Informationen in präziser, transparenter, verständlicher und leicht zugänglicher Form in einer klaren und einfachen Sprache übermitteln muss.

Artikel 5 Absatz 1 Buchstabe b DSGVO beschreibt die Zweckbindung. Demnach dürfen die personenbezogenen Daten nur für festgelegte, eindeutige und legitime Zwecke erhoben werden. Sie dürfen auch nicht in einer Weise weiterverarbeitet werden, die mit einer dieser Zwecke nicht vereinbar wäre. Eine Erklärung, dass die Daten zum Beispiel allgemein für die Nutzung eines Fitness-Armbandes oder für das Betreiben der Smarthome-Komponenten erforderlich sind, würde also nicht ausreichen.

Die im Artikel 5 Absatz 1 Buchstabe c beschriebene Datenminimierung verstärkt die Zweckbindung. Demnach müssen die Daten dem Zweck angemessen und erheblich sowie auf das für die Zwecke der Verarbeitung notwenige Maß beschränkt sein.

Nach Artikel 5 Absatz 1 Buchstabe d der Datenschutz-Grundverordnung müssen die verarbeiteten personenbezogenen Daten sachlich richtig und erforderlichenfalls auf dem neusten Stand sein. Laut Artikel 15 hat der Nutzer das Recht eine unverzügliche Berichtigung oder Vervollständigung seiner personenbezogenen Daten vom Verantwortlichen zu verlangen.

Das Recht auf Vergessenwerden beziehungsweise Recht auf Löschung wird im Artikel 17 DSGVO behandelt. Demnach hat der Nutzer das Recht eine unverzügliche Löschung seiner Daten vom Verantwortlichen zu Verlangen. Gründe bei denen der Verantwortliche verpflichtet ist die betroffenen Daten zu löschen, werden anschließend in diesem Artikel aufgeführt. Für beide Maßnahmen, für das Berichtigen und das Löschen, muss der Verantwortliche angemessene Maßnahmen treffen. Das Einlegen eines Widerspruchs des Betroffenen gegen die Verarbeitung seiner Daten, ist eines der im Artikel 17 Absatz 1 aufgeführten Gründe. Mit dem Widerspruchsrecht befasst sich Artikel 21 DSGVO umfassend. Dazu gehört die Bestimmung, dass der Betroffene spätestens zum Zeitpunkt der ersten Kommunikation auf das Widerspruchsrecht hingewiesen werden muss.

Der Begriff Speicherbegrenzung, der im Artikel 5 Ansatz 1 Buchstabe e behandelt wird, ist aus der Sicht des Autors etwas irreführend. Speicherdauerbegrenzung wäre hier eindeutiger. Denn dieser Absatz definiert die Dauer der erlaubten Datenspeicherung. Die Daten dürfen nur so lange in einer Form gespeichert werden, die die Identifizierung des Betroffenen ermöglicht, wie es für die Verarbeitungszwecke nötig ist. In Ausnahmen darf die Speicherung diese Zeit überschreiten.

Je kürzer die Produktlebenszyklen der Geräte oder Dienste in Internet der Dinge werden oder je mehr Dienste der Verbraucher nutzt, desto höher ist die Wahrscheinlichkeit, dass er die schon einmal eingegebenen Daten in einem weiteren Gerät oder beim anderen Dienst weiter nutzen will. Eine Hilfestellung bietet dafür der Artikel 20 der Datenschutz-

Grundverordnung. Laut diesem Artikel hat der Nutzer das Recht seine Daten in einem strukturierten, gängigen und maschinenlesbaren Format vom Verantwortlichen zu bekommen und diese einem anderen Verantwortlichen zur Verfügung zu stellen.

Der Verantwortliche ist für die Einhaltung der in diesem Kapitel genannten und aus der Sicht des Autors relevanten sowie auch für andere in der DSGVO behandelten Grundsätze verantwortlich und muss dessen Einhaltung nachweisen können.

2.3 Literaturhinweise

Sowohl im Bereich des Internets der Dinge als auch im Bereich des Datenschutzrechts konnte der Autor fast ausschließlich mit Online-Quellen arbeiten. Vor allem zum Thema Internet der Dinge im Verbraucherbereich gibt es so gut wie keine gute Offline-Literatur.

Folgende Literatur empfiehlt der Autor für das Thema Internet der Dinge:

(Müller, 2016): Das Buch bietet eine Übersicht über einige Bereiche des Internets der Dinge. Die Lektüre beschreibt die Thematik jedoch nicht detailliert und ist daher für einen Einstieg in das Thema Internet der Dinge geeignet.

(Dhanjani, 2015): Das Buch richtet sich eher an erfahrene Software-Entwickler. Es befasst sich mit Soft- und Hardware-Werkzeugen zum Aufdecken der Schwachstellen vor allem im Smarthome-Bereich.

Folgende Links empfiehlt der Autor für die Erweiterung des allgemeinen Verständnisses über das Internet der Dinge und um Details zu einzelnen Spezifikationen zu erfahren:

https://www.itwissen.info

https://www.bigdata-insider.de

https://wirtschaftslexikon.gabler.de

Für das Datenschutzrecht empfiehlt der Autor folgende Bücher:

(Helfrich, 2018): Eine umfangreiche Sammlung der Gesetzestexte zum Thema Datenschutzrecht.

(Bauer, 2018): Dieses Buch befasst sich mit dem Datenschutz bei der Datenverarbeitung im Gesundheitswesen. Es wird auf die Technologien des Internets der Dinge in diesem Bereich eingegangen.

Als Online-Quellen für Informationen über das Datenschutzrecht kann der Autor folgende Links empfehlen:

https://www.datenschutz.org

https://dsgvo-gesetz.de

https://www.bvdw.org

3 STAND DER WISSENSCHAFT

3.1 Ermittlungsgrundlagen und Vorgehensweise

Der Stand der Wissenschaft basiert auf durchgeführten Studien und Erkenntnissen aus der Rechtsprechung, die sich auf den Datenschutz im Internet der Dinge im Verbraucherbereich beziehen. Diese Studien können nicht den kompletten Themenbereich dieser Arbeit abdecken. Sie eignen sich aber gut dafür, einen Überblick darüber zu gewinnen, welche Punkte in diesem Bereich bisher erforscht wurden und wie der Kenntnisstand über diese Punkte in der ersten Hälfte des Jahres 2019 ist. Der Autor hat zwei Voraussetzungen für das Einbeziehen der Studien festgelegt. Zum einen müssen die einzubeziehenden Studien für die Öffentlichkeit frei verfügbar sein. Studien, die nur gegen eine Gebühr eingesehen werden können, werden in dieser Arbeit also nicht berücksichtigt. Zum anderen wird berücksichtigt, dass die technische Entwicklung im Bereich des Internets der Dinge schnell voranschreitet und die Technik nach zwei bis drei Jahren Lebenszeit als veraltet gilt. Häufig bringen Hersteller Nachfolgemodelle der Geräte für diesen Bereich in einem Zyklus von einem Jahr auf den Markt. Auf der rechtlichen Seite wurde der Datenschutz mit der im Jahr 2016 in Kraft getretenen Datenschutz-Grundverordnung auf eine neue Grundlage gestellt. Aus den genannten Gründen werden nur die aus dem Jahr 2016 oder jüngere Studien berücksichtigt. Die ermittelten Studien teilen sich in zwei Studienarten auf. Umfragestudien sind eine Art dieser Studien. Sie befassen sich mit der Meinung der Verbraucher zum Thema Datenschutz und zu den Anwendungsbereichen des Internets der Dinge. Die andere Studienart sind Überprüfungen der Geräte auf die Einhaltung der Datenschutzbestimmungen. Diese umfassen eine Überprüfung der Technikgestaltung inklusive Voreinstellungen und eine Überprüfung der dazugehörenden Datenschutztexte.

In den folgenden Kapiteln werden Inhalte der ausgewählten Studien nach Datenschutzprinzipien zerlegt. Daraus ergeben sich Bestandteile der einzelnen Studien, die nach Datenschutzprinzipien gruppiert werden. Die Studien beinhalten auch nicht relevante Bestandteile, diese werden aussortiert. Relevante Bereiche werden durch Erkenntnisse aus der Rechtsprechung ergänzt. Mit Hilfe dieser Methode wird der Stand der Wissenschaft in den einzelnen Bereichen des Datenschutzes ermittelt. Im anschließenden Unterkapitel werden die Erkenntnisse ausgewertet.

3.2 Einbezogene Studien

Einige Studien befassen sich mit mehreren Datenschutzprinzipien. Die Untersuchungsmethoden dieser Studien werden in diesem Unterkapitel beschrieben. Die nach den Datenschutzprinzipien sortierten Ergebnisse der Studien folgen in den folgenden Unterkapiteln. Untersuchungsmethoden der Studien oder Urteile der Rechtsprechung, die sich nur auf einen Grundsatz beziehen, werden in den folgenden Unterkapiteln direkt im Abschnitt des betroffenen Grundsatzes beschrieben.

Im Oktober 2017 hat The Economist Intelligence Unit[26] im Auftrag von ForgeRock eine Studie namens What the Internet of Things means for consumer privacy durchgeführt, um herauszufinden, was das Internet der Dinge für die Privatsphäre der Verbraucher bedeutet. Für die Studie wurden 1629 Menschen aus acht Ländern im Alter von 16 bis über 65 Jahren befragt. Die Stichproben wurden gleichmäßig auf Frauen und Männer aufgeteilt. (The Economist Intelligence Unit, 2018)

Im Jahr 2016 haben 7 Aufsichtsbehörden eine deutschlandweite Prüfaktion auf Datenschutzmängel durchgeführt. Geprüft wurden Fitness-Armbänder und Smartwatches mit Gesundheitsfunktionen, inklusive der dazugehörigen Apps der Hersteller, die vom Google Play Store sowie auch vom Apple App Store bezogen wurden. Insgesamt waren es 16 Wearables von Herstellern, die zu diesem Zeitpunkt zusammen einen Marktanteil von 70 Prozent in Deutschland abdeckten. Die Überprüfung umfasste rechtliche Fragen und die Technik der Geräte. (ULD, 2016) Leider geben die Aufsichtsbehörden keine genauen Zahlen der Ergebnisse bekannt, sondern nur welche Widersprüche zum Datenschutzrecht gefunden wurden. Das ist für diese Arbeit trotzdem nützlich, da man so Anhaltspunkte dafür bekommt, welche Bereiche genauer zu prüfen sind.

Das Marktwächter-Team von der Verbraucherzentrale NRW hat im Jahr 2016 zwölf Wearables und die dazugehörigen Fitness Apps, jeweils vom Google Play Store und vom Apple App Store, auf Datenschutzmängel untersucht. Die Untersuchung umfasste eine rechtliche sowie auch eine technische Prüfung. Zusätzlich wurden 1055 Verbraucher im Alter ab 14 Jahren telefonisch nach ihren Datenschutzbedenken befragt. (Marktwächter.de, 2017)

Deloitte, ein Dienstleister in der Wirtschaftsbranche, hat im Jahr 2017 eine Umfrage-Studie Namens *Automotive Data Treasure* durchgeführt. Die Studie befasste sich zum Teil mit dem Datenschutz bei Connected Car Services (CCS). Befragt wurden über 1000 Konsumenten ab dem Alter von 18 Jahren in 5 europäischen Ländern bezüglich ihrer Einstellung zum Datenschutz und zu eventuellen Kaufentscheidungskriterien für ein vernetztes Auto. (Deloitte, 2017)

Zwischen September 2017 und Februar 2018 hat ConPolicy, ein Institut für Verbraucherpolitik, eine Studie im Auftrag des Bundesministeriums für Bildung und Forschung durchgeführt. Bei dieser Studie wurden 22 in Deutschland erhältliche Smarthome-Anwendungen untersucht. Unter diesen Anwendungen waren acht Beleuchtungssysteme, zehn Kamerasysteme und vier Sprachassistenten. Geprüft wurden Datenschutztexte, Kontaktmöglichkeiten für Datenschutzfragen und Berechtigungseinstellungen zur Datenerhebung auf die Kompatibilität zur DSGVO. (ConPolicy, 2018)

[26] The Economist Intelligence Unit: Ein britisches Analyseunternehmen für Beratungs- und Prognosedienste.

3.3 Datenschutz aus der Sicht der Verbraucher

Welchen Stellenwert die informationelle Selbstbestimmung beziehungsweise der Datenschutz für die Verbraucher haben, kann man an den Umfragewerten der Studien erkennen. Folgende Umfragewerte zur Bedeutung des Datenschutzes konnte der Autor aus den oben genannten Studien gewinnen:

- Die Umfrage des Beratungsdienstleisters The Economist Intelligence Unit zum Thema Internet der Dinge, ergab, dass 92 Prozent der Befragten selbst kontrollieren wollen, welche ihrer Daten automatisch verarbeitet werden. (The Economist Intelligence Unit, 2018) Die Kontrolle über die eigenen Daten betrifft gleich mehrere Grundsätze des Datenschutzes. Dazu zählen die Rechtmäßigkeit der Verarbeitung personenbezogener Daten, Transparenz und Intervenierbarkeit.
- 74 Prozent dieser Befragten sind davon überzeugt, dass schon kleine Eingriffe in die Privatsphäre eventuell zu einer Einschränkung der Grundrechte führen können. (The Economist Intelligence Unit, 2018)
- Laut der Studie der Verbraucherzentrale NRW, stört es 78 Prozent der Befragten, keine Kontrolle über die persönlichen Informationen zu haben, die sie online preisgeben. (Marktwächter.de, 2017)

Folgende Unterkapitel befassen sich mit den Datenschutzprinzipien, zu denen eine Verbrauchermeinung aus den Studien ermittelt werden konnte.

3.3.1 Rechtmäßigkeit der Verarbeitung

Personenbezogene Daten der Verbraucher dürfen verarbeitet werden, wenn der Verbraucher der Verarbeitung für bestimmte Zwecke einwilligt oder die Verarbeitung erforderlich ist, um den Vertrag zu erfüllen oder vorvertragliche Maßnahmen durchzuführen. Aus der Sicht des Autors sind das die wichtigsten Bestimmungen des Grundsatzes der Rechtmäßigkeit der Verarbeitung personenbezogener Daten im Internet der Dinge im Verbraucherbereich. Folgende Umfragewerte konnten zu diesem Grundsatz ermittelt werden:

- Bei der Umfrage des Beratungsdienstleisters The Economist Intelligence Unit gaben 89 Prozent der Befragten an, dass sie sich bei dem Gedanken, dass Dritte ohne Einwilligung Zugriff zu ihren Daten haben, nicht wohl fühlen. (The Economist Intelligence Unit, 2018)
- Die Umfrage des Dienstleisters Deloitte ergab, dass 63 Prozent der Befragten die Befürchtung haben, dass ihre Daten an Dritte weitergegeben oder verkauft werden und 36 Prozent dieser Befragten, dass sie unerwünschte Werbung bekommen. (Deloitte, 2017)

3.3.2 Transparenz

Transparenz ist ein weiterer wichtiger Grundsatz des Datenschutzrechtes. Dieser Grundsatz besagt, dass der Verbraucher schon bei der Erhebung seiner Daten detailliert darüber informiert werden muss, wie seine Daten verarbeitet werden. Er hat auch während der weiteren Verarbeitung seiner Daten, jederzeit das Recht Informationen über diese Verarbeitung zu bekommen. Folgende Umfragewerte zeigen die Bedeutung der Transparenz für die Verbraucher:

- Laut der Umfrage von The Economist Intelligence Unit wollen 92 Prozent der Befragten informiert werden, wenn Daten über sie automatisch erfasst werden (The Economist Intelligence Unit, 2018) und
- 48 Prozent der Befragten der Deloitte Studie wollen eine klare Kommunikation darüber, welche Daten zu welchem Zweck verwendet werden. (Deloitte, 2017)

3.3.3 Recht auf Vergessenwerden

Das Recht auf Vergessenwerden besagt, dass der Verbraucher von dem Verarbeiter verlangen kann, seine Daten unverzüglich zu löschen.

- 57 Prozent der Befragten der Studie von The Economist Intelligence Unit gaben an, dass das Recht, die Daten endgültig löschen zu lassen, das wichtigste Verbraucherrecht, hinsichtlich der Nutzung privater Daten durch Dritte, darstellt. (The Economist Intelligence Unit, 2018)

3.4 Erkenntnisse aus Überprüfungen und Urteilen

Bei Überprüfungen der Geräte auf das Einhalten der Datenschutzbestimmungen, wurden mehr Datenschutzprinzipien behandelt als bei den Umfrage-Studien. Erkenntnisse, die aus den Überprüfungen gewonnen werden konnten, sind in diesem Kapitel zusammengetragen. Wie im letzten Kapitel sind die Erkenntnisse nach den Datenschutzprinzipien gruppiert. Erkenntnisse über die Einhaltung der Datenschutzbestimmungen können nicht nur aus Studien, sondern auch aus Rechtsfällen und den daraus folgenden Urteilen gewonnen werden. Diese sind in diesem Kapitel ebenfalls berücksichtigt.

3.4.1 Rechtmäßigkeit der Verarbeitung

Der Grundsatz der Rechtmäßigkeit der Verarbeitung personenbezogener Daten wurde durch mehrere Studien in unterschiedlichen Anwendungsbereichen des Internets der Dinge überprüft. Die nachfolgenden Ergebnisse dieser Studien konnten dazu ermittelt werden.

Die meisten Erkenntnisse zu diesem Grundsatz konnten der Studie des Marktwächter-Teams von der Verbraucherzentrale NRW entnommen werden:

- 20 von 24 geprüften Fitness-Apps bauen eine Verbindung in das Internet auf, um Daten auf der Seite des Anbieters zu verarbeiten. Keine von diesen Apps erlaubte eine Verarbeitung direkt auf dem Gerät.
- 15 dieser 20 Apps übermitteln auch Daten zum Nutzungsverhalten an Anbieter. Diese Daten sind für die reine Funktionalität der App vermutlich nicht nötig.
- 19 Apps übermitteln Daten nicht nur an den Anbieter, sondern auch Drittanbieter.
- Durch die Deaktivierung der App-Berechtigungen, kann der Datenfluss zumindest teilweise kontrolliert werden.
- Sechs Anbieter der Apps räumen sich die Möglichkeit ein, Änderungen in den Datenschutzerklärungen jederzeit vornehmen zu können, ohne den Nutzer informieren zu müssen.
- Fünf der Anbieter halten es sich offen, personenbezogene Daten ihrer Nutzer bei Zusammenschlüssen oder Übernahme durch andere Unternehmen weiterzugeben. (Marktwächter.de, 2017)
- Deutsche Aufsichtsbehörden haben herausgefunden, dass einige Hersteller Fitness-Daten der Nutzer für eigene Forschungs- und Marketingzwecke verwenden und an Dritte weitergeben, ohne den Nutzer zu informieren oder seine Einwilligung dafür einzuholen. (ULD, 2016)

3.4.2 Transparenz

Mit dem Grundsatz der Transparenz haben sich nicht nur Studien befasst. Auch ein Landgericht hatte diesbezüglich ein Urteil gesprochen.

Das Bundesministerium für Bildung und Forschung hat Datenschutzerklärungen von Smarthome-Systemen untersuchen lassen. Die Studie ergab folgende Ergebnisse:

- Datenschutzerklärungen waren nur bei 75 Prozent der Beleuchtungssysteme und bei 70 Prozent der Videokameras vorhanden. Sie waren zum Teil nicht in deutscher Sprache aufzufinden.
- Sprachassistenten hatten alle eine Datenschutzerklärung in deutscher Sprache.
- Die Länge der Datenschutzerklärungen betrug rund 4 bis rund 6 Seiten.
- Die Gestaltung der Datenschutzerklärungen bot nur bei den Sprachassistenten mit Drill-Down-Menüs oder Navigationsleisten einen angemessenen Lesekomfort.
- Kontaktdaten für Datenschutzfragen wurden bei 88 Prozent der Beleuchtungssysteme und bei 70 Prozent der Videokameras gefunden. Anbieter von Sprachassistenten hatten alle eine Kontaktmöglichkeit geboten. (ConPolicy, 2018)

Auch die Verbraucherzentrale NRW und deutsche Aufsichtsbehörden haben sich in ihren Studien mit der Transparenz befasst.

- Die Verbraucherzentrale fand heraus, dass drei der untersuchten Anbieter ihre Datenschutzhinweise nur in englischer Sprache bereitstellen und nur zwei über die besondere Sensibilität der Gesundheitsdaten informieren (Marktwächter.de, 2017)
- Aufsichtsbehörden fanden heraus, dass die Datenschutzerklärungen in der Regel lang und schwer verständlich sind. Außerdem enthalten sie zu wichtigen Datenschutzfragen nur pauschale Hinweise und sind teilweise nicht in deutscher Sprache vorhanden (ULD, 2016)

Die genannten Erkenntnisse aus den Studien werden durch die Erkenntnis aus einem Rechtsfall erweitert. Am 10. Juni 2016 verurteilte das Landgericht Frankfurt am Main die deutsche Tochter des südkoreanischen Fernsehgeräteherstellers Samsung, es zu unterlassen, allgemeine Geschäftsbedingungen (AGB) und Datenschutzrichtlinien zu verwenden, die über 50 Seiten lang und unübersichtlich sind. Samsung hatte AGB und Datenschutzrichtlinien verwendet, die jeweils 56 Bildschirmseiten lang waren. Abschnitte dieser Texte konnten nicht einzeln ausgewählt oder durchsucht werden. Sie waren auch nicht unterteilt oder voneinander abgehoben. Einige verwendete Begriffe waren definitionsbedürftig. Begriffsdefinitionen befanden sich erst im hinteren Teil der Texte. (ratgeberrecht.eu, 2016) Damit verstoß Samsung gegen das Transparenzgebot, laut dem derartige Bestimmungen in präziser, transparenter, verständlicher und leicht zugänglicher Form und in einer klaren einfachen Sprache zu übermitteln seien.

3.4.3 Informationspflicht bei der Erhebung der Daten

Zur Informationspflicht bei der Erhebung der personenbezogenen Daten, die auch zum Grundsatz der Transparenz gehört, wurde ein Studienergebnis ermittelt.

- Dem Marktwächter-Team der Verbraucherzentrale NRW ist aufgefallen, dass bei 16 von 19 Apps technische Daten an Drittanbieter senden, bevor der Nutzer über die Erhebung der Daten informiert wird und den Nutzungsbedingungen zustimmt. (Marktwächter.de, 2017)

3.4.4 Verbot der Verarbeitung besonderer Kategorien der Daten

Gesundheitsdaten gehören zu besonderen Kategorien personenbezogener Daten. Die Verarbeitung dieser Daten ist nach Artikel 9 DSGVO verboten. Es sei denn, es liegt ein Ausnahmefall vor, wie zum Beispiel die Einwilligung des Nutzers.

- Laut der Studie des Marktwächter-Teams senden 20 von 24 Apps Gesundheitsdaten an die Anbieter. Eine Einwilligung des Nutzers zur Verarbeitung dieser Daten, holt sich jedoch nur ein Anbieter. (Marktwächter.de, 2017)
- Laut der Studie der Aufsichtsbehörden klärt fast kein Hersteller der Wearables über die besonders schützenswerten Gesundheits- und Standortdaten auf. (ULD, 2016)

3.4.5 Auskunftsrecht

- Laut der Studie der Aufsichtsbehörden wurde das Recht auf Auskunft, welches auch mit dem Transparenzgrundsatz verwandt ist, von Anbietern nicht beachtet. *„Tests, bei den Anbietern Auskunft über die gespeicherten Daten zu erhalten, wurden entweder mit pauschalen Verweisen auf Datenschutzerklärungen beantwortet oder wegen vermeintlicher Nicht-Zuständigkeit abgewiesen.“* (ULD, 2016)

3.4.6 Zweckbindung

Im Jahr 2017 musste VIZIO, ein Hersteller für vernetzte Fernsehgeräte, nach einer Beschwerde der US-amerikanischen Behörde Federal Trade Commission, 2,2 Millionen US-Dollar Bußgeld zahlen. VIZIO hatte den Grundsatz der Zweckbindung verletzt, indem ohne Einwilligung der Nutzer personenbezogene Daten gesammelt, analysiert, mit anderen Daten verknüpft und für Werbezwecke benutzt wurden. Das Unternehmen muss diese Praxis zukünftig unterlassen und die bis zum 1. März 2016 gesammelten Daten löschen sowie seine Datenschutzbestimmungen erneuern. (Federal Trade Commision, 2017)

3.4.7 Recht auf Vergessenwerden

Das Recht auf Vergessenwerden, das laut der Studie von The Economist Intelligence Unit für 57 Prozent der Befragten das wichtigste Verbraucherrecht ist, wird laut der Studie der Aufsichtsbehörden von vielen Anbietern zumindest bei der Entwicklung nicht beachtet. Weder im Nutzerkonto noch am Gerät dieser Anbieter selbst kann man seine Daten selbstständig vollständig löschen. (ULD, 2016)

3.5 Auswertung

Aus den Umfragewerten kann man erkennen, dass der Datenschutz eine große Bedeutung für die deutliche Mehrheit der Menschen in Deutschland hat. Das belegen die Umfragewerte, dass 92 Prozent der Befragten selbst Kontrolle über ihre Daten behalten wollen, 78 Prozent Angst haben diese Kontrolle zu verlieren und 74 Prozent den Datenschutz sogar mit dem Grundrecht verbinden. Ob die einzelnen Grundsätze des Datenschutzrechts den Verbrauchern bewusst sind, kann man aus den Studien nicht eindeutig erkennen. Zu einigen Grundsätzen haben die Verbraucher eine deutliche Meinung, einige werden aber komplett außer Acht gelassen. Der Einschätzung des Autors nach, liegt das an den Umfängen und der Fragestellungen der Studien. Aus den Umfragewerten geht hervor, dass es den Verbrauchern besonders wichtig ist, dass ihre Daten nur mit ihrer Einwilligung verarbeitet werden und dass sie immer gut und ausführlich über diese Verarbeitung informiert werden. Für 57 Prozent der Befragten ist das Recht auf Vergessenwerden sehr wichtig. Das ist zwar eine Mehrheit. Für fast die Hälfte scheint es aber nicht so wichtig zu sein, die Möglichkeit zu haben, ihre Daten endgültig und komplett löschen zu lassen.

Während Umfrage-Studien dabei helfen, das Wissen und die Einstellung der Verbraucher zu analysieren, helfen Überprüfungen der Anwendungssysteme, festzustellen inwieweit sich Hersteller und Diensteanbieter an die Datenschutzbestimmungen halten. Ergebnisse der Überprüfungen der Datenschutzerklärungen zeigen, dass viele davon gesetzliche Anforderungen nicht erfüllen. Vor allem der Grundsatz der Transparenz wird oft nicht umgesetzt. So sind einige Datenschutzerklärungen zu lang, zu unübersichtlich und schwer zu verstehen. Einige sind nicht in der jeweiligen Landessprache verfügbar und bei manchen Geräten sind sie gar nicht aufzufinden. Positiv fällt auf, dass bei allen geprüften Sprachassistenzsystemen Datenschutzerklärungen vorhanden waren und bei diesen keine Verstöße gegen Datenschutzbestimmungen gefunden wurden. Studien zeigen, dass bei den Systemen Daten nicht lokal, sondern auf der Seite des Anbieters verarbeitet werden. Wenn nur Daten verarbeitet werden, die für die Funktion der Anwendung notwendig sind und der Verbraucher ausführlich darüber aufgeklärt wird, spricht es nicht gegen die Datenschutzbestimmungen. Studien zeigen aber auch, dass nicht nur notwendige Daten gesammelt werden und der Verbraucher nicht immer nach seiner Einwilligung gefragt oder sogar gar nicht darüber informiert wird. In diesen Fällen ist die Verarbeitung nicht mehr gesetzeskonform. Die Rechtsfälle, die sich mit der Einhaltung der Datenschutzbestimmungen bei vernetzten Fernsehgeräten befassten, zeigen, dass der Datenschutz bei der Technikgestaltung noch nicht in jedem Fall beachtet wird. In den Studien wurde auch versucht, Anbieter zu kontaktieren, um Rechte der Verbraucher, wie Auskunftsrecht oder das Recht auf das Löschen der Daten, wahrzunehmen. Dass in einigen Fällen entweder keine Kontaktmöglichkeit gefunden wurde oder die Anfrage ignoriert wurde, zeigt dass in diesem Bereich auch noch Datenschutzdefizite bestehen.

Durch vorliegende Studien wurden nicht alle Bereiche des Datenschutzrechts erfasst. Die Forschung des Autors im nächsten Kapitel hat die Aufgabe den bisher untersuchten Bereich zu erweitern und zu prüfen inwieweit sich Unterschiede zu den Erkenntnissen aus den vorliegenden Studien ergeben.

4 DATENSCHUTZANALYSE BEI ANWENDUNGSSYSTEMEN

Nachdem im letzten Kapitel der Stand der Wissenschaft mit Hilfe der Ergebnisse der bereits erfolgten Studien und Rechtsfälle analysiert wurde, wird in diesem Kapitel die Einhaltung der Datenschutzprinzipien im Internet der Dinge mittels einer Untersuchung der im Frühjahr 2019 aktuellen Anwendungssysteme analysiert. Dazu werden zunächst die zu analysierenden Schwerpunkte des Datenschutzes ermittelt. Diese ergeben sich aus den bereits ermittelten Datenschutzprinzipien und den für die Verbraucher wichtigsten Datenschutzkriterien. Um die Einstellung der Verbraucher zum Datenschutz und die wichtigsten Datenschutzkriterien für sie in diesem Bereich zu ermitteln, wird eine Umfragestudie durchgeführt. Diese Studie wird im nächsten Unterkapitel näher beschrieben. Auf Grund der großen und unübersichtlichen Anzahl der intelligenten Geräte in unterschiedlichen Anwendungsbereichen des Internets der Dinge, kann nicht jedes einzelne existierende Gerät beziehungsweise System im Rahmen dieser Arbeit überprüft werden. Deshalb werden zuerst Schwerpunktanwendungsgebiete und anschließend Schwerpunktsysteme innerhalb dieser Anwendungsgebiete ermittelt. Auf Grund der dominierenden Stellung dieser Systeme können sie stellvertretend für den kompletten jeweiligen Bereich untersucht werden. Mit der Ermittlung der Schwerpunkte und der Untersuchung der Systeme auf die Einhaltung der Schwerpunktdatenschutzprinzipien befassen sich nachfolgende Unterkapiteln.

4.1 Umfragestudie

Die Umfragestudie wurde im Zeitraum vom 2. Mai 2019 bis zum 5. Mai 2019 durchgeführt. Es wurden gezielte Fragen gestellt, die dabei helfen Schwerpunkte bei den Anwendungsgebieten, bei den Anwendungssystemen und beim Datenschutz im Internet der Dinge zu ermitteln. Gefragt wurden 122 Bürgerinnen und Bürger der Bundesrepublik Deutschland (BRD) im Alter von 18 bis 70 Jahren. Es wurden keine personenbezogenen Daten der Befragten erhoben. Die Antworten wurden anonym behandelt und gespeichert. Die Befragten wurden im Vorfeld über dieses Vorgehen informiert. Das Ziel der Studie war die Einstellung der Verbraucher zum Datenschutz im Internet der Dinge zu ermitteln. Die Fragen an die Verbraucher deckten 3 Teilbereiche ab. Als Erstes wurde erfragt, inwieweit der jeweilige Befragte Berührungspunkte zu den Geräten hat, die im Internet der Dinge agieren. Des Weiteren wurde gefragt, wie die allgemeine Einstellung der Verbraucher zum Datenschutz ist. Anschließend wurde die Bedeutung der einzelnen Datenschutzprinzipien für die Befragten in Bezug auf die genutzten Anwendungssysteme erfragt. Die Antworten konnte der jeweilige Befragte per Auswahl von einem oder von mehreren vorgegebenen möglichen Antworten treffen. Bei einigen Fragen konnte eine eigene Antwort in ein freies Textfeld eingetragen werden, wenn die Wunschantwort des Befragten nicht unter den vorgegebenen Antworten zu finden war. Die Umfrage wurde mit Hilfe einer Webanwendung für Online-Umfragen auf der Webseite www.umfrageonline.com erstellt. Die Webanwendung ermöglicht die Beantwortung der Fragen direkt auf der Webseite sowie auch das Ausrucken des Umfrageformulars, um die Fragen auf Papier beantworten zu

können. Für die Verteilung der Umfrage an die Verbraucher und für die Beantwortung wurden unterschiedliche, jedoch ausschließlich digitale Medien genutzt. Von den 122 Befragten haben 9 Befragte ihre Fragebögen nicht vollständig ausgefüllt und die Beantwortung nicht abgeschlossen. Da unvollständige Fragebögen die Auswertung verzerren könnten, wurden diese aus der Wertung herausgenommen. Somit wurde die gültige statistische Masse aus 113 befragten Bürgerinnen und Bürger der BRD gebildet.

Die Umfrage hat gezeigt, dass nur 18,5 Prozent der Befragten keine Geräte besitzen, die im Internet der Dinge agieren. Daran sieht man, dass eine große Mehrheit der Bevölkerung Berührungspunkte mit dem Internet der Dinge hat. Das Internet der Dinge verbindet die Mehrheit der Befragten mit der Sorge um ihre Daten. Das zeigt der Wert, dass nur 19,4 Prozent der Befragten sich keine Sorgen darüber macht, dass die smarten Geräte mehr Daten erfassen könnten, als den Nutzern bewusst ist. Bei 42,6 Prozent der Befragten beeinflusst die Sorge um die persönlichen Daten die Entscheidung beim Kauf von smarten Geräten. Die Mehrheit der Befragten sieht die Verantwortung für den Datenschutz beim Gesetzgeber und beim Hersteller. Das bestärkt die Richtigkeit der Entscheidung, sich bei der Analyse des Datenschutzes auf die gesetzlichen Regelungen und auf die Hersteller zu konzentrieren.

4.2 Ermittlung der Schwerpunkte

Wie schon beschrieben, kann auf Grund der großen und unübersichtlichen Anzahl der intelligenten Gräte in unterschiedlichen Anwendungsbereichen des Internets der Dinge, nicht jedes einzelne existierende Gerät beziehungsweise System vom Autor überprüft werden. Jedes Anwendungsgebiet wird jedoch von einem oder wenigen Systemen so dominiert, dass man diese Systeme als Stellvertreter für das ganze Anwendungsgebiet ansehen kann. Dazu kommt, dass nicht jedes Anwendungsgebiet für das Thema dieser Arbeit gleich wichtig ist. Dieses Kapitel befasst sich mit der Ermittlung der für diese Arbeit wichtigsten Anwendungsgebiete, der Schwerpunktsysteme innerhalb der Anwendungsgebiete und der Schwerpunkte des Datenschutzes. Weitere Forschung dieser Arbeit konzentriert sich anschließend auf diese Schwerpunkte.

4.2.1 Schwerpunktanwendungsgebiete

Dieses Unterkapitel befasst sich mit der Frage, in welchem Anwendungsgebiet beziehungsweise in welchen Anwendungsgebieten des Internets der Dinge der Datenschutz für die Nutzer am wichtigsten ist. Aus der Sicht des Autors sind hierbei zwei Kriterien zu beachten. Zum einen gilt es herauszufinden, in welchem Anwendungsgebiet die wichtigsten und sensibelsten Daten der Nutzer erhoben werden. Zum anderen darf das individuelle Empfinden der Nutzer nicht vernachlässigt werden.

Die Datenschutz-Grundverordnung weist einigen Kategorien der personenbezogenen Daten eine besondere Bedeutung zu. Diese Kategorien der besonders wichtigen und sensiblen Daten werden im Artikel 9 der DSGVO definiert. Die Verarbeitung dieser Daten

ist, bis auf einige im selben Artikel der DSGVO definierten Ausnahmefälle, untersagt. Geräte eines Anwendungsgebietes des Internets der Dinge sind dafür konzipiert, um vor allem diese Kategorien der Benutzerdaten zu erheben und zu verarbeiten. Dieses Anwendungsgebiet sind die Wearables. Wie schon in vorherigen Kapiteln beschrieben, erheben und verarbeiten Wearables genetische, biometrische und Gesundheitsdaten der Nutzer. Da diese Daten zu den im Artikel 9 der DSGVO beschriebenen Kategorien gehören, legt der Autor Wearables als ein Schwerpunktanwendungsgebiet für die folgende Untersuchung fest. Laut der Auswertung der Umfragestudie des Autors hat fast jeder zweite Befragte Wearables in Nutzung. Das stärkt die Bedeutung dieses Anwendungsgebietes und untermauert die Richtigkeit der Entscheidung Wearables als einen Schwerpunkt festzulegen. Bei der Studie gaben 49 der 113 Befragten an, dass sie Wearables nutzen, was 43,4 Prozent entspricht.

Um die Frage zu beantworten, welchem Anwendungsgebiet des Internets der Dinge die Nutzer bei der Verarbeitung ihrer personenbezogenen Daten am kritischsten gegenüberstehen, werden mehrere Umfragestudien ausgewertet. Neben den im Internet veröffentlichten Studien unterschiedlicher Quellen aus dem Jahr 2018, wird auch die vom Autor im Jahr 2019 durchgeführte Studie ausgewertet.

Eine der Umfragestudien, von denen die Ergebnisse zum Teil im Internet veröffentlicht wurden, ist die Studie von Convios Consulting[27]. Sie wurde von den E-Mail-Anbietern GMX und WEB.DE in Auftrag gegeben. Für diese Studie wurden im März 2018 insgesamt 1.008 Internetnutzer ab 14 Jahren befragt. Zum Zeitpunkt der Umfrage hatte jeder fünfte Deutsche einen digitalen Sprachassistenten und ebenso viele planten eine Anschaffung so eines Geräts. Rund 62 Prozent der Befragten hatten Bedenken Sprachassistenten zu verwenden. Ein Drittel davon befürchtete sogar, dass die private Kommunikation permanent überwacht und von unbefugten Dritten mitgehört und gespeichert wird. (GMX, 2018)

Vom 31. Januar bis zum 6. Februar 2018 wurde eine Umfragestudie von Statista durchgeführt, die von nextMedia.Hamburg[28] in Auftrag gegeben wurde. Laut dieser Studie besaßen zum Zeitpunkt der Umfrage 14 Prozent der Befragten einen Sprachassistenten. Mehr als drei Viertel, genauer gesagt 77 Prozent der Befragten, fühlten sich in Bezug auf den Datenschutz bei Sprachassistenten unsicher. (nextMedia.Hamburg, 2018)

Bei einer Studie des deutschen Softwareunternehmens für IT-Sicherheitslösungen G Data wurden im Jahr 2018 eintausend deutsche Internetnutzer befragt wie groß ihr Vertrauen zu den vernetzten Geräten ist. Am wenigsten vertrauten Nutzer zum Zeitpunkt der Umfrage den Smarthome-Geräten und den intelligenten Audiogeräten. Dabei hatten 42,5 Prozent wenig oder sogar gar kein Vertrauen in vernetzte Audiogeräte und 44,2 Prozent in Smarthome-Geräte. Bei der Frage wie sicher Nutzer die Geräte in Bezug auf Schadprogramme und andere Cybergefahren halten, schnitten intelligente Audiogeräte am schlechtesten ab. Mehr als die Hälfte, genau 62,5 Prozent, der Befragten gaben an,

[27] Convios Consulting: Ein deutsches Unternehmen für Unternehmensberatung, Systemplanung und Systementwicklung.

[28] nextMedia.Hamburg: Ein deutsches Unternehmen, das eine innovationsorientierte Zusammenarbeit zwischen Medien- und Digitalunternehmen, Hochschulen, ihren Studierenden sowie engagierten Treibern aus Hamburg unterstützt. (nextMedia.Hamburg, 2018)

intelligente Audiogeräte für wenig oder gar nicht sicher zu halten. Ebenso waren mehr als die Hälfte der Befragten der Meinung, dass Unternehmen seit der Einführung der EU-DSGVO nicht verantwortungsvoller mit persönlichen Daten umgehen würden. (gdata.de, 2018)

NORDLIGHT research, ein deutsches Unternehmen aus Hilden für individuelle Marktforschungslösungen, führte ebenfalls im Frühjahr 2018 eine Umfragestudie durch. Bei dieser Studie wurden 1100 Bundesbürger ab 14 Jahren in deutschen Haushalten mit einem Internetanschluss nach Ihrer Meinung zum Smarthome befragt. Es wurden vernetzte Audiogeräte zum Anwendungsgebiet des Smarthomes gezählt. Bei der Frage, wie hoch die Befragten die Gefahr sehen von Smarthome-Geräten ausspioniert zu werden, gaben lediglich 18 Prozent an, dass sie es für unbedenklich halten. Rund die Hälfte gab an, dass sie die Gefahr für hoch einschätzen. (NORDLIGHT research, 2018)

Die bisherigen Studien deuten auf ein ziemlich eindeutiges Ergebnis hin. In jeder betrachteten Studie hielten die Nutzer intelligente Audiogeräte für eine große oder sogar die größte Gefahr für ihre persönlichen Daten. Diese Audiogeräte kann man nicht eindeutig einem Anwendungsgebiet zuordnen, weil sie zum Teil mehrere Anwendungsgebiete berühren. Sie werden als intelligente oder als vernetzte Audiogeräte oder auch als Sprachassistenten bezeichnet. In dieser Arbeit hat der Autor Sprachassistenten dem Anwendungsgebiet der vernetzten Audiogeräte zugeordnet. Um die Ergebnisse der im Jahr 2018 durchgeführten Studien zu untermauern, wird die vom Autor im Frühjahr 2019 durchgeführte Umfragestudie hinzugezogen. Bei der vom Autor durchgeführten Studie wurden Nutzer gefragt, welche Smarthome-Geräte sie besitzen. Die meisten Befragten, mit 68,8 Prozent, gaben an, intelligente Beleuchtungssteuerung einzusetzen. Mit 56,3 Prozent besitzt mehr als die Hälfte der Befragten auch Geräte der Unterhaltungselektronik oder Sprachassistenten. Da Sprachassistenten auch Internetradio und Musik von Streamingdiensten oder aus eigenen Musikquellen abspielen können, kann man sie auch der Unterhaltungselektronik zuordnen. Die Nutzer wurden auch gefragt, beim Einsatz welcher Geräte sie die größten Sorgen haben, dass diese mehr Daten von ihnen sammeln, als sie es wollen beziehungsweise welchen Geräten sie am meisten misstrauen.

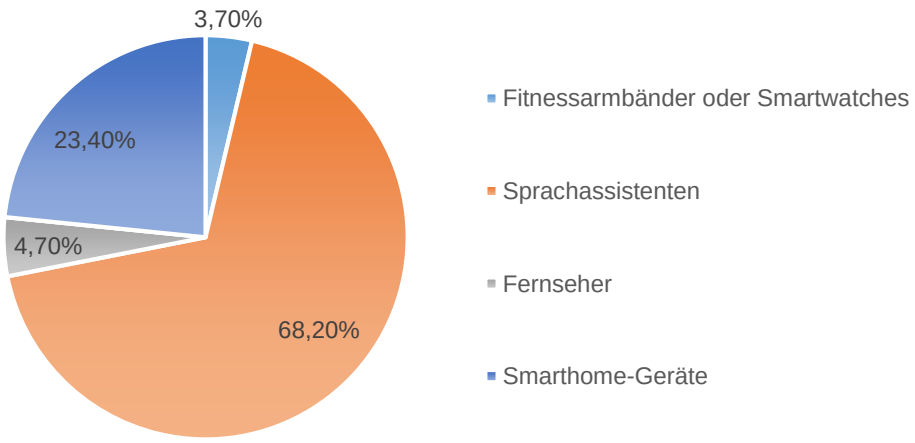


Abbildung 17: Misstrauen zu den vernetzten Geräten
Quelle: Eigene Umfragestudie

Mit 68,75 Prozent misstrauen mehr Nutzer den Sprachassistenten als allen anderen Geräten zusammen. Abbildung 17 zeigt welcher Anteil der befragten Nutzer welchen Geräten am meisten misstrauen.

Die Ergebnisse der vom Autor durchgeführten Studie bestätigen das schon aus den vorherigen Studien ermittelte Datenschutzempfinden der Nutzer gegenüber den vernetzten Geräten. Die Angst der Nutzer von vernetzten Audiogeräten ausspioniert zu werden ist sogar gegenüber dem Vorjahr gestiegen.

Auf Grund der ermittelten besonders hohen Sensibilität der Daten, die Wearables erheben und verarbeiten und auf Grund der besonders großen Bedenken der Nutzer gegenüber den vernetzten Audiogeräten, werden diese zwei Anwendungsgebiete des Internets der Dinge vom Autor als Schwerpunktanwendungsgebiete für weitere Untersuchungen festgelegt.

4.2.2 Schwerpunktsysteme

Nachdem die Wearables und vernetzte Audiogeräte beziehungsweise Sprachassistenten als Schwerpunktanwendungsgebiete ermittelt wurden, wird in diesem Unterkapitel ermittelt, welche Systeme dieser Schwerpunkte im Weiteren untersucht werden. Wie bei allen anderen Anwendungsgebieten gibt es auch bei diesen zwei Schwerpunktgebieten vielfältige Systeme innerhalb des jeweiligen Anwendungsgebietes. Die Vielfalt der Anwendungssysteme ist zwar unüberschaubar, jedoch wird jedes Anwendungsgebiet von einer überschaubaren Anzahl der Hersteller dieser Systeme dominiert. Da es für den Autor unmöglich ist, jedes existierende Anwendungssystem zu untersuchen, werden in dieser Arbeit Systeme analysiert, die das jeweilige Gebiet so dominieren, dass sie als Stellvertreter für das gesamte Anwendungsgebiet angesehen werden können.

Bei der Ermittlung der wichtigsten Hersteller von Wearables wird geprüft, welche Hersteller den Markt in diesem Bereich dominieren. Für diese Ermittlung werden die Weltmarktanteile der Hersteller der letzten 2 Quartale, für die es im Frühjahr 2019 verfügbare Werte gibt, herangezogen. Tabelle 1 zeigt die vom Marktforschungsunternehmen IDC ermittelten Werte für die weltweiten Marktanteile der Hersteller in diesem Bereich. Man erkennt, dass in den zwei letzten Quartalen, für die Werte verfügbar sind, dieselben fünf Hersteller den Markt für Wearables dominieren.

Tabelle 1: Weltweite Marktanteile der Hersteller von Wearables

Hersteller	Marktanteil in Prozent im Quartal 3 2018	Marktanteil in Prozent im Quartal 4 2018
Apple	13,1	27,4
Xiaomi	21,5	12,6
Huawei	5,9	9,6
Fitbit	10,9	9,4
Samsung	5,6	6,8
Andere	43	34,3

Quelle: statista.com, 2019

Für diese Arbeit ist nicht nur die weltweite Marktaufteilung interessant, sondern auch von welchen Herstellern Geräte in Deutschland vorwiegend genutzt werden. Im Rahmen der vom Autor durchgeführten Studie wurden die Nutzer gefragt, von welchem Hersteller sie Wearables besitzen. Abbildung 18 zeigt, dass es zwar Abweichungen von den weltweiten Marktanteilen gibt, jedoch auch in Deutschland dieselben Hersteller diesen Bereich anführen.

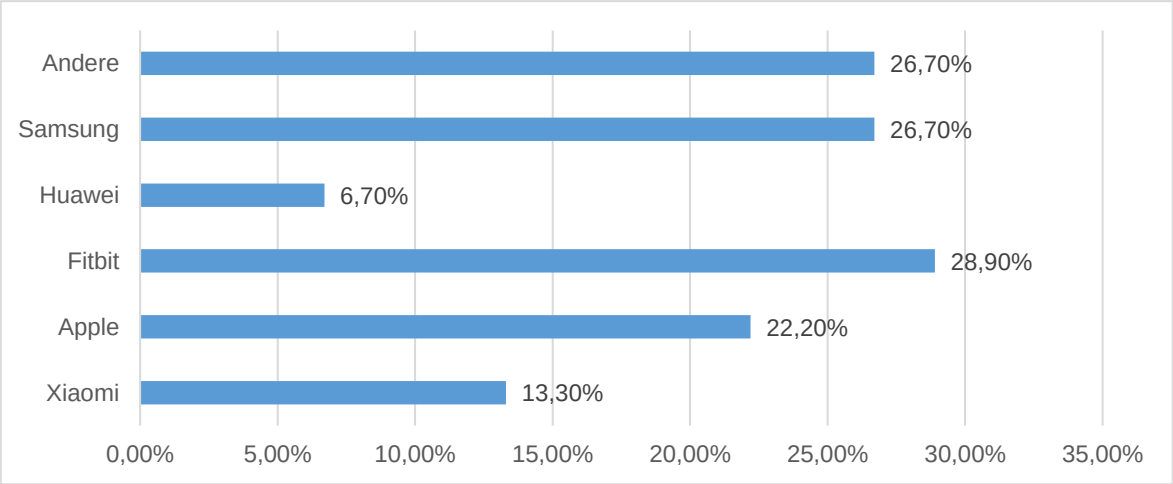


Abbildung 18: Anteile der genutzten Wearables nach Hersteller in Deutschland
Quelle: Eigene Studie

Nachdem die wichtigsten Hersteller der Wearables ermittelt wurden, muss noch ermittelt werden welche Art der Wearables vorwiegend genutzt wird. Diese Frage wurde den Teilnehmern der Umfragestudie des Autors gestellt. Abbildung 19 zeigt, dass vorwiegend Fitnessarmbänder und Smartwatches genutzt werden. Der Anteil von anderen Arten der Wearables ist so gering, dass er vernachlässigt werden kann.

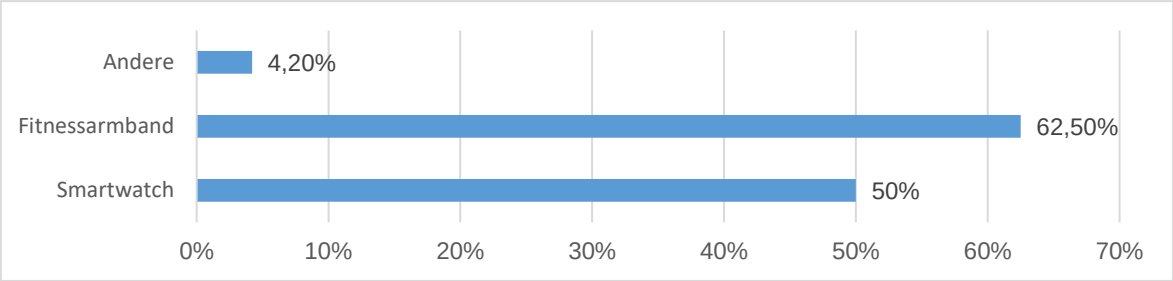


Abbildung 19: Arten der genutzten Wearables in Deutschland
Quelle: Eigene Studie

Als Grundlage der Ermittlung der dominierenden vernetzten intelligenten Audiosysteme werden ebenfalls weltweite Marktanteile der Hersteller dieser Systeme in den letzten zwei Quartalen, für die Marktwerte verfügbar sind, verwendet. Da auch für diesen Bereich vorwiegend die Nutzung in Deutschland interessant ist, wird die Studie des Autors unterstützend hinzugezogen. Abbildung 20 zeigt die weltweiten Marktanteile der Hersteller von Sprachassistenten. An dieser Abbildung erkennt man, dass die Hersteller Amazon und Google den Markt noch beherrschen. Man erkennt auch, dass vor allem asiatische Hersteller mit großer Geschwindigkeit aufholen.

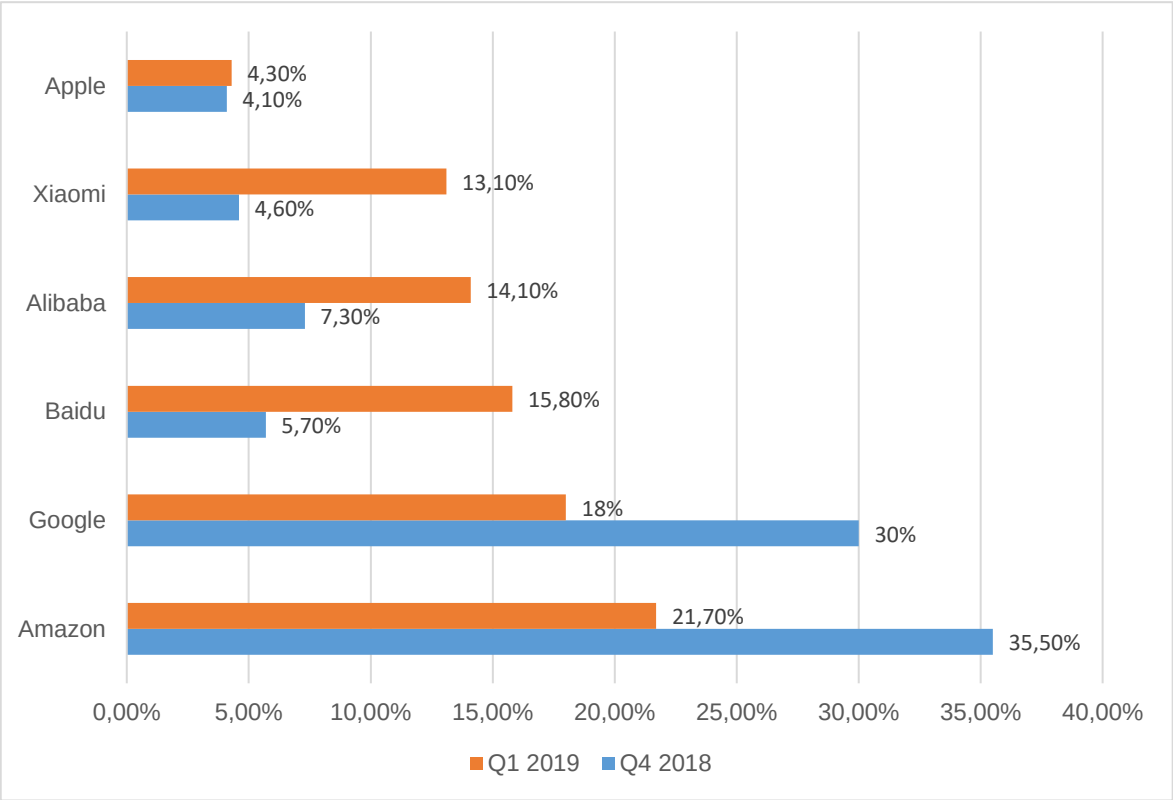


Abbildung 20: Weltweite Marktanteile am Absatz von intelligenten Lautsprechern
Quelle: statista.com, 2019

Bei der Frage an die Nutzer in Deutschland, welche Sprachassistenten sie im Besitz haben, sieht man, dass die asiatischen Hersteller in Deutschland im Frühjahr 2019 noch kaum eine Bedeutung haben. Hier dominieren mit einem großen Abstand die Hersteller Amazon und Google. Abbildung 21 verdeutlicht diesen Umstand. Damit kann man Systeme dieser beiden Hersteller als Stellvertreter für das gesamte Anwendungsgebiet der vernetzten Audiosysteme in Deutschland ansehen.

Da die Anzahl der Modelle der Sprachassistenten dieser beiden Hersteller im Frühjahr 2019 noch überschaubar ist, werden im Weiteren alle zu diesem Zeitpunkt verfügbaren und aktuellen Modelle dieser Systeme überprüft.

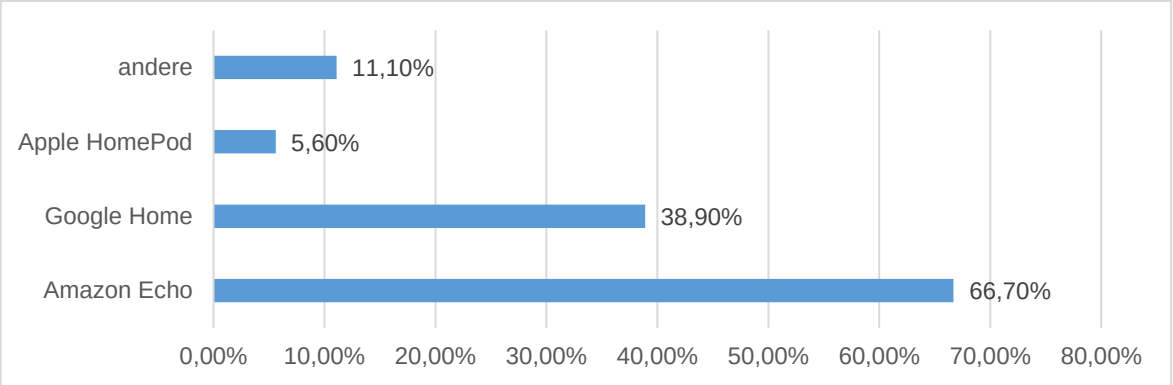


Abbildung 21: Anteile der Sprachassistenten im Besitz deutscher Anwender
Quelle: Eigene Studie

4.2.3 Datenschutzschwerpunkte

Dieses Unterkapitel befasst sich mit der Frage, in welchen Punkten der Datenschutz im Internet der Dinge für die Verbraucher besonders wichtig ist. Um herauszufinden auf welcher Seite Verbraucher die Verantwortung für den Datenschutz sehen, wurden Nutzer im Rahmen der Studie des Autors gefragt, ob der Gesetzgeber, der Hersteller oder der Verbraucher selbst für den Datenschutz verantwortlich ist. Mehr als die Hälfte der Befragten sehen den Gesetzgeber, mit 59,3 Prozent, und die Hersteller, mit 66,7 Prozent, in der Verantwortung. Nur 38,9 Prozent der Befragten sehen diese Verantwortung beim Nutzer selbst. Aus diesem Grund konzentriert sich diese Arbeit im Weiteren auf die gesetzlichen Vorgaben und die Einhaltung dieser Vorgaben seitens der Hersteller. In vorherigen Kapiteln wurde schon festgestellt, dass die EU Datenschutz-Grundverordnung seit dem 25. Mai 2018 die wichtigsten Regelungen zum Datenschutz in der Europäischen Union enthält. Im Rahmen der Umfragestudie des Autors wurde auch nach der Meinung der Verbraucher zu dieser Verordnung gefragt. Obwohl diese Verordnung nach Meinung von 28,7 Prozent der Befragten die Arbeit erschwert, sind mehr Verbraucher einer positiven Meinung dazu. Genau 37 Prozent der Befragten finden es gut, dass der Datenschutz EU-weit verbindlich angeglichen wurde und 31,5 Prozent finden, dass der Datenschutz dadurch verbessert wurde. Eine große Mehrheit findet die Bestrebungen den Datenschutz geografisch auszuweiten gut. Somit befürworten 94,44 Prozent der Befragten internationale Regelungen für den Datenschutz. Die Mehrheit, 65,74 Prozent, ist sogar für den weltweiten, nicht nur den europäischen Datenschutz. Die Abbildung 22 verdeutlicht grafisch diese Meinungsvertretung der Verbraucher.

Abbildung 22: Wie weit der Datenschutz geografisch ausgedehnt werden sollte
Quelle: eigene Studie

Im zweiten Kapitel wurden Datenschutzprinzipien aus den in der EU Datenschutz-Grundverordnung behandelten Datenschutzgrundsätzen und den Verbraucherrechten ermittelt. Da die DSGVO die wichtigsten datenschutzrechtlichen Regelungen für diese Arbeit enthält, werden die Datenschutzschwerpunkte unter Beachtung der Einstellung der Verbraucher und der technischen Überprüfbarkeit aus diesen Datenschutzprinzipien abgeleitet. Daraus ergeben sich folgende Schwerpunkte:

- Rechtmäßigkeit der Verarbeitung der personenbezogenen Daten
    - Einwilligung des Nutzers vor der Verarbeitung der ihn betreffenden personenbezogenen Daten nach Artikel 6 Absatz 1 Buchstabe a) DSGVO

    - Erforderlichkeit der Verarbeitung personenbezogener Daten für die Erfüllung des Vertrages oder zur Durchführung vorvertraglicher Bedingungen nach Artikel 6 Absatz 1 Buchstabe b) DSGVO
- Bedingungen für die Einwilligung der Verarbeitung der personenbezogenen Daten
    - Einwilligung des Nutzers für die Verarbeitung seiner Daten für andere Sachverhalte nach Artikel 7 Absatz 2 DSGVO
    - Möglichkeit des Einwilligungswiderrufs nach Artikel 7 Absatz 3 DSGVO
    - Einfachheit des Einwilligungswiderrufs nach Artikel 7 Absatz 3 DSGVO
    - Zwang zur Einwilligung der Verarbeitung der personenbezogenen Daten für Zwecke, die für die Erfüllung des Vertrages nicht erforderlich sind nach Artikel 7 Absatz 4 DSGVO
    - Alter des Nutzers nach Artikel 8 DSGVO
- Verarbeitung besonderer Kategorien personenbezogener Daten
    - Einwilligung des Nutzers oder Ausnahmegründe für dir Verarbeitung dieser Daten nach Artikel 9 DSGVO
- Transparenz
    - Verständlichkeit der übermittelten Informationen über die Verarbeitung der Nutzerdaten nach Artikel 12 Absatz 1 DSGVO
    - Reaktion auf Anfragen des Nutzers nach Artikel 12 Absatz 3 und 4 DSGVO
    - Entgelt für die Zurverfügungstellung der Informationen über die verarbeiteten Daten nach Artikel 12 Absatz 5 DSGVO
- Informationspflicht bei der Erhebung der personenbezogenen Daten
    - Zeitpunkt der Information über die Erhebung der Nutzerdaten nach Artikel 13 Absatz 1 und 2 DSGVO
- Auskunftsrecht nach Artikel 15 Absatz 1 DSGVO
- Recht auf Berichtigung nach Artikel 16 DSGVO
- Recht auf Löschung nach Artikel 17 Absatz 1 Buchstabe b) DSGVO
- Recht auf Datenübertragbarkeit nach Artikel 20 DSGVO
- Datenschutz durch Technikgestaltung und Voreinstellungen nach Artikel 25 Absatz 1 und 2 DSGVO
- Sicherheit der Verarbeitung nach Artikel 32 DSGVO

4.2.4 Schlussfolgerung

Durch die Ermittlung der Schwerpunkte der einzelnen Bereiche unter der Beachtung der gesetzlichen Regelungen und der Einstellung und Wünsche der Verbraucher ergibt sich die Schlussfolgerung, dass im Weiteren folgende Systeme auf die Einhaltung der ermittelten Schwerpunktdatenschutzprinzipien untersucht werden:

- Smartwatches und Firnessarmbänder der fünf führenden Hersteller in diesem Bereich und
- Sprachassistenten der führenden zwei Hersteller im Bereich der vernetzten intelligenten Audiosysteme.

4.3 Überprüfung der Schwerpunkte

Nachdem die Schwerpunkte bei den Systemen im Internet der Dinge und dem Datenschutz in diesem Bereich ermittelt wurden, werden diese Systeme auf die Einhaltung der Datenschutzvorgaben überprüft.

4.3.1 Prüfverfahren und Prüfumgebungen

Die zu überprüfenden Anwendungssysteme bestehen aus zwei hauptsächlichen Komponenten, der Hardware und der auf dieser Hardware laufenden Software. Die Hardware teilt sich auf zwei Seiten auf. Hardware, die sich im Besitz der Nutzer befindet, sind die Clients[29]. In diesem Fall sind es Wearables und vernetzte Lautsprecher. Clients dienen der Aufnahme und der Ausgabe der Daten. Für die Aufnahme der Daten besitzen die meisten Smartwatches und Fitnessarmbänder Sensoren für Pulsmessung, Positionserkennung und Schrittzähler. Einige Geräte sind mit weiteren Sensoren und Mikrofonen ausgestattet. Vernetzte Audiosysteme besitzen zur Aufnahme der Daten Mikrofone oder Videokameras. Die Ausgabe der Daten findet bei beiden Kategorien der Clients über Lautsprecher oder Bildschirme statt. Die Verarbeitung der Daten findet nicht auf den Clients selbst, sondern auf den Servern der Anbieter statt. Diese Anwendungssysteme funktionieren also nach dem Client-Server-Prinzip. Die Clients selbst, also Wearables und vernetzte Audiosysteme, sind ohne entsprechende Dienste kaum funktionsfähig. Dienste sind die eigentliche Künstliche Intelligenz der Anwendungssysteme. Sie laufen mit Hilfe der Software auf den Servern und Clients der jeweiligen Systeme. Sie steuern die Aufnahme der Daten über die in Clients integrierten Sensoren. Anschließend entscheidet die Software auf den Servern wie die Daten verarbeitet werden und welche Daten auf den Endgeräten ausgegeben werden. Bei den zu prüfenden Anwendungssystemen spielen Dienste der Anbieter die Hauptrolle. Nutzungsbedingungen und Datenschutztexte der Anbieter sind hauptsächlich auf diese Dienste ausgerichtet. Die Hardware, in diesem Fall Smartwatches, Fitnessarmbänder und vernetzte Lautsprecher, wird für diese Dienste entwickelt und produziert. Die Hersteller Xiaomi, Fitbit, Huawei, Samsung und Google bieten einen Dienst für mehrere Gerätearten ihrer eigenen Marke an. Google bietet seinen Dienst jedem Hersteller an, der Geräte für Googles Dienst herstellt. Wearables von Huawei nutzen das Betriebssystem Wear OS von Google. Somit nutzen Geräte von Huawei, neben den eigenen Diensten, auch die Dienste von Google. Nur der Dienst von Apple wird ausschließlich von einer in dieser Arbeit behandelten Geräteart genutzt, da Apple nur eine Art der Wearables herstellt und seine Dienste anderen Herstellern nicht anbietet. Abbildung 23 zeigt die Struktur der Funktionsweise der Wearables. Diese Struktur wird auch vom Autor zur Überprüfung der Einhaltung der Datenschutzvorgaben beim Einsatz von Wearables hergestellt und genutzt.

[29] Client: Eine Anwendung, die mit Hilfe der Dienste des Servers arbeitet.

Abbildung 23: Struktur der Funktionsweise von Wearables
Quelle: Eigene Darstellung

Zur Überprüfung der Datenschutzvorgaben bei Wearables werden jeweils ein im Frühjahr 2019 aktuelles Modell der Smartwatches und der Fitnessarmbänder von jedem betroffenen Hersteller genutzt. Dazu gehören folgende Smartwatches:

- Xiaomi Amazfit Stratos,
- Fitbit Versa,
- Huawei Watch 2,
- Samsung Gear S3 und
- Apple Watch Series 4.

Bei den Fitnessarmbändern werden folgende Modelle zur Überprüfung genutzt:

- Xiaomi Mi Band 3,
- Fitbit Charge 3,
- Huawei Band 3 und
- Samsung Gear Fit 2 Pro.

Wie bei den Wearables, wird auch bei den Sprachassistenten ein Dienst für mehrere unterschiedliche Modelle der Clients genutzt. Amazon stellt zwei Formen von Clients für seinen Dienst für Sprachassistenten her. Eine Form der Clients sind vernetzte Lautsprecher mit Mikrofonen. Die andere Form der Clients sind vernetzte Lautsprecher mit einem Bildschirm und einer Videokamera. Google stellt Geräte dieser Art nur ohne Videokamera und Bildschirm her. Bei Clients der Sprachassistenten ohne Bildschirm werden Einstellungen mit Hilfe des Bildschirms eines Smartphones vorgenommen. Clients mit einem eigenen Bildschirm, wie bei Amazon Echo Show, kommen ohne Smartphones aus, da Einstellungen direkt auf dem Bildschirm des Gerätes vorgenommen werden können. Abbildung 24 zeigt die Struktur der Funktionsweise der Sprachassistenten. Diese Struktur wird vom Autor hergestellt und zum Überprüfen der Datenschutzvorgaben bei der Sprachassistenten genutzt.

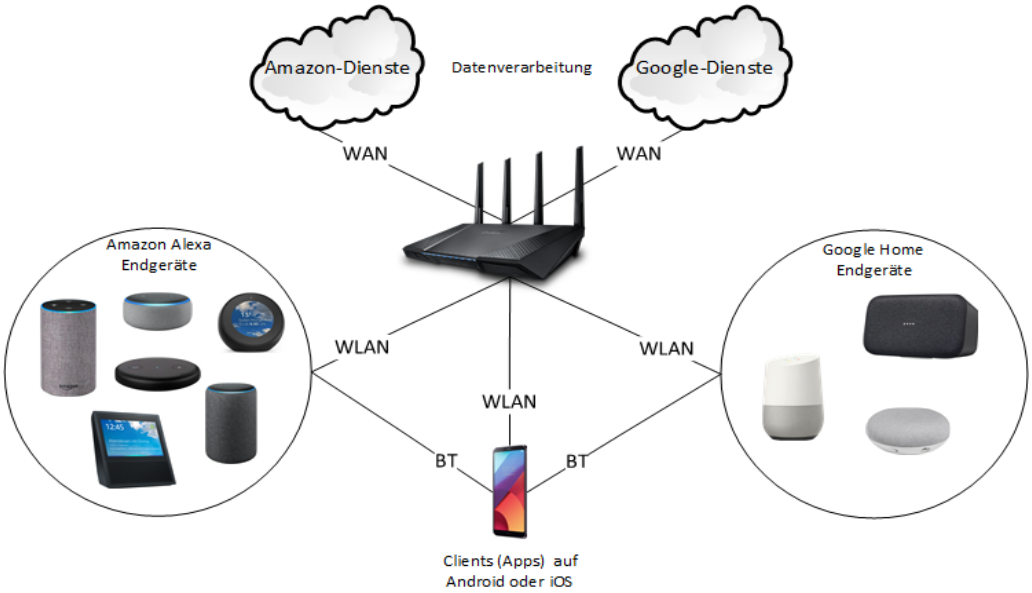


Abbildung 24: Struktur der Funktionsweise von Sprachassistenten
Quelle: Eigene Darstellung

Die Überprüfung bei Sprachassistenten findet, wie auch bei Wearables, mit Hilfe der im Frühjahr aktuellen Endgeräte statt. Wie die Abbildung 24 zeigt werden Geräte Google Home, Google Home Mini und Google Home Max für die Überprüfung der Datenschutzeinhaltung beim Einsatz der Sprachassistenten von Google genutzt. Zur Überprüfung der Datenschutzeinhaltung bei Sprachassistenten von Amazon werden Geräte mit integriertem Bildschirm sowie auch ohne Bildschirm genutzt. Zu den Geräten ohne Bildschirm gehören Amazon Echo 2, Amazon Echo Dot 3, Amazon Echo Input und Amazon Echo Plus. Amazon Echo Spot und Amazon Echo Show besitzen einen integrierten Bildschirm und werden ebenfalls getestet.

Zur Überprüfung der Einhaltung der Datenschutzprinzipien werden bei allen zu prüfenden Anwendungssystemen Datenschutztexte, Hardware der Clients sowie die dazugehörige Software untersucht. Da Datenschutztexte nicht explizit für jedes Gerätemodell, sondern für den geräteübergreifenden Dienst der jeweiligen Hersteller beziehungsweise der Diensteanbieter gelten, werden sechs Datenschutzerklärungen der Anbieter der Dienste für Wearables geprüft. Google bietet seine Dienste für Wearables und Sprachassistenten an und hat für beide Bereiche dieselbe Datenschutzrichtline. Explizit nur für Sprachassistenten wird die Datenschutzrichtlinie von Amazon geprüft. Diese gilt, wie schon beschrieben, für alle Sprachassistenzendgeräte von Amazon. Hardware und Software der Geräte werden auf datenschutzrelevante Auffälligkeiten und Einstellungsmöglichkeiten untersucht. Dabei wird bei der Untersuchung jedes Dienstes und der dazugehörigen Geräte jeweils ein Prüfprotokoll erstellt. In diesen Protokollen werden Ergebnisse der Untersuchungen zu den überprüfbaren und relevanten Datenschutzprinzipien festgehalten. Sprachassistenzgeräte beider Hersteller weisen ein nach Artikel 25 DSGVO wichtiges Merkmal für den Datenschutz auf. Diese Geräte besitzen eine Hardwaretaste, die es dem Nutzer ermöglicht

integrierte Mikrofone abzuschalten. Die Funktionalität dieser Hardwaretasten wird ebenfalls überprüft, indem jeweils bei eingeschalteten und ausgeschalteten Mikrofonen Datenflüsse zwischen den Sprachassistenten und dem Internet gemessen werden. Ergebnisse dieser Messungen werden in gesonderten Prüfprotokollen festgehalten. Abbildung 25 zeigt ein Beispiel der Testumgebung für diese Überprüfungen.

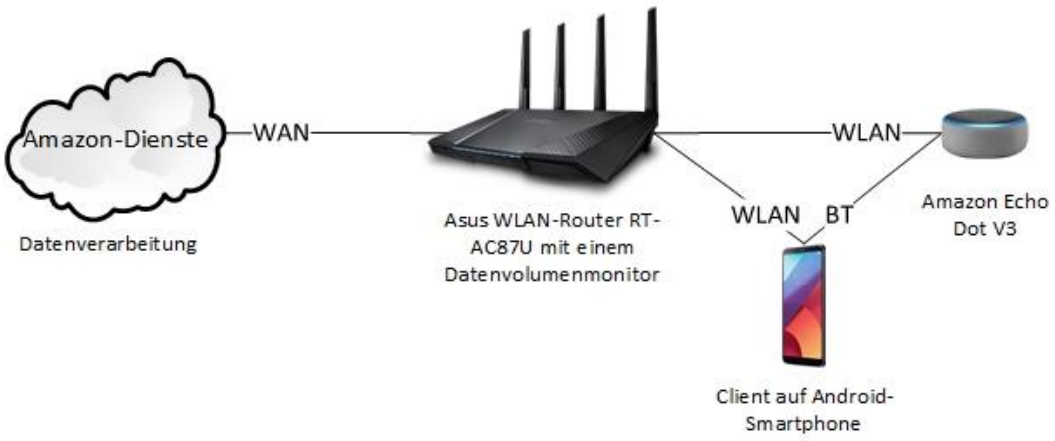


Abbildung 25: Testumgebung für die Überprüfung der Handwaretasten
Quelle: Eigene Darstellung

Anschließend werden die Ergebnisse aller Prüfprotokolle nach Datenschutzprinzipien gruppiert und in folgendem Unterkapitel zusammengefasst. Detailliertere Beschreibungen der Abläufe und Ergebnisse der Überprüfungen kann man den in der Anlage enthaltenen Prüfprotokollen entnehmen.

4.3.2 Prüfergebnisse

4.3.2.1 Rechtmäßigkeit der Verarbeitung

Die Rechtmäßigkeit der Verarbeitung personenbezogener Daten der Nutzer ist das erste Kriterium nach dem Anwendungssysteme überprüft werden. Nach Artikel 6 Absatz 1 Buchstabe a) DSGVO sollte der Nutzer vor der Erhebung seiner Daten, also vor der Nutzung des Dienstes, um eine Einwilligung zur Verarbeitung der ihn betreffenden personenbezogenen Daten gefragt werden. Bei der Überprüfung, inwieweit sich die betroffenen Diensteanbieter an dieses Gebot halten, wurde festgestellt, dass bei allen getesteten Systemen vor der Nutzung darauf hingewiesen wird, dass man mit der Nutzung des Dienstes den Nutzungsbedingungen des Diensteanbieters zustimmt. Nutzungsbedingungen für die jeweiligen Dienste enthalten unter anderem auch Datenschutzbestimmungen. Eine Nutzung der Dienste ohne eine Einwilligung zur Verarbeitung seiner Daten erteilt zu haben, ist demnach nicht möglich. Um zu sehen, welche Daten vom Dienst erhoben werden, muss der Nutzer Datenschutztexte einsehen. Diese sind bei allen Anbietern über eine oder mehrere Verknüpfungen erreichbar. Laut der Umfragestudie des Autors lesen lediglich 16,8 Prozent der Nutzer diese

Nutzungsbestimmungen. Diensteanbieter Samsung und Apple bieten dem Nutzer die Möglichkeit an, zusätzlich die Verarbeitung seiner Daten für weitere Zwecke einzuwilligen. Positiv anzumerken ist, dass der Verbraucher bei der Nutzung der Wearables von Samsung nicht gezwungen wird, die Verarbeitung besonderer Kategorien seiner Daten nach Artikel 9 DSGVO einzuwilligen. Diese Einwilligung ist im Gegensatz zu den anderen Diensteanbietern bei Samsung optional. Da bei Wearables diese Kategorien der Nutzerdaten zur Erfüllung der Funktionalität des Dienstes erforderlich sind, ist der Dienst ohne dieser Daten nur sehr eingeschränkt nutzungsfähig. Bei den Anbietern Apple, Huawei, Amazon und Google willigt man die Verarbeitung seiner Daten mit dem Fortfahren der Nutzung des Dienstes implizit ein. Bei Xiaomi, Fitbit und Samsung geschieht das explizit mittels eines Einwilligungshakens. Wobei dieser Einwilligungshaken bei Xiaomi voraktiviert ist, was nicht den Vorgaben des Artikels 25 DSGVO entspricht.

4.3.2.2 Bedingungen für die Einwilligung

Bei der Überprüfung, der Einwilligungsmöglichkeiten zur Verarbeitung der Daten für weitere Sachverhalte, wurde festgestellt, dass nur bei Xiaomi kein separates Ersuchen für so eine Einwilligung erfolgt. Bei allen anderen getesteten Systemen konnte man die Verarbeitung der Daten für weitere Zwecke, wie zum Beispiel personalisierte Werbung, einwilligen. Das Erteilen und Zurückziehen der Einwilligung erfolgt auf unterschiedlichen Wegen und ist unterschiedlich einfach beziehungsweise schwierig. Einzelheiten zu diesen Einwilligungsmöglichkeiten können den Prüfprotokollen entnommen werden.

Die Einwilligung zur generellen Verarbeitung der Nutzerdaten kann ebenfalls auf unterschiedlichen Wegen zurückgezogen werden. Bei Xiaomi kann das Zurückziehen dieser Einwilligung einfach in der dazugehörigen App oder per E-Mail erfolgen. Bei allen anderen Anbietern kann man die Einwilligung durch das Löschen des Accounts zurückziehen. Damit ist der Widerruf seiner Einwilligung nach Meinung des Autors nur bei Xiaomi so einfach wie die Erteilung dieser Einwilligung. Einen Hinweis nach Artikel 7 Absatz 3 DSGVO, dass der Nutzer die Einwilligung zur Verarbeitung seiner Daten jederzeit widerrufen kann, konnte der Autor nur bei Apple nicht finden.

Alle Diensteanbieter prüfen bei der Registrierung das Alter der Nutzer nach Artikel 8 DSGVO. Bei Xiaomi, Google und Fitbit wird darauf hingewiesen, dass Personen, die das 16. Lebensjahr nicht vollendet haben, den Dienst nur mit einer Zustimmung der Erziehungsberechtigten nutzen können. Bei Apple, Huawei und Samsung müssen die Nutzer mindestens 16 Jahre alt sein. Alle Amazon-Dienste können nur von Erwachsenen ab dem vollendeten 18. Lebensjahr genutzt werden.

4.3.2.3 Verarbeitung besonderer Kategorien personenbezogener Daten

Alle betroffenen Wearable-Dienste verarbeiten biometrische und Gesundheitsdaten nach Artikel 9 DSGVO. Von Sprachassistenzsystemen werden diese Daten nicht explizit erhoben. Sie können jedoch zufällig aufgenommen werden. Bei allen betroffenen Wearables stimmt der Nutzer vor der Nutzung des Dienstes der Verarbeitung der besonderen Kategorien der personenbezogenen Daten zu. Bei Fitbit, Huawei und Samsung

werden diese Daten vor der Einwilligung explizit erläutert. Bei Samsung hat der Nutzer, wie schon beschrieben, die Möglichkeit die Einwilligung zur Verarbeitung dieser Daten nicht zu erteilen. Xiaomi und Google erläutern diese Daten in ihren Datenschutztexten, ohne explizite Einwilligung für die Verarbeitung dieser Daten vor der Nutzung des Dienstes einzuholen. Bei Apple und Amazon hat der Autor keine Erwähnung dieser Art von personenbezogenen Daten gefunden.

4.3.2.4 Transparenz

Laut der Umfragestudie des Autors ist es rund 91 Prozent der Befragten wichtig oder sehr wichtig, vor der Benutzung eines Gerätes in einer klaren und einfachen Sprache darüber informiert zu werden, welche Daten vom ihm erhoben und zu welchem Zweck diese verarbeitet werden. Nach Artikel 12 Absatz 1 DSGVO soll diese Information außerdem noch präzise, transparent, verständlich und leicht zugänglich sein. Diese Information stellen alle getesteten Dienstanbieter in ihren Datenschutzerklärungen beziehungsweise Nutzungsbedingungen, die Datenschutztexte beinhalten bereit. Manche Diensteanbieter, wie zum Beispiel Huawei, informieren die Nutzer noch zusätzlich vor dem ersten Starten der Software in Form einer kurzen Meldung, dass besondere Kategorien der personenbezogenen Daten erhoben werden. Datenschutzerklärungen sind bei allen Anbietern im Google Play Store beziehungsweise im Apple App Store über eine Verknüpfung zu einem Dokument im Internet einsehbar. Zusätzlich kann man bei allen Anbietern die Datenschutztexte auch über eine Verknüpfung aus der Software heraus abrufen. Die Anbieter Xiaomi, Fitbit, Huawei, Amazon und Google stellen ihre Datenschutztexte im Play Store nur in englischer Sprache bereit. Lediglich bei Samsung und bei Apple sind diese Texte auf diesem Weg in deutscher Sprache verfügbar. Aus der Software heraus sind Datenschutztexte jedoch bei allen getesteten Anbietern in deutscher Sprache abrufbar. Rund 83 Prozent der Befragten der Studie des Autors gaben an, dass sie diese Texte nicht lesen. Als den Hauptgrund für das Nichtlesen der Texte gaben die meisten Nutzer zu lange Texte an. Auf die Frage wie lang der Datenschutztext maximal sein sollte, damit er gelesen wird, gab die Mehrzahl maximal zwei Seiten an. Wie man in der Tabelle sieht, sind Datenschutztexte aller Anbieter zu lang für das Empfinden der Verbraucher.

Tabelle 2: Länge der Datenschutztexte

Diensteanbieter	Länge des Datenschutztextes
Xiaomi / Huami	21
Fitbit	11
Huawei	15
Apple	8
Samsung	8
Amazon	7
Google	32

Quelle: Eigene Studie

Nach Artikel 12 Absatz 3 DSGVO kann der Betroffene auf Antrag Informationen über die gemäß den Artikeln 15 bis 22 ergriffenen Maßnahmen anfordern. Der Verantwortliche hat einen Monat Zeit darauf zu reagieren. Tabelle 3 zeigt die Antwortzeiten der Diensteanbieter auf Anfragen des Autors nach den im Artikel 15 DSGVO beschriebenen Informationen. Wie man sieht, hat ein Anbieter auf diese Anfrage gar nicht reagiert. Alle anderen haben die Frist zur Reaktion eingehalten.

Tabelle 3: Reaktionszeiten auf Anfragen nach Artikel 12 DSGVO

Anbieter	Anfragedatum	Anfrageweg	Antwortdatum
Xiaomi	25.03.2019	E-Mail	Keine Reaktion
Fitbit	27.03.2019	E-Mail	02.04.2019
Huawei	26.03.2019	E-Mail	27.03.2019
Apple	26.03.2019	E-Mail	29.03.2019
Samsung	25.03.2019	Webseitenformular	17.04.2019
Amazon	26.03.2019	Webseitenformular	10.04.2019
Google	27.03.2019	Webseitenformular	29.03.2019

Quelle: Eigene Studie

Alle Anbieter haben die Informationen nach Artikeln 13 bis 22 DSGVO unentgeltlich zur Verfügung gestellt.

4.3.2.5 Informationspflicht bei der Datenerhebung

Zum Zeitpunkt der Erhebung personenbezogener Daten hat der Verantwortliche dem Betroffenen die im Artikel 13 DSGVO aufgezählte Informationen mitzuteilen. Keiner der getesteten Anbieter teilt diese Daten dem Nutzer aktiv mit. Diese Informationen werden dem Nutzer in den Datenschutztexten bereitgestellt. Vor der Nutzung eines Dienstes hat der Nutzer die Möglichkeit Datenschutztexte nach diesen Informationen zu durchsuchen. In Folgendem werden Punkte aufgezählt, die der Autor weder in der Software noch in den Datenschutztexten der Diensteanbieter finden konnte.

Bei Xiaomi beziehungsweise dem Tochterunternehmen Huami konnte der Autor keine Information über das Beschwerderecht bei einer Aufsichtsbehörde finden. Bei Apple konnten keine Informationen zum Bestehen des Rechts auf Einschränkung der Verarbeitung, zum Recht auf einen Widerspruch und das Recht auf den Widerruf der Einwilligung gefunden werden. Bei Fitbit, Huawei und Google konnten keine Informationen zum Bestehen einer automatisierten Entscheidungsfindung einschließlich Profiling gefunden werden. Bei Google wurden auch keine Kontaktdaten des Datenschutzbeauftragten gefunden.

4.3.2.6 Rechte der Betroffenen

Nach Artikeln 15 bis 20 DSGVO hat der Betroffene ein Recht auf Auskunft über die Verarbeitung sowie auch das Recht auf Berichtigung, Löschung, Einschränkung und Übertragbarkeit seiner Daten. Nach Artikel 21 DSGVO hat er das Recht der Verarbeitung seiner Daten zu widersprechen.

Reaktionen der Diensteanbieter auf das Recht auf Auskunft über die Verarbeitung der Daten der Nutzer wurden bereits im Unterkapitel 4.3.2.5 beschrieben. Die Untersuchung, inwieweit der Nutzer sein Recht auf die Berichtigung seiner Daten wahrnehmen kann, ergab dass man bei allen getesteten Diensten seine Daten unverzüglich ändern kann. Das wichtigste Benutzerrecht ist laut der Umfragestudie des Autors das Recht auf die Löschung seiner Daten. Bei allen getesteten Wearable-Systemen kann der Nutzer seine Daten in der jeweiligen Smartphone-App löschen lassen. Bei den Sprachassistenz-Systemen von Amazon und Google können alle Sprachaufzeichnungen vom Nutzer gelöscht werden. Es können auch alle Daten des Nutzers durch das Löschen des Kundenkontos gelöscht werden. Auch das Recht auf die Datenübertragbarkeit kann der Nutzer bei allen Systemen ohne Probleme ausüben. Alle Dienste ermöglichen es den Nutzern ihre Daten in verschiedenen Formaten herunterzuladen. Bei Amazon Alexa kann der Nutzer seine aufgenommenen Sprachbefehle in Schriftform im CSV-Format und in Sprachform im MP3-Format herunterladen.

4.3.2.7 Datenschutz durch Technikgestaltung

Bei der Untersuchung der Technikgestaltung der Wearables wurde festgestellt, dass die Daten des Nutzers von jedem Gerät gelöscht werden können, indem man das jeweilige Gerät auf Werkseinstellungen zurücksetzt. Das Zurücksetzen ist bei allen Geräten, außer bei Fitbit, unkompliziert gestaltet. Das Zurücksetzen eines Fitbit-Fitnessarmbandes erfolgt mittels einer komplizierten Reihenfolge von Aktionen. Außerdem benötigt man dafür das dazugehörige USB-Kabel. Alle getesteten Wearable-Geräte verfügen über keine Möglichkeit das Aufzeichnen, Speichern oder Senden der Daten per Hardware-Taste zu unterbinden. Diese Einstellungen kann man jedoch teilweise in den dazugehörigen Smartphone-Apps vornehmen. Alle getesteten Geräte verfügen nur über die Sensoren, die für seine Funktion oder zur Erbringung des Dienstes benötigt werden. Alle getesteten Geräte lassen sich nach dem Koppeln mit einem Smartphone beziehungsweise Tablet für andere Geräte sperren, was unbefugte Verbindungen zum Wearable verhindert. Laut der Umfragestudie des Autors ist 57,94 Prozent der Befragten sehr wichtig bei einem datenerhebenden Gerät die Aufzeichnung der Daten jederzeit per Knopfdruck unterbrechen zu können. Diesem Wunsch der Verbraucher kommen Hersteller der Sprachassistenten entgegen. Wie schon im Unterkapitel 4.3.1 beschrieben, verfügen alle getesteten Sprachassistenzgeräte über eine Hardware-Taste, mit der man das Mithören der Geräte ausschalten kann. Um festzustellen, ob das Betätigen der Tasten zum Abschalten der Mikrofone, die Mikrofone tatsächlich abschaltet, wurden Datenströme zwischen den Sprachassistenten und dem Internet gemessen. Bei eingeschalteten Mikrofonen sind Sprachassistenten im Lauschmodus. Sie warten auf einen Befehl zum Aufzeichnen der Gespräche. Bei Amazon heißen diese Befehle Alexa oder Computer. Bei Google löst man die Aufzeichnung mit dem Befehl Okay Google aus. Aufgezeichnete Daten werden zur Verarbeitung an die Server der Diensteanbieter gesendet. Bei ausgeschalteten Mikrofonen sollten also keine Daten von Sprachassistenten zu dem mit dem Internet verbundenen Router fließen. Überprüfungen der Sprachassistenten von Google und Amazon bestätigten diese Theorie. Details zu dem Testverfahren, zu den Testwerkzeugen und zu den Ergebnissen des Tests sind in den Prüfprotokollen in der Anlage festgehalten.

4.3.2.8 Datenschutz durch datenschutzfreundliche Voreinstellungen

Bis auf einige wenige Ausnahmen sind die Voreinstellungen auf allen getesteten Geräten datenschutzfreundlich. Die Einwilligungshäkchen zur Erhebung der Daten sind bei den meisten Geräten als deaktiviert voreingestellt. Die Sichtbarkeit der Geräte wird nach dem Koppeln mit einem Smartphone oder Tablet automatisch auf unsichtbar für andere Geräte eingestellt. Bei einigen Geräten sind jedoch nicht alle Einstellungen datenschutzfreundlich voreingestellt. Im Unterkapitel 4.3.2.1 wurde schon erwähnt, dass vor dem Erstellen eines Mi-Benutzerkontos bei Xiaomi per Bestätigungshäkchen voraktiviert ist, dass man die Datenschutzbestimmungen gelesen hat und denen zustimmt. Bei Fitbit und Google sind optionale Zustimmungen für die Verarbeitung für weitere Zwecke wie für Werbung per Voreinstellung aktiviert. Bei dem Sprachassistenten Echo Show von Amazon ist beim Eingeben des WLAN-Passwortes und des Passwortes für das Amazon-Konto die Sichtbarkeit des Passwortest voreingestellt. Alle beschriebenen Voreinstellungen lassen sich vom Nutzer ändern.

4.3.2.9 Sicherheit der Verarbeitung

Welche technischen und organisatorischen Maßnahmen der Verantwortliche nach Artikel 32 DSGVO ergreift, um die Sicherheit der Verarbeitung zu gewährleisten, konnte nur eingeschränkt untersucht werden, da der Autor keinen Zugriff auf die IT-Infrastrukturen der Unternehmen hat. Es wurden Datenschutztexte nach diesbezüglichen Informationen der Anbieter durchsucht. Auch Geräte und die dazugehörige Software wurden auf Sicherheitseinstellungen untersucht. Laut den Datenschutztexten wird die Datenübertragung bei Xiaomi und Amazon mittels SSL[30] verschlüsselt. Amazon nutzt zusätzlich Verschlüsselungsmechanismen nach PCI-DSS[31]. Apple und Fitbit nutzen TSL[32] als Verschlüsselungsverfahren für die Datenübertragung. Der Zugang zum Dienst über Smartphone-Apps konnte bei jedem System mit Hilfe eines Passworts geschützt werden. Der direkte Zugang auf das Wearable ist bei Xiaomi, Fitbit, Huawei und Samsung jedoch nicht geschützt. Alle Wearables sind gegen das unbefugte Koppeln mit Geräten Dritter geschützt.

4.4 Auswertung

Es wurden 2 Anwendungsbereiche des Internets der Dinge näher untersucht. In einem Bereich werden mit biometrischen Daten und Gesundheitsdaten der Nutzer die sensibelsten personenbezogenen Daten erhoben. Beim anderen Bereich handelt es sich um den Bereich mit dem größten datenschutzrechtlichen Misstrauen der Verbraucher. In den beiden Bereichen wird der Markt im Jahr 2019 von einigen wenigen Herstellern für Anwendungssysteme dominiert. Die Hersteller mit einer geringen Marktabdeckung können somit vernachlässigt werden, ohne die Ergebnisse der Untersuchungen wesentlich zu

[30] SSL: Ein Verschlüsselungsprotokoll zur sicheren Datenübertragung
[31] PCI-DSS: Ein internationaler Sicherheitsstandard, um digitalen Datendiebstahl zu verhindern
[32] TSL: Weiterentwicklung des SSL-Protokolls

verzerren. Die Ergebnisse der Untersuchungen der marktbeherrschenden Systeme können damit als Ergebnisse für den gesamten jeweiligen Bereich angesehen werden.

Bei den Untersuchungen der Anwendungssysteme wurde festgestellt, dass die Hersteller sich überwiegend an die datenschutzrechtlichen Vorgaben halten. Jedoch gibt es noch einige Unstimmigkeiten. Vor allem ist die Aufklärung der Nutzer über die Erhebung und Verarbeitung ihrer personenbezogenen Daten bei allen Herstellern beziehungsweise Diensteanbietern noch mangelhaft. Die Datenschutztexte sind zu lang, teilweise schwer zu verstehen und zum Teil nur über Umwege abrufbar. Im Google Play Store sind bei den meisten Anbietern englischsprachige Datenschutzerklärungen verlinkt, was für einige Nutzer im deutschen Sprachraum nur schwer zu verstehen ist. Auf Anfragen bezüglich der Verarbeitung personenbezogener Daten haben fast alle Verarbeiter mit Standardantworten reagiert und darauf verwiesen, dass die Antworten auf die Fragen der Nutzer in den Datenschutztexten zu finden sind. Die Informationspolitik der Hersteller beziehungsweise der Diensteanbieter bezüglich des Datenschutzes ist nach Meinung des Autors nicht nutzerfreundlich. Bei der Ausübung anderer Nutzerrechte gab es jedoch keine Probleme. Hierbei verhalten sich die getesteten Anbieter vorbildlich. Der Datenschutz durch Technikgestaltung und datenschutzfreundliche Voreinstellungen wird bis auf einige Ausnahmen von den meisten getesteten Anbietern eingehalten. Besonders positiv aufgefallen ist die Möglichkeit Mikrofone der Sprachassistenten mit Hilfe von Hardware-Tasten jederzeit abschalten zu können. Messungen der Datenströme ergaben, dass diese Tasten tatsächlich wie von den Herstellern angegeben funktionieren.

5 ZUSAMMENFASSUNG UND SCHLUSSFOLGERUNG

Der Datenschutz hat für die deutsche Bevölkerung eine lange Tradition. Es war schon ein wichtiges Thema als es das Internet der Dinge noch gar nicht gab. Es ist eines der Gründe für die weite Entwicklung der Datenschutzgesetze in Deutschland. Das Internet der Dinge ist mit rund 20 Jahren ein noch junges Fachgebiet. Die Anfangsjahre des Internets der Dinge waren überwiegend von Ideen und Visionen bestimmt. Erst seit der flächendenkenden Verfügbarkeit des schnellen mobilen Internets, hat das Internet der Dinge an praktischer Bedeutung gewonnen. Auf Grund der noch jungen Geschichte des Internets der Dinge, ist die Technik in diesem Bereich noch nicht ausgereift. Es gibt kaum technische Standards und kaum allgemeingültige Definitionen. Man findet noch kaum gute Literatur zu diesem Thema. Dieser Umstand hat sich erschwerend auf die Bearbeitung des Kapitels zu den theoretischen Grundlagen ausgewirkt. Im Bereich der Datenschutzgesetze ist die Politik aktuell dabei diese auf die Erfordernisse in dem neuen Bereich des Internets einzustellen. Einige Verordnungen wie zum Beispiel die ePrivacy-Verordnung sind noch in der Entwicklung. Andere, wie die EU Datenschutz-Grundverordnung, wurden bereits auf neue Herausforderungen eingestellt. In den letzten Jahren gab es bereits einige Forschungen zum Thema Datenschutz in Bezug auf zum Internet der Dinge verwandten Themen. Da das Internet der Dinge im Jahr 2019 noch einer schnellen Entwicklung unterliegt, sind Forschungen zu diesem Thema schnell veraltet und nicht mehr anwendbar. Deshalb wurde der Stand der Wissenschaft in dieser Arbeit auf Grundlage von maximal 3 Jahre alten Studien und Ereignissen ermittelt. Die Forschung des Autors im Frühjahr 2019 zeigt, dass Hersteller und Diensteanbieter im Bereich des Internets der Dinge sich an die neuen Datenschutzbestimmungen anpassen. Ein gutes Beispiel dafür ist, dass im Gegensatz zu früheren Studien, die Forschung des Autors zeigt, dass mittlerweile alle getesteten Diensteanbieter vor der Erhebung der personenbezogenen Daten die Nutzer darauf hinweisen. Nicht geändert hat sich dagegen der Umstand, dass die Transparenz im Bezug der Erhebung von personenbezogenen Daten immer noch mangelhaft ist. Die Nutzer werden auch im Jahr 2019 nicht aktiv über die Verarbeitung ihrer Daten informiert. Informationen darüber müssen die Nutzer den Datenschutzerklärungen entnehmen, die zu lang und teilweise zu schwer zu verstehen sind. Auch bei direkten Fragen an die Verarbeiter wird man nur auf diese Datenschutztexte verwiesen. Der Autor ist zuversichtlich, dass auch in diesem Bereich in absehbarerer Zeit Verbesserungen eintreten werden. Diensteanbieter und Hersteller haben die Herausforderung, sich gleichzeitig auf die schnelle Entwicklung der Technologien und auf die noch junge EU Datenschutz-Grundverordnung einzustellen. Auch wenn die DSGVO nicht kritikfrei ist, spielt sie eine wichtige Vorreiterrolle für den internationalen Datenschutz. Auch nichteuropäische Hersteller müssen die Bestimmungen dieser Verordnung einhalten, wenn sie ihre Produkte für den europäischen Markt anbieten wollen. Somit prägt die DSGVO nicht nur Europa, sondern die ganze Welt. Es ist möglich, dass Hersteller aus Vereinfachungsgründen ihre für die Europäische Union angepasste Datenschutzeinstellungen auch für andere Märkte anwenden.

Die Ergebnisse dieser Arbeit beruhen auf den Forschungsergebnissen des Autors zum Thema Datenschutz im Internet der Dinge im Verbraucherbereich aus der zweiten Hälfte

des Jahres 2018 und aus der ersten Hälfte des Jahres 2019. Sowohl der Themenbereich des Internets der Dinge als auch der Themenbereich des Datenschutzes, würden den Umfang einer Diplomarbeit sprengen, wenn man versuchen würde die kompletten Bereiche lückenlos zu erforschen. Die Forschung dieser Arbeit musste sich deshalb auf die wichtigsten Bereiche konzentrieren und weniger bedeutsame Bereiche vernachlässigen. Somit wurden nicht alle Datenschutzgrundsätze einbezogen und nicht jedes existierende System innerhalb des Internets der Dinge untersucht. Bei der Untersuchung der Geräte musste sich der Autor an die Grenzen des Möglichen halten. Es konnte zum Beispiel nicht geprüft werden, welche Daten tatsächlich erhoben werden und wie die Daten tatsächlich verarbeitet werden. Bei diesen Punkten wird im Rahmen dieser Arbeit den Angaben der Anbieter vertraut. Es konnten auch die technischen und organisatorischen Maßnahmen der Anbieter und Hersteller innerhalb der Unternehmen nicht getestet werden, da man keinen Zugang dazu hat. Bei der Erforschung des Standes der Wissenschaft, konnten nicht alle existierenden Studien einbezogen werden. Deshalb konnte auch hier keine hundertprozentige Abdeckung des Forschungsstandes erreicht werden. Es können auch die für einen Menschen normalen Fehler bei der Forschung des Autors nicht ausgeschlossen werden. Unter Beachtung der Forschungsmöglichkeiten bietet diese Arbeit einen Forschungsstand für das Frühjahr 2019, von dem man verallgemeinernd auf den kompletten Bereich des Datenschutzes im Internet der Dinge im Verbraucherbereich schließen kann.

IV. LITERATURVERZEICHNIS

Adam, C. (2015). *CONNECTED CAR: DAS VERNETZTE AUTO*. Abgerufen am 25. 11 2018 von Heimnetzen.de: https://heimnetzen.de/blog/connected-car-das-vernetzte-auto/

Auto-ID Labs. (07. 11 2018). *Auto-ID Labs*. Abgerufen am 07. 11 2018 von Auto-ID Labs: https://autoidlabs.org/

Bauer, C. e. (2018). *E-Helth: Datenschutz und Datensicherheit.* Wiesbaden: Springer Gabler.

bvdw.org. (2019). *ePrivacy-Verordnung*. Abgerufen am 15. 02 2019 von bvdw.org: https://www.bvdw.org/themen/recht/kommunikationsrecht-eprivacy/

BVerfG. (15. 12 1983). *Volkszählungsurteil*. Abgerufen am 14. 02 2019 von openJur.de: https://openjur.de/u/268440.html

ConPolicy. (2018). *BIG DATA IM BEREICH HEIM UND FREIZEIT.* Abgerufen am 04. 03 2019 von abida ASSESSING BIG DATA: https://www.abida.de/sites/default/files/Gutachten_HeimUndFreizeit.pdf

datenschutz.org. (kein Datum). *ePrivacy-Verordnung: Die Ergänzung zur EU-Datenschutzverordnung*. Abgerufen am 16. 02 2019 von Datenschutz.org.

Datenschutzbehörden des Bundes und der Länder. (2018). Positionsbestimmung der Konferenz der unabhängigen Datenschutzbehörden des. *Zur Anwendbarkeit des TMG für nicht-öffentliche Stellen.* Düsseldorf. Abgerufen am 25. 02 2019 von file:///C:/Users/vik-t/OneDrive/Studium/_WINGS%20-%20WI/Aktuelle%20Module/Diplom/11%20Thema/Quellen/DSK-Positionsbestimmung_TMG,%202018%20(2019.02.25).pdf

datenschutzexperte.de. (kein Datum). *Anwendungsbereich des Telemediengesetzes*. Abgerufen am 18. 02 2019 von datenschutzexperte.de: https://www.datenschutzexperte.de/telemediengesetz-tmg/

datensicherheit.de. (05. 12 2016). *Gesundheits-Apps und Wearables: Datenschutz ungenügend*. Abgerufen am 27. 11 2018 von datensicherheit.de: https://www.datensicherheit.de/aktuelles/gesundheits-apps-und-wearables-datenschutz-ungenuegend-26249

Deloitte. (2017). *Automotive Data Treasure.* Abgerufen am 04. 03 2019 von deloitte.com: https://www2.deloitte.com/content/dam/Deloitte/de/Documents/risk/Risk-Advisory-Risk-Automotive-Data-Treasure-Frage-nach-dem-Datenschatz-2017.pdf

Dhanjani, N. (2015). *IoT-Hacking.* Heildelberg: dpunkt.verlag GmbH.

Die Bundesbeauftragte für den Datenschutz und die Informationsfreiheit. (o.J.). *BDSG und DSGVO - Garanten der informationellen Selbstbestimmung*. (Die Bundesbeauftragte für den Datenschutz und die Informationsfreiheit, Herausgeber) Von

https://www.bfdi.bund.de/DE/Datenschutz/Ueberblick/Was_ist_Datenschutz/Artikel/DasBundesdatenschutzgesetzSichertPers%C3%B6nlichkeitsrechte.html abgerufen

Duden. (23. 11 2018). *Duden*. Abgerufen am 23. 11 2018 von Duden: https://www.duden.de/rechtschreibung/Smarthome

Ehmann, E. (2016). *Datenschutz von A-Z.* Kissing: WEKA MEDIA GmbH & Co. KG.

Ehmann, E., & Kranig, T. (2017). *Erste Hilfe zur Datenschutz-Grundverordnung.* München: C.H. Beck oHG.

Elektronik Kompendium. (11. 11 2018). *LPWAN - Low Power Wide Area Network*. Abgerufen am 11. 11 2018 von Elektronik Kompendium: https://www.elektronik-kompendium.de/sites/kom/2207181.htm

elektronik-kompendium.de. (28. 11 2018). *M2M - Maschine-zu-Maschine-Kommunikation*. Abgerufen am 28. 11 2018 von Elektronik-Kompendium: https://www.elektronik-kompendium.de/sites/kom/1502061.htm

elektrosmoginfo.de. (21. 10 2008). *Funktionsweise des zellularen Mobilfunks*. Abgerufen am 29. 11 2018 von Elektrosmoginfo: http://www.ralf-woelfle.de/elektrosmog/redir.htm?http://www.ralf-woelfle.de/elektrosmog/technik/zell_mf.htm

EUR-Lex. (24. 11 2018). *Document 32015R0758*. Abgerufen am 24. 11 2018 von EUR-Lex: https://eur-lex.europa.eu/legal-content/DE/TXT/?uri=CELEX%3A32015R0758

Federal Trade Commision. (06. 02 2017). *VIZIO to Pay $2.2 Million to FTC.* Abgerufen am 2019.02.05 von FEDERAL TRADE COMMISSION: https://www.ftc.gov/news-events/press-releases/2017/02/vizio-pay-22-million-ftc-state-new-jersey-settle-charges-it

Fischer, D. (25. 04 2013). *Was ist ein Botnetz?* Abgerufen am 28. 11 2018 von kaspersky.de: https://www.kaspersky.de/blog/was-ist-ein-botnetz/981/

Fischer, T. (20. 07 2016). *Internet of Things-Buzzwords: Das bedeuten die Schlagwörter*. Abgerufen am 28. 11 2018 von ExpertenDerIT: https://www.expertenderit.de/blog/internet-of-things-buzzwords-das-bedeuten-die-schlagwoerter?hsCtaTracking=6d6f65d8-0d01-425c-8f98-e32d36d4f13c%7C1ec95a02-5646-43e0-87d2-51c2c320a19a

gdata.de. (2018). *G DATA-Security-Umfrage: Deutsche misstrauen Smart Home-Geräten.* Abgerufen am 01. 03 2019 von gdata.de: https://www.gdata.de/news/2018/09/31109-g-data-security-umfrage-deutsche-misstrauen-smart-home-geraten

Glenz, T. (15. 08 2017). *Der besondere Schutz der Beichte*. Abgerufen am 12. 02 2019 von katholisch.de: https://www.katholisch.de/aktuelles/aktuelle-artikel/der-besondere-schutz-der-beichte

GMX. (2018). *Sprachassistenten: Neue Herausforderung für Datenschutz.* Abgerufen am 01. 03 2019 von GMX Newsroom: https://newsroom.gmx.net/2018/07/19/sprachassistenten-neue-herausforderung-fuer-datenschutz/

Günter, M. (14. 11 2017). *Datenschutz und Datensicherheit für IoT-Produkte*. Abgerufen am 27. 11 2018 von Informatik Aktuell: https://www.informatik-aktuell.de/betrieb/netzwerke/datenschutz-und-datensicherheit-fuer-iot-produkte.html

Handelsblatt. (05. 07 2016). *Vernetzte Fernseher erobern die Haushalte*. Abgerufen am 20. 11 2018 von Handelsblatt: https://www.handelsblatt.com/technik/it-internet/smart-tvs-vernetzte-fernseher-erobern-die-haushalte/13832552.html

heise.de. (21. 09 2018). *Mirai: Die Entwickler des IoT-Botnetzes arbeiten jetzt für das FBI*. Abgerufen am 28. 11 2018 von heise online: https://www.heise.de/security/meldung/Mirai-Die-Entwickler-des-IoT-Botnetzes-arbeiten-jetzt-fuer-das-FBI-4169926.html

Helfrich, M. (2018). *Datenschutzrecht.* München: dtv Verlagsgesellschaft mbH & Co. KG.

Hippokrates. (ca. 400 v.Chr.). *Der Hippokratische Eid*. Abgerufen am 12. 02 2019 von aerztekammer-bw.de: https://www.aerztekammer-bw.de/10aerzte/40merkblaetter/20recht/10gesetze/hippoeid.pdf

Horvath, S. (17. 07 2012). *Aktueller Begriff: Internet der Dinge.* Abgerufen am 07. 11 2018 von Bundestag.de: https://www.bundestag.de/blob/192512/cfa9e76cdcf46f34a941298efa7e85c9/internet_der_dinge-data.pdf

Infotip Kompendium. (27. 02 2018). *Infotip Kompendium*. Abgerufen am 14. 11 2018 von IoT - INTERNET OF THINGS - Das Internet der Dinge: https://kompendium.infotip.de/IoT.html

ITWissen.info. (14. 11 2018). *ITWissen.info*. Abgerufen am 14. 11 2018 von Wissens-Portal ITwissen.info: https://www.itwissen.info/

kaspersky.de. (28. 11 2018). *Was sind DDoS-Angriffe?* Abgerufen am 28. 11 2018 von kaspersky.de: https://www.kaspersky.de/resource-center/threats/ddos-attacks

KUNBUS GmbH. (24. 11 2018). *KFZ Bussysteme, Protokolle und Standards 1*. Abgerufen am 24. 11 2018 von Kunbus: https://www.kunbus.de/kfz-bussysteme-protokolle-und-standards-1.html

Lackes, R., & Siepermann, M. (19. 02 2018). *Internet der Dinge*. Abgerufen am 11.07 2018 von Gabler Wirtschaftslexikon: https://wirtschaftslexikon.gabler.de/definition/internet-der-dinge-53187

Littmann, S. (13. 08 2015). *Bundesversicherungsamt sollte werbeträchtige Leistungen verbieten*. Abgerufen am 29. 11 2018 von wiwi.de:

https://www.wiwo.de/finanzen/vorsorge/einige-krankenkassen-foerdern-fitness-tracker-bundesversicherungsamt-sollte-werbetraechtige-leistungen-verbieten/12174652.html

Litzekl, N. (05. 12 2017). *Was ist ein Cyber-physisches System (CPS)?* Abgerufen am 28. 11 2018 von BigData Insider: https://www.bigdata-insider.de/was-ist-ein-cyber-physisches-system-cps-a-668494/

Litzel, N. (01. 09 2016). *Was ist das Internet of Things?* (Litzel, Nico) Abgerufen am 09. 11 2018 von BigData Insider: https://www.bigdata-insider.de/was-ist-das-internet-of-things-a-590806/

Loesche, D. (11. 12 2017). *Marktanteile der VoD-Anbieter in Deutschland*. Abgerufen am 20. 02 2019 von statista.de: https://de.statista.com/infografik/12214/marktanteile-der-vod-anbieter-in-deutschland/

Marktwächter.de. (25. 04 2017). *Wearables und Fitness-Apps: Daten außer Kontrolle*. Abgerufen am 03. 03 2019 von Marktwächter: https://www.marktwaechter.de/pressemeldung/wearables-und-fitness-apps-daten-ausser-kontrolle

menschenrechtskonvention.eu. (kein Datum). *Privatsphäre und Familienleben*. Abgerufen am 14. 02 2019 von menschenrechtskonvention.eu: https://www.menschenrechtskonvention.eu/privatsphaere-und-familienleben-9292/

Müller, S. (2016). *Internet of Things (IoT).* Norderstedt: Books on Demand.

nextMedia.Hamburg. (2018). *NEXTMEDIA.HAMBURG-STUDIE ZU VOICE-ASSISTENTEN.* Abgerufen am 01. 03 2019 von nextMedia.Hamburg: https://www.nextmedia-hamburg.de/nextmedia-hamburg-studie-zu-voice-assistenten/

NORDLIGHT research. (06. 05 2018). *VERBRAUCHERINTERESSE AN SMART-HOME-PRODUKTEN HOCH – KAUFBEREITSCHAFT UND NUTZUNG ABER NOCH GERING*. Abgerufen am 01. 03 2019 von NORDLIGHT research: https://www.nordlight-research.com/de/publikationen/presse/presse-detail/verbraucherinteresse-an-smart-home-produkten-hoch-kaufbereitschaft-und-nutzung-aber-noch-gering.html

o.V. (2018). *DSGVO.* Wrochaw: AmazonFulfillment.

Pipek, V. (26. 09 2014). *Ubiquitous Computing*. Abgerufen am 06. 11 2018 von Enzyklopedie der Wirtschaftsinformatik: http://www.enzyklopaedie-der-wirtschaftsinformatik.de/lexikon/technologien-methoden/Rechnernetz/Ubiquitous-Computing/index.html

ratgeberrecht.eu. (10. 06 2016). *„Smart-TV“ von Samsung: unzulässige AGB und Datenschutzerklärung*. Abgerufen am 04. 03 2019 von Anwaltskanzlei Weiß & Partner: https://www.ratgeberrecht.eu/internetrecht-aktuell/smart-tv-von-samsung-unzulaessige-agb-und-datenschutzerklaerung.html

Reinis, M. (2018). *Datenschutzgesetze 2018.* Norderstedt: Books on Demand.

Rummel, C. (10. 04 2018). *Das vernetzte Auto: Datenverarbeitung in Echtzeit*. Abgerufen am 25. 11 2018 von Industry Of Things: https://www.industry-of-things.de/das-vernetzte-auto-datenverarbeitung-in-echtzeit-a-686637/

Schmitz, P. (15. 01 2018). *Was ist eine Backdoor?* Abgerufen am 16. 02 2019 von security-insider.de: https://www.security-insider.de/was-ist-eine-backdoor-a-676126/

Schneider, J. (2018). *IT- und Computerrecht.* München: dtv Verlagsgesellschaft mbH & Co. KG.

Statista. (2018). *Prognose zur Anzahl der vernetzten Geräte im Internet der Dinge.* Abgerufen am 07. 11 2018 von Statista.

The Economist Intelligence Unit. (2018). *What the Internet of Thingsmeans for consumer privacy.* Abgerufen am 03. 03 2019 von forgerock: https://www.forgerock.com/resources/view/68775648/analyst-report/what-iot-means-for-consumer-privacy.pdf

ULD. (05. 12 2016). *Datenschutzaufsichtsbehörden prüften Wearables: Datenschutz-Mängel bei Fitness-Armbändern und Smart Watches*. Abgerufen am 03. 03 2019 von Unabhängiges Landeszentrum für Datenschutz Schleswig-Holstein: https://www.datenschutzzentrum.de/artikel/1070-Datenschutzaufsichtsbehoerden-prueften-Wearables-Datenschutz-Maengel-bei-Fitness-Armbaendern-und-Smart-Watches.html

verbraucherzentrale.nrw. (13. 06 2016). *Datenkrake im Smart-TV: Klage gegen Samsung*. Abgerufen am 04. 03 2019 von Verbraucherzentrale Nordrhein-Westfalen: https://www.verbraucherzentrale.nrw/aktuelle-meldungen/digitale-welt/fernsehen/datenkrake-im-smarttv-klage-gegen-samsung-12319

Weiser, M. (09 1991). *The Computer for the 21st Century.* Abgerufen am 06. 11 2018 von Donald Bren School of Information & Computer Sciences: https://www.ics.uci.edu/~corps/phaseii/Weiser-Computer21stCentury-SciAm.pdf

V. EHRENWÖRTLICHE ERKLÄRUNG

Ich erkläre hiermit ehrenwörtlich, dass ich die vorliegende Arbeit selbstständig angefertigt habe. Die aus fremden Quellen direkt oder indirekt übernommenen Gedanken sind als solche kenntlich gemacht. Es wurden keine anderen als die angegebenen Stellen und Hinweise verwandt.

Alle Quellen, die dem World Wide Web entnommen oder in einer sonstigen digitalen Form verwendet wurden, ohne allgemein zugänglich zu sein, sind der Arbeit als elektronische Kopie beigefügt. Der Durchführung einer elektronischen Plagiatsprüfung stimme ich hiermit zu. Die eingereichte Datei entspricht der eingereichten Druckfassung.

Die vorliegende Arbeit wurde bisher keiner anderen Prüfungsbehörde vorgelegt und auch noch nicht veröffentlicht.

Rostock, den 28.06.2019

VI. ANLAGENVERZEICHNIS

VII. ANLAGEN

Anlage 1 – Ergebnisse der Umfragestudie

Frage 1	Anzahl der Teilnehmer
Für welche der folgenden Anwendungsbereiche besitzen Sie bereits Geräte oder planen ein Gerät anzuschaffen?	108
Antworten	
49 (45.4 %): Wearables (z.B. Fitnessarmband oder Smartwatch) 74 (68.5%): Vernetzte Fernsehgeräte (z.B. Smart TV) 18 (16.7%): Sprachassistenten (z.B. Amazon Echo oder Google Home) 17 (15.7%): Smarthome (z.B. intelligente Lichtsteuerung oder Heizungsregelung) 10 (9.3%): Vernetztes Auto 20 (18.5%): Ich besitze keine smarten Geräte und plane es auch nicht	

Frage 2	Anzahl der Teilnehmer
Welche Arten der Wearables besitzen?	48
Antworten	
24 (50.0 %): Smartwatch 30 (62.5%): Fitnessarmband - (0 .0 %): Vernetzte Kleidung - (0 .0 %): Vernetzte Brille 2 (4 .2%): Andere	

Frage 3	Anzahl der Teilnehmer
Von welchem Hersteller sind ihre Wearables?	45
Antworten	
6 (13.3%): Xiaomi 10 (22.2%): Apple 13 (28.9%): Fitbit 3 (6.7%): Huawei 12 (26.7%): Samsung 12 (26.7%): Andere	

Frage 4	Anzahl der Teilnehmer
Von welchem Hersteller sind ihre Wearables?	45
Antworten	
6 (13.3%): Xiaomi 10 (22.2%): Apple 13 (28.9%): Fitbit 3 (6.7%): Huawei 12 (26.7%): Samsung 12 (26.7%): Andere	

Frage 5	Anzahl der Teilnehmer
Von welchem Hersteller ist Ihr vernetztes Fernsehgerät?	74
Antworten	
4 6 (62.2%): Samsung 14 (18.9%): LG 8 (10 .8%): Philips 4 (5.4 %): Panasonic 5 (6.8%): Sony 2 (2.7%): Andere	

Frage 6	Anzahl der Teilnehmer
Von welchem Hersteller und welches Modell ist Ihr vernetztes Auto?	8
Antworten	
Auto eigenes von Fiat VOLVO Hundei Tucson BMW 2er Gran Tourer ford Opel Insignia Business Innovation VW Renault	

Frage 7	Anzahl der Teilnehmer
Welche der folgenden Sprachassistenten besitzen Sie?	18
Antworten	
12 (66.7%): Amazon Echo (Alexa) 7 (38.9%): Google Home (Google Assistant) 1 (5.6%): Apple HomePod (Siri) 2 (11.1%): Andere	

Frage 8	Anzahl der Teilnehmer
Welche Art der Smarthome-Geräte besitzen Sie?	16
Antworten	
9 (56.3%): Sprachassistenten, Unterhaltungselektronik 11 (68.8%): Beleuchtungssteuerung 7 (4 3.8%): Steckdosen - (0 .0 %): Intelligente Stromzähler 2 (12.5%): Haushaltsgeräte 1 (6.3%): Andere	

Frage 9	Anzahl der Teilnehmer
Sind sie darüber besorgt, dass smarte Geräte mehr Daten erfassen könnten, als es Ihnen bewusst ist?	108
Antworten	
14 (13.0 %): Ja, ich bin sehr besorgt 26 (24 .1%): Ja, ich bin besorgt 47 (4 3.5%): Ich bin etwas besorgt 21 (19.4 %): Nein, ich bin gar nicht besorgt	

Frage 10	Anzahl der Teilnehmer
Beeinflusst die Sorge um Ihre persönlichen Daten Ihre Kaufentscheidung von smarten Geräten?	108
Antworten	
46 (4 2.6%): Ja 62 (57.4 %): Nein	

Frage 11	Anzahl der Teilnehmer
Beim Einsatz welcher Geräte hätten Sie die größten Sorgen, dass diese mehr Daten von Ihnen einsammeln, als Sie es wollen? Welchen Geräten misstrauen Sie am meisten?	107
Antworten	
4 (3.7%): Fitnessarmbänder oder Smartwatches 73 (68.2%): Sprachassistenten 5 (4 .7%): Fernseher - (0 .0 %): Auto 25 (23.4 %): Smarthome-Geräte	

Frage 12	Anzahl der Teilnehmer
Wer ist Ihrer Meinung nach für den Schutz der personenbezogenen Daten der Nutzer verantwortlich?	108
Antworten	
64 (59.3%): Der Gesetzgeber 72 (66.7%): Der Hersteller 4 2 (38.9%): Der Nutzer	

Frage 13	Anzahl der Teilnehmer
Es gibt Bestrebungen den Datenschutz international anzugleichen. Wie weit sollte der Datenschutz Ihrer Meinung nach gleich geregelt werden?	108
Antworten	
6 (5.6%): Deutschlandweit 31 (28.7%): Europaweit 71 (65.7%): Weltweit	

Frage 14	Anzahl der Teilnehmer
Seit dem 25. Mai 20 16 ist die EU Datenschutz-Grundverordnung in Kraft und seit dem 25. Mai 20 18 verbindlich. Was halten Sie von dieser Verordnung?	108
Antworten	
40 (37.0 %): Es ist gut, dass der Datenschutz EU-weit angeglichen wurde 34 (31.5%): Der Datenschutz wurde verbessert, reicht aber noch nicht 15 (13.9%): Diese Verordnung bringt keine Verbesserung des Datenschutzes 31 (28.7%): Diese Verordnung erschwert die Arbeit 12 (11.1%): Ich habe keine Meinung dazu 3 (2.8%): Andere	

Frage 15	Anzahl der Teilnehmer
Wie wichtig ist es für Sie, dass Sie vor der Benutzung eines Gerätes in einer klaren und einfachen Sprache darüber informiert werden, welche und zu welchem Zweck Daten von Ihnen erhoben werden?	108
Antworten	
50 (4 6.3%): Sehr wichtig 49 (4 5.4 %): Wichtig 9 (8.3%): Weniger wichtig - (0 .0 %): Unwichtig	

Frage 16	Anzahl der Teilnehmer
Lesen Sie vor der Nutzung eines Gerätes immer die Nutzungsbedingungen, bevor Sie diesen zustimmen?	108
Antworten	
18 (16.8%): Ja 89 (83.2%): Nein	

Frage 17	Anzahl der Teilnehmer
In welchen Fällen überspringen Sie das Lesen der Nutzungsbedingungen?	107
Antworten	
62 (57.9%): Wenn der Text zu lang ist 48 (4 4 .9%): Wenn der Text unverständlich ist 20 (18.7%): Wenn der Text nicht leicht zugänglich ist 27 (25.2%): Ich lese so etwas grundsätzlich nicht	

Frage 18	Anzahl der Teilnehmer
Ist es wichtig für Sie, dass die Datenschutzerklärung dem Gerät auch in Papierform vorliegt?	108
Antworten	
22 (20.4 %): Ja 86 (79.6%): Nein	

Frage 19	Anzahl der Teilnehmer
Wie lang sollten Nutzungsbedingungen bzw. die Datenschutzerklärung maximal sein, damit ich diese lesen würde?	79
Antworten	
2 Seiten; Eine Seite; Max 1 Seite; 2 Seiten. Schriftgröße 13 bis 16; 100 Wörter; 2 Seiten; Schwer zu sagen; Eine Seite; Eine Seite; Stichpunkthaltige Sätze max. 10; Genauso lange, dass die wichtigen Eckpunkte in verständlicher Form erklärt sind und ich erfahre, wo ich spezielle Feinheiten finde; Jede ausreichend lange Datenschutzerklärung ist zu lang; Eine halbe Seite; A5 Seite; 3 DIN A4 Seiten; 5 Zeilen; 1 Seite; 1-2 Seiten; A5 Seite; 2 Seiten; Lesezeit von etwa 3 Minuten; 2 Seiten; Nur die wichtigsten Sätze; Eine DIN-A4 Seite in Schriftgröße 8; Halbe Seite; Maximal eine halbe Seite; Bis zu zwei Seiten; 1 Seite; 1min Lesezeit; 10 Sätze; Wesentliche Aussagen sollten auf einer A4 -Seite Platz finden..; 2 Seiten; 5 Seiten; 3sätze; Lese ich sowieso nicht; Halbe A4 -Seite	

Frage 20	Anzahl der Teilnehmer
Wie wichtig ist es für Sie, dass smarte Geräte nur die Daten von Ihnen erfassen, deren Erfassung und Verarbeitung Sie ausdrücklich zugestimmt haben?	107
Antworten	
61 (57.0 %): Sehr wichtig 38 (35.5%): Wichtig 8 (7.5%): Weniger wichtig 1 (0 .9%): Unwichtig	

Frage 21	Anzahl der Teilnehmer
Wie wichtig ist es für Sie, dass nur die Daten von smarten Geräten erfasst werden, die für die Funktion des Gerätes benötigt werden?	107
Antworten	
54 (50 .5%): Sehr wichtig 44 (4 1.1%): Wichtig 9 (8.4 %): Weniger wichtig - (0 .0 %): Unwichtig	

Frage 22	Anzahl der Teilnehmer
Würden Sie Ihre personenbezogenen Daten freiwillig bereitstellen, wenn Sie im Gegenzug dafür eine Belohnung bekommen (z.B. Prämien oder Boni von Krankenkassen für die Preisgabe Ihrer Gesundheitsdaten)?	108
Antworten	
12 (11.1%): Ja 61 (56.5%): Nein 35 (32.4 %): Es kommt auf die Höhe der Belohnung an	

Frage 23	Anzahl der Teilnehmer
Welche der folgenden Benutzerrechte bezüglich der von Ihnen erhobenen Daten sind für Sie wichtig?	108
Antworten	
74 (68.5%): Recht auf Auskunft über die Verarbeitung Ihrer Daten 63 (58.3%): Recht auf Berichtigung Ihrer Daten 99 (91.7%): Recht auf Löschung Ihrer Daten 31 (28.7%): Recht auf Übertragbarkeit Ihrer Daten 1 (0.9%): Keines davon	

Frage 24	Anzahl der Teilnehmer
Welche dieser Rechte haben Sie schon einmal in Anspruch genommen?	108
Antworten	
22 (20 .4 %): Recht auf Auskunft 6 (5.6%): Recht auf Berichtigung 38 (35.2%): Recht auf Löschung 5 (4 .6%): Recht auf Übertragbarkeit 57 (52.8%): Noch keines davon	

Frage 25	Anzahl der Teilnehmer
Wie wichtig ist es Ihnen bei einem Gerät (z.B. bei einem Sprachassistenten), die Aufzeichnung Ihrer Daten jederzeit per Knopfdruck unterbrechen zu können?	107
Antworten	
62 (57.9%): Sehr wichtig 34 (31.8%): Wichtig 10 (9.3%): Weniger wichtig 1 (0 .9%): Unwichtig	

Frage 26	Anzahl der Teilnehmer
Nach der Datenschutz-Grundverordnung beträgt der Bußgeldrahmen für Datenschutzverstöße bis zu 20 Millionen Euro oder im Fall eines Unternehmens bis zu 4 % des gesamten weltweit erzielten Jahresumsatzes. Finden Sie diese Größenordnung angemessen?	107
Antworten	
74 (69.2%): Ja 12 (11.2%): Nein, sollte niedriger sein 21 (19.6%): Nein, sollte höher sein	

Anlage 2 – Prüfprotokolle

Prüfungsprotokoll - Xiaomi Dienste und Wearables

Allgemeine Beschreibung

- Überprüfung der Datenschutzprinzipien beim Dienst Mi Fit
- Benötigte Komponenten sind eine Client-App auf einem Android-Gerät und ein Wearable
- Die App Mi Fit wird am 22.03.2019 aus dem Google Store bezogen
- Die App wurde zu diesem Zeitpunkt über 10 Millionen Mal heruntergeladen und hat eine Durchschnittsbewertung von 3,6 von 5 Sternen.
- Entwickler der App ist Anhui Huami Information Technology
- HUAMI-Datenschutzrichtlinie ist vom 25.12.2018

Rechtmäßigkeit der Verarbeitung

Zu überprüfendes Datenschutzprinzip
Wird vor der Erhebung der Daten der Nutzer um eine Einwilligung zu der Verarbeitung der ihn betreffenden personenbezogenen Daten für einen oder mehrere Zwecke gefragt?
Rechtliche Grundlage
Artikel 6 Absatz 1 Buchstabe a) DSGVO
Ergebnis
Zum Nutzen des Dienstes ist Erstellung eines Benutzerkontos erforderlich. Vor der Erstellung hat man die Möglichkeit mittels eines Links zur HUAMI-Datenschutzrichtlinie zu gelangen. Man kann mit der Erstellung des Nutzerkontos nur dann fortfahren, wenn man der Datenschutzrichtlinie und damit der Verarbeitung seiner personenbezogenen Daten zustimmt. Das Bestätigungshäkchen ist per Voreinstellung bereits aktiviert. Bei einem bereits vorhandenem Benutzerkonto wird man beim ersten Starten der App darauf hingewiesen, dass personenbezogene Daten erhoben werden. Man kann nur mit Zustimmung fortfahren.

Zu überprüfendes Datenschutzprinzip
In welcher Form erfolgt die Einwilligung zur Verarbeitung der personenbezogenen Daten?
Rechtliche Grundlage
Artikel 6 Absatz 1 Buchstabe a) DSGVO
Ergebnis
Mittels eines Zustimmungshäkchens in der App.

Zu überprüfendes Datenschutzprinzip
Ist die Verarbeitung für die Erfüllung des Vertrages oder zur Durchführung vorvertraglicher Bedingungen erforderlich?
Rechtliche Grundlage
Artikel 6 Absatz 1 Buchstabe b) DSGVO
Ergebnis
Personenbezogene Daten werden gebraucht, um Dienstleistungen erfüllen zu können.

Bedingungen für die Einwilligung

Zu überprüfendes Datenschutzprinzip
Betrifft die Einwilligung noch andere Sachverhalte? Wenn Ja, erfolgt das Ersuchen um eine Einwilligung in einer verständlichen und leicht zugänglichen Form in einer klaren und einfachen Sprache und ist diese von anderen Sachverhalten klar zu unterscheiden?
Rechtliche Grundlage
Artikel 7 Absatz 2 DSGVO
Ergebnis
In der HUAMI-Datenschutzrichtlinie werden Sachverhalte erläutert für die Daten des Nutzers gebraucht werden. Man stimmt mit einem Zustimmungshaken allen Regelungen der Richtlinie zu. Es gibt kein separates Ersuchen um Einwilligung für weitere Daten. Die Datenschutzrichtlinie ist in deutscher Sprache.

Zu überprüfendes Datenschutzprinzip
Kann der Nutzer die Einwilligung jederzeit widerrufen? Wird die betroffene Person über die Möglichkeit eines Widerrufs vor der Abgabe der Einwilligung in Kenntnis gesetzt?
Rechtliche Grundlage
Artikel 7 Absatz 3 DSGVO
Ergebnis
Die Einwilligung kann durch das Aufrufen folgender Option in der Mi Fit App widerrufen werden: Profil > Einstellungen > Produktbeschreibung > Ausüben der Benutzerrechte > Autorisierung widerrufen – Widerruf der Zustimmung zur Softwarelizenz- und Servicevereinbarung und zur Datenschutzrichtlinie Die Einwilligung kann auch mittels einer Anfrage per E-Mail widerrufen werden. In der Datenschutzrichtlinie, die vor der Erteilung der Einwilligung eingesehen werden kann, wird auf die Möglichkeit des Widerrufs hingewiesen.

Zu überprüfendes Datenschutzprinzip
Ist der Widerruf der Einwilligung so einfach wie die Erteilung der Einwilligung?
Rechtliche Grundlage
Artikel 7 Absatz 3 DSGVO
Ergebnis
Der Widerruf in der App ist fast so einfach wie die Erteilung der Einwilligung.

Zu überprüfendes Datenschutzprinzip
Muss der Nutzer der Einwilligung der Verarbeitung personenbezogener Daten zustimmen, die für die Erfüllung des Vertrags nicht erforderlich ist?
Rechtliche Grundlage
Artikel 7 Absatz 4 DSGVO
Ergebnis
Man hat die Möglichkeit mittels des Android-Betriebssystems der App einzelne Berechtigungen zu entziehen. Nach Entzug der Berechtigungen funktioniert die App weiter, jedoch nicht mehr die Funktionen, die auf die Berechtigungen angewiesen sind.

Zu überprüfendes Datenschutzprinzip
Wird geprüft, ob der Nutzer mindestens 16 Jahre alt ist?
Rechtliche Grundlage
Artikel 8 DSGVO
Ergebnis
In der Datenschutzrichtlinie werden Regelungen des Artikels 8 DSGVO erläutert. Bei der Erstellung eines Benutzerkontos wird das Alter abgefragt. Bei einem Alter von unter 16 Jahren, wird zusätzlich eine Einwilligung eines Erziehungsberechtigten benötigt. In der App ist das Alter des Nutzers nur als 16 oder höher einstellbar.

Verarbeitung besonderer Kategorien personenbezogener Daten

Zu überprüfendes Datenschutzprinzip
Werden besondere Kategorien personenbezogener Daten Verarbeitet? Wenn ja, hängt diese Verarbeitung von einer expliziten Einwilligung des Nutzers ab? Erfolgt die Verarbeitung aus im Artikel 9 Absatz 2 Buchstaben b) bis j) beschriebenen Ausnahmegründen?
Rechtliche Grundlage
Artikel 9 DSGVO
Ergebnis
Es werden biometrische und Gesundheitsdaten des Nutzers verarbeitet. Es gibt keine explizite Einwilligung nur für diese Daten. Es wird vor dem Nutzen des Dienstes der Verarbeitung aller in der HUAMI-Datenschutzrichtline beschriebenen Daten zugestimmt.

Transparenz

Zu überprüfendes Datenschutzprinzip
Werden Informationen und Mitteilungen von Artikeln 13 bis 22 in präziser, transparenter, verständlicher und leicht zugänglicher Form in einer klaren und einfachen Sprache übermittelt?
Rechtliche Grundlage
Artikel 12 Absatz 1 DSGVO
Ergebnis
Im Google App Store ist unter dem Link zur Datenschutzerklärung ein Dokument mit Mi Fit Nutzungsbedingungen in englischer Sprache zu finden. Im hinteren Teil dieses Textes sind auch die Datenschutzbestimmungen in englischer Sprache zu finden. Dieser Text ist im Internet unter der Adresse http://cdn.awsbj0.fds.api.mi-img.com/mifit/1480831742.html zu finden. Eine Datenschutzrichtlinie in deutscher Sprache ist vor dem Nutzen der App über einen Link oder jederzeit in der App über den Weg Profil > Einstellungen > Produktbeschreibung > Datenschutz-Bestimmungen einsehbar. Die deutschsprachige Datenschutzrichtlinie ist in Schriftgröße 11 der Schriftart Arial 21 Seiten lang. Benutzerrechte, zu denen Datenberichtigung, Datenlöschung, Datenübertragbarkeit, Widerspruch der Einwilligung gehören, können ohne Umstand unverzüglich in der App ausgeübt werden.

Zu überprüfendes Datenschutzprinzip
Hat der Verantwortliche innerhalb eines Monats auf die Anfrage des Nutzers zu Artikeln 15 bis 22 reagiert?
Rechtliche Grundlage
Artikel 12 Absatz 3 und 4 DSGVO
Ergebnis
Keine Reaktion auf die Anfrage per E-Mail.

Zu überprüfendes Datenschutzprinzip
Werden Informationen nach Artikeln 13 bis 22 DSGVO unentgeltlich zur Verfügung gestellt?
Rechtliche Grundlage
Artikel 12 Absatz 5 DSGVO
Ergebnis
Laut Datenschutzrichtlinie wird die erste Anfrage unentgeltlich beantwortet. Für weitere Anfragen könnte Entgelt berechnet werden.

Informationspflicht bei der Erhebung personenbezogener Daten

Zu überprüfendes Datenschutzprinzip	
Teilt der Verantwortliche zum Zeitpunkt der Erhebung personenbezogener Daten des Nutzers folgende Daten mit?	
Rechtliche Grundlage	
Artikel 13 Absatz 1 und 2 DSGVO	
Ergebnis	
Namen und die Kontaktdaten des Verantwortlichen sowie gegebenenfalls seines Vertreters.	ja
Gegebenenfalls Kontaktdaten des Datenschutzbeauftragten.	ja
Zwecke, für die die personenbezogenen Daten verarbeitet werden sollen, sowie die Rechtsgrundlage für die Verarbeitung.	ja
Dauer, für die die personenbezogenen Daten gespeichert werden oder die Kriterien für die Festlegung dieser Dauer.	ja
Bestehen eines Rechts auf Auskunft.	ja
Bestehen eines Rechts auf Berichtigung.	ja
Bestehen eines Rechts auf Löschung.	ja
Bestehen eines Rechts auf Einschränkung der Verarbeitung.	ja
Bestehen eines Widerspruchsrechts gegen die Verarbeitung.	ja
Bestehen des Rechts auf Datenübertragbarkeit.	ja
Bestehen eines Rechts, die Einwilligung jederzeit zu widerrufen.	ja
Bestehen eines Beschwerderechts bei einer Aufsichtsbehörde	nein
Auskunft darüber, ob die Bereitstellung der personenbezogenen Daten gesetzlich oder vertraglich vorgeschrieben oder für einen Vertragsabschluss erforderlich ist.	ja
Auskunft darüber, ob die betroffene Person verpflichtet ist, die personenbezogenen Daten bereitzustellen, und welche möglichen Folgen die Nichtbereitstellung hätte.	ja
Bestehen einer automatisierten Entscheidungsfindung einschließlich Profiling und aussagekräftige Informationen dazu.	ja

Auskunftsrecht

Zu überprüfendes Datenschutzprinzip
Erteilt der Verantwortliche Auskunft über die verarbeiteten personenbezogenen Daten auf Anfrage des Nutzers? Wenn ja, stellt der Verarbeiter folgende Informationen zur Verfügung?
Rechtliche Grundlage
Artikel 15 Absatz 1
Ergebnis
Am 25.03.2019 wurde per E-Mail eine Anfrage an das Huami Privacy Team gestellt. Die E-Mail-Adresse lautet privacy@huami.com. Am29.04.2019 (über ein Monat Wartezeit nach Artikel 12 Absatz 3 DSGVO) wurde die Anfrage noch nicht beantwortet.

Recht auf Berichtigung

Zu überprüfendes Datenschutzprinzip
Werden personenbezogene Daten auf Anfrage berichtigt?
Rechtliche Grundlage
Artikel 16 DSGVO
Ergebnis
Nickname, Profilbild, Körpergröße, Körpergewicht, Geschlecht, Aktivitätsziel oder Gewichtsziel können direkt und unverzüglich vom Nutzer in der App geändert werden Änderung weiterer Daten kann per E-Mail angefragt werden. Die E-Mail ist an privacy@huami.com zu senden.

Recht auf Löschung

Zu überprüfendes Datenschutzprinzip
Werden personenbezogene Daten des Nutzers gelöscht, wenn der Nutzer die Einwilligung widerruft?
Rechtliche Grundlage
Artikel 17 Absatz 1 Buchstabe b)
Ergebnis
Personenbezogene Daten des Nutzers können durch das Aufrufen der entsprechenden Option in der Mi Fit App oder auf der Webseite https://mifit.huami.com/t/account_mifit gelöscht werden

Recht auf Datenübertragbarkeit

Zu überprüfendes Datenschutzprinzip
Werden Daten auf Anfrage dem Nutzer in einem strukturierten, gängigen und maschinenlesbaren Format zur Verfügung gestellt?
Rechtliche Grundlage
Artikel 20 DSGVO
Ergebnis
Personenbezogene Daten des Nutzers können durch das Aufrufen folgender Optionen in der Mi Fit App übertragen werden: Profil > Einstellungen > Produktbeschreibung > Ausüben der Benutzerrechte > Daten übertragen. Hier hat man die Möglichkeit die Daten direkt an ein anderes Konto zu übertragen oder herunterzuladen. Beides funktioniert unverzüglich.

Datenschutz durch Technikgestaltung und Voreinstellungen

Zu überprüfendes Datenschutzprinzip
Privacy By Design: Ist die Technik im Sinne der Datenschutzgrundsätze gestaltet?
Rechtliche Grundlage
Artikel 25 Absatz 1 DSGVO
Ergebnis
Das Löschen aller Daten vom Gerät ist durch das Zurücksetzen auf Werkseinstellungen durch den Nutzer jederzeit möglich. Das Wearable verfügt über keine Möglichkeit das Aufzeichnen, Speichern oder Senden der Daten zu unterbinden. Das Gerät enthält nur die Sensoren und andere Komponenten, die für seine Funktion oder zur Erbringung des Dienstes benötigt werden.

Zu überprüfendes Datenschutzprinzip
Privacy By Default: Sind die Voreinstellungen so eingestellt, dass nur die personenbezogenen Daten erhoben werden, deren Verarbeitung für den jeweiligen bestimmten Verarbeitungszweck erforderlich ist?
Rechtliche Grundlage
Artikel 25 Absatz 2 DSGVO
Ergebnis
Beim Erstellen eines Mi-Benutzerkontos ist das Bestätigungshäkchen, dass man die Datenschutzbestimmungen gelesen hat und denen zustimmt, voraktiviert. Die Sichtbarkeit des Wearables für weitere Geräte ist nach dem Anmelden automatisch deaktiviert.

Sicherheit der Verarbeitung

Zu überprüfendes Datenschutzprinzip
Ergreift der Verantwortliche unter Berücksichtigung der Verhältnismäßigkeit technische und organisatorische Maßnahmen, um Sicherheit der Verarbeitung zu gewährleisten?
Rechtliche Grundlage
Artikel 32 Absatz 1 DSGVO
Ergebnis
Laut der HUAMI-Datenschutzrichtlinie wird die Datenübertragung mit SSL und anderen Algorithmen verschlüsselt. Koppelung eines Smartphones oder Tablets erfolgt nur nach einer Bestätigung auf dem Wearable. In der App kann das Wearable für andere Geräte unsichtbar gemacht werden. Zugang zum Dienst ist passwortgeschützt, zum Wearable jedoch frei. In der App können Daten gewählt werden, die das Wearable erheben soll. Direkt auf dem Wearable besteht keine Möglichkeit Sensoren an oder auszuschalten.

Prüfungsprotokoll - Apple Dienste und Wearables

Allgemeine Beschreibung

- Überprüfung der Datenschutzprinzipien beim Dienst Apple Health
- Benötigte Komponenten sind eine Client-App auf einem Apple-Gerät und das Wearable Apple Watch
- Die App Apple Health ist auf den Apple Smartphones vorinstalliert
- Entwickler der App ist Apple Inc.
- Aktuelle Datenschutzrichtlinie ist vom 22.05.2018

Rechtmäßigkeit der Verarbeitung

Zu überprüfendes Datenschutzprinzip
Wird vor der Erhebung der Daten der Nutzer um eine Einwilligung zu der Verarbeitung der ihn betreffenden personenbezogenen Daten für einen oder mehrere Zwecke gefragt?
Rechtliche Grundlage
Artikel 6 Absatz 1 Buchstabe a) DSGVO
Ergebnis
Vor dem Anmelden Stimmt man den Nutzungsbedingungen zu. Datenerhebung für Werbezwecke oder für Verbesserung der Dienste kann man separat zustimmen.

Zu überprüfendes Datenschutzprinzip
In welcher Form erfolgt die Einwilligung zur Verarbeitung der personenbezogenen Daten?
Rechtliche Grundlage
Artikel 6 Absatz 1 Buchstabe a) DSGVO
Ergebnis
Mittels der Nutzung der App.

Zu überprüfendes Datenschutzprinzip
Ist die Verarbeitung für die Erfüllung des Vertrages oder zur Durchführung vorvertraglicher Bedingungen erforderlich?
Rechtliche Grundlage
Artikel 6 Absatz 1 Buchstabe b) DSGVO
Ergebnis
Personenbezogene Daten werden gebraucht, um Dienstleistungen erfüllen zu können.

Bedingungen für die Einwilligung

Zu überprüfendes Datenschutzprinzip
Betrifft die Einwilligung noch andere Sachverhalte? Wenn Ja, erfolgt das Ersuchen um eine Einwilligung in einer verständlichen und leicht zugänglichen Form in einer klaren und einfachen Sprache und ist diese von anderen Sachverhalten klar zu unterscheiden?
Rechtliche Grundlage
Artikel 7 Absatz 2 DSGVO
Ergebnis
Einwilligung für andere Sachverhalte ist optional. Das wird in der Apple-Datenschutzrichtlinie beschrieben. In den Einstellungen des iPhones kann man Datenberechtigungen an- und ausschalten.

Zu überprüfendes Datenschutzprinzip
Kann der Nutzer die Einwilligung jederzeit widerrufen? Wird die betroffene Person über die Möglichkeit eines Widerrufs vor der Abgabe der Einwilligung in Kenntnis gesetzt?
Rechtliche Grundlage
Artikel 7 Absatz 3 DSGVO
Ergebnis
Der Widerruf der Einwilligung ist durch das Löschen des Accounts realisierbar. Man wird nicht darüber informiert.

Zu überprüfendes Datenschutzprinzip
Ist der Widerruf der Einwilligung so einfach wie die Erteilung der Einwilligung?
Rechtliche Grundlage
Artikel 7 Absatz 3 DSGVO
Ergebnis
Nein, da es in der App keine Option zum einfachen Widerruf gibt.

Zu überprüfendes Datenschutzprinzip
Muss der Nutzer der Einwilligung der Verarbeitung personenbezogener Daten zustimmen, die für die Erfüllung des Vertrags nicht erforderlich ist?
Rechtliche Grundlage
Artikel 7 Absatz 4 DSGVO
Ergebnis
Nein. Der Nutzer kann zusätzlichen Verarbeitungen optional zustimmen.

Zu überprüfendes Datenschutzprinzip
Wird geprüft, ob der Nutzer mindestens 16 Jahre alt ist?
Rechtliche Grundlage
Artikel 8 DSGVO
Ergebnis
Beim Erstellen eines Benutzerkontos ist nur das Alter von 16 oder höher erlaubt. In der App und in der Account-Verwaltung im Internet https://appleid.apple.com/account/manage ist ebenfalls das Alter des Nutzers nur als 16 oder höher einstellbar.

Verarbeitung besonderer Kategorien personenbezogener Daten

Zu überprüfendes Datenschutzprinzip
Werden besondere Kategorien personenbezogener Daten Verarbeitet? Wenn ja, hängt diese Verarbeitung von einer expliziten Einwilligung des Nutzers ab? Erfolgt die Verarbeitung aus im Artikel 9 Absatz 2 Buchstaben b) bis j) beschriebenen Ausnahmegründen?
Rechtliche Grundlage
Artikel 9 DSGVO
Ergebnis
In der Apple Datenschutzrichtlinie werden diese Kategorien der personenbezogenen Daten nicht angesprochen.

Transparenz

Zu überprüfendes Datenschutzprinzip
Werden Informationen und Mitteilungen von Artikeln 13 bis 22 in präziser, transparenter, verständlicher und leicht zugänglicher Form in einer klaren und einfachen Sprache übermittelt?
Rechtliche Grundlage
Artikel 12 Absatz 1 DSGVO
Ergebnis
Die Apple Datenschutzrichtlinie ist unter der Webadresse https://www.apple.com/legal/privacy/de-ww zu finden. Die Datenschutzrichtlinie ist 8 Seiten lang. Sie ist in einer gut verständlichen Sprache geschrieben. Sie ist fachlich aber nicht einfach zu verstehen.

Zu überprüfendes Datenschutzprinzip
Hat der Verantwortliche innerhalb eines Monats auf die Anfrage des Nutzers zu Artikeln 15 bis 22 reagiert?
Rechtliche Grundlage
Artikel 12 Absatz 3 und 4 DSGVO
Ergebnis
Reaktion bereits am 29.03.2019. Jedoch wurde nur darauf hingewiesen, dass man die Informationen in den Datenschutztexten findet.

Zu überprüfendes Datenschutzprinzip
Werden Informationen nach Artikeln 13 bis 22 DSGVO unentgeltlich zur Verfügung gestellt?
Rechtliche Grundlage
Artikel 12 Absatz 5 DSGVO
Ergebnis
Informationen, die zur Verfügung gestellt wurden, wurden kostenlos gestellt.

Informationspflicht bei der Erhebung personenbezogener Daten

Zu überprüfendes Datenschutzprinzip	
Teilt der Verantwortliche zum Zeitpunkt der Erhebung personenbezogener Daten des Nutzers folgende Daten mit?	
Rechtliche Grundlage	
Artikel 13 Absatz 1 und 2 DSGVO	
Ergebnis	
Namen und die Kontaktdaten des Verantwortlichen sowie gegebenenfalls seines Vertreters.	ja
Gegebenenfalls Kontaktdaten des Datenschutzbeauftragten.	ja
Zwecke, für die die personenbezogenen Daten verarbeitet werden sollen, sowie die Rechtsgrundlage für die Verarbeitung.	ja
Dauer, für die die personenbezogenen Daten gespeichert werden oder die Kriterien für die Festlegung dieser Dauer.	ja
Bestehen eines Rechts auf Auskunft.	ja
Bestehen eines Rechts auf Berichtigung.	ja
Bestehen eines Rechts auf Löschung.	ja
Bestehen eines Rechts auf Einschränkung der Verarbeitung.	nein
Bestehen eines Widerspruchsrechts gegen die Verarbeitung.	nein
Bestehen des Rechts auf Datenübertragbarkeit.	ja
Bestehen eines Rechts, die Einwilligung jederzeit zu widerrufen.	nein
Bestehen eines Beschwerderechts bei einer Aufsichtsbehörde	ja
Auskunft darüber, ob die Bereitstellung der personenbezogenen Daten gesetzlich oder vertraglich vorgeschrieben oder für einen Vertragsabschluss erforderlich ist.	ja
Auskunft darüber, ob die betroffene Person verpflichtet ist, die personenbezogenen Daten bereitzustellen, und welche möglichen Folgen die Nichtbereitstellung hätte.	ja
Bestehen einer automatisierten Entscheidungsfindung einschließlich Profiling und aussagekräftige Informationen dazu.	ja

Auskunftsrecht

Zu überprüfendes Datenschutzprinzip
Erteilt der Verantwortliche Auskunft über die verarbeiteten personenbezogenen Daten auf Anfrage des Nutzers? Wenn ja, stellt der Verarbeiter folgende Informationen zur Verfügung?
Rechtliche Grundlage
Artikel 15 Absatz 1
Ergebnis
Die Anfrage wurde am 26.03.2019 über die https://www.apple.com/de/privacy/contact gestellt. Am 29.03.2019 wurde auf die Anfrage geantwortet. Die Antwort verweist darauf, dass die nötigen Informationen in den Datenschutztexten nachzulesen sind.

Recht auf Berichtigung

Zu überprüfendes Datenschutzprinzip
Werden personenbezogene Daten auf Anfrage berichtigt?
Rechtliche Grundlage
Artikel 16 DSGVO
Ergebnis
In der Health-App lassen sich Geburtstag, Geschlecht, Blutgruppe, Hauttyp vom Nutzer direkt verändern. Datenkorrektur kann auch auf der Webseite https://privacy.apple.com durchgeführt werden.

Recht auf Löschung

Zu überprüfendes Datenschutzprinzip
Werden personenbezogene Daten des Nutzers gelöscht, wenn der Nutzer die Einwilligung widerruft?
Rechtliche Grundlage
Artikel 17 Absatz 1 Buchstabe b)
Ergebnis
Der Nutzer hat die Möglichkeit alle seine Daten per Health-App oder auf der Webseite https://privacy.apple.com zu löschen.

Recht auf Datenübertragbarkeit

Zu überprüfendes Datenschutzprinzip
Werden Daten auf Anfrage dem Nutzer in einem strukturierten, gängigen und maschinenlesbaren Format zur Verfügung gestellt?
Rechtliche Grundlage
Artikel 20 DSGVO
Ergebnis
In der Health-App hat der Nutzer seine Daten zu exportieren. Im Internet können die Daten unter der Adresse https://privacy.apple.com in folgenden Formaten heruntergeladen werden: App-Nutzungs- und Aktivitätsdaten als Tabellenkalkulationen oder Dateien im JSON-, CSV-, XML- oder PDF-Format. Dokumente, Fotos und Videos in ihrem Originalformat. Kontakte, Kalender und Lesezeichen im VCF-, ICS- und HTML-Format.

Datenschutz durch Technikgestaltung und Voreinstellungen

Zu überprüfendes Datenschutzprinzip
Privacy By Design: Ist die Technik im Sinne der Datenschutzgrundsätze gestaltet?
Rechtliche Grundlage
Artikel 25 Absatz 1 DSGVO
Ergebnis
Für die Kopplung der Apple Watch mit dem iPhone wird vom iPhone eine Grafik auf dem Display der Watch abgelesen. Für die Zeit des Nichttragens der Watch ist ein Sperrcode einstellbar. Es ist auch einstellbar, dass nach 10 erfolglosen Versuchen den Sperrcode einzugeben, alle Daten gelöscht werden. Das Zurücksetzen der Apple Watch ist direkt auf der Watch und per Health-App möglich. Per App lässt sich der Herzfrequenzsensor abschalten.

Zu überprüfendes Datenschutzprinzip
Privacy By Default: Sind die Voreinstellungen so eingestellt, dass nur die personenbezogenen Daten erhoben werden, deren Verarbeitung für den jeweiligen bestimmten Verarbeitungszweck erforderlich ist?
Rechtliche Grundlage
Artikel 25 Absatz 2 DSGVO
Ergebnis
Voreinstellungen sind verhältnismäßig gesetzt.

Sicherheit der Verarbeitung

Zu überprüfendes Datenschutzprinzip
Ergreift der Verantwortliche unter Berücksichtigung der Verhältnismäßigkeit technische und organisatorische Maßnahmen, um Sicherheit der Verarbeitung zu gewährleisten?
Rechtliche Grundlage
Artikel 32 Absatz 1 DSGVO
Ergebnis
Daten auf dem iPhone werden verschlüsselt, sobald das Gerät gesperrt wird. Für Datenübertragung wird laut der Datenschutzrichtlinie Verschlüsselungsverfahren Transport Layer Security (TLS) angewendet.

Prüfungsprotokoll - Fitbit Dienste und Wearables

Allgemeine Beschreibung

- Überprüfung der Datenschutzprinzipien beim Fitness-Dienst Fitbit.
- Benötigte Komponenten sind die Client-App Fitbit auf einem Android-Gerät und ein Fitbit-Wearable.
- Die App Fitbit wird am 27.03.2019 aus dem Google Store bezogen.
- Die App wurde zu diesem Zeitpunkt über 10 Millionen Mal heruntergeladen und hat eine Durchschnittsbewertung von 3,9 von 5 Sternen.
- Entwickler der App ist Fitbit, Inc.
- Aktuelle Datenschutzrichtlinie ist vom 18.09.2018

Rechtmäßigkeit der Verarbeitung

Zu überprüfendes Datenschutzprinzip
Wird vor der Erhebung der Daten der Nutzer um eine Einwilligung zu der Verarbeitung der ihn betreffenden personenbezogenen Daten für einen oder mehrere Zwecke gefragt?
Rechtliche Grundlage
Artikel 6 Absatz 1 Buchstabe a) DSGVO
Ergebnis
Vor dem Anmelden muss man der Datenschutzerklärung sowie auch der Übertragung persönlicher Daten in die USA und andere Länder zustimmen. Ohne Zustimmung ist das Anmelden nicht möglich.

Zu überprüfendes Datenschutzprinzip
In welcher Form erfolgt die Einwilligung zur Verarbeitung der personenbezogenen Daten?
Rechtliche Grundlage
Artikel 6 Absatz 1 Buchstabe a) DSGVO
Ergebnis
Mittels der Zustimmungshäkchen für die Datenschutzrichtlinie und Übertragung der daten in die USA vor der Nutzung in der App.

Zu überprüfendes Datenschutzprinzip
Ist die Verarbeitung für die Erfüllung des Vertrages oder zur Durchführung vorvertraglicher Bedingungen erforderlich?
Rechtliche Grundlage
Artikel 6 Absatz 1 Buchstabe b) DSGVO
Ergebnis
Personenbezogene Daten werden gebraucht, um Dienstleistungen erfüllen zu können.

Bedingungen für die Einwilligung

Zu überprüfendes Datenschutzprinzip
Betrifft die Einwilligung noch andere Sachverhalte? Wenn Ja, erfolgt das Ersuchen um eine Einwilligung in einer verständlichen und leicht zugänglichen Form in einer klaren und einfachen Sprache und ist diese von anderen Sachverhalten klar zu unterscheiden?
Rechtliche Grundlage
Artikel 7 Absatz 2 DSGVO
Ergebnis
Nein. Der Verarbeitung der Daten für andere Sachverhalte kann separat zugestimmt werden.

Zu überprüfendes Datenschutzprinzip
Kann der Nutzer die Einwilligung jederzeit widerrufen? Wird die betroffene Person über die Möglichkeit eines Widerrufs vor der Abgabe der Einwilligung in Kenntnis gesetzt?
Rechtliche Grundlage
Artikel 7 Absatz 3 DSGVO
Ergebnis
Vor dem Anmelden wird der Nutzer darauf hingewiesen, dass man mit dem Löschen des Nutzerkontos die Einwilligung zur Datenverarbeitung widerruft. Das Löschen des Kontos ist jederzeit in der App oder auf der Webseite möglich.

Zu überprüfendes Datenschutzprinzip
Ist der Widerruf der Einwilligung so einfach wie die Erteilung der Einwilligung?
Rechtliche Grundlage
Artikel 7 Absatz 3 DSGVO
Ergebnis
Es wird darauf hingewiesen, dass man mit der Löschung des Kontos der Verarbeitung die Einwilligung widerruft.

Zu überprüfendes Datenschutzprinzip
Muss der Nutzer der Einwilligung der Verarbeitung personenbezogener Daten zustimmen, die für die Erfüllung des Vertrags nicht erforderlich ist?
Rechtliche Grundlage
Artikel 7 Absatz 4 DSGVO
Ergebnis
Nein. Der Nutzer kann vor dem Nutzen des Dienstes und auch später in der App selbst wählen, ob er einer zusätzlichen Verarbeitung seiner Daten zustimmt oder nicht.

Zu überprüfendes Datenschutzprinzip
Wird geprüft, ob der Nutzer mindestens 16 Jahre alt ist?
Rechtliche Grundlage
Artikel 8 DSGVO
Ergebnis
Beim Erstellen eines Benutzerkontos wird geprüft, ob das Alter unter 16 eingegeben wurde. In diesem Fall wird darauf hingewiesen, dass Kinder im Alter unter 16 nur mit einem Erziehungsberechtigten den Dienst nutzen können.

Verarbeitung besonderer Kategorien personenbezogener Daten

Zu überprüfendes Datenschutzprinzip
Werden besondere Kategorien personenbezogener Daten Verarbeitet? Wenn ja, hängt diese Verarbeitung von einer expliziten Einwilligung des Nutzers ab? Erfolgt die Verarbeitung aus im Artikel 9 Absatz 2 Buchstaben b) bis j) beschriebenen Ausnahmegründen?
Rechtliche Grundlage
Artikel 9 DSGVO
Ergebnis
Es werden biometrische und Gesundheitsdaten des Nutzers verarbeitet. Vor dem Nutzen des Dienstes wird darauf hingewiesen. Es wird explizit nach Einwilligung der Verarbeitung dieser Daten gefragt. Vor der Zustimmung werden diese Daten explizit erläutert.

Transparenz

Zu überprüfendes Datenschutzprinzip
Werden Informationen und Mitteilungen von Artikeln 13 bis 22 in präziser, transparenter, verständlicher und leicht zugänglicher Form in einer klaren und einfachen Sprache übermittelt?
Rechtliche Grundlage
Artikel 12 Absatz 1 DSGVO
Ergebnis
Im Google App Store ist unter dem Link zur Datenschutzerklärung die Fitbit Datenschutzrichtlinie in englischer Sprache vom 18. September 2018 abrufbar. Vor dem Einrichten eines Fitbit-Kontos hat man die Möglichkeit per Link eine Fitbit-Datenschutzrichtline in deutscher Sprache abzurufen. Diese ist ebenfalls vom 18 September 2018. Man kann sie auch jederzeit in der App aufrufen. Zusätzlich ist die Datenschutzrichtlinie auch im Internet unter der Adresse https://www.fitbit.com/de/legal/privacy-policy zu finden Die Datenschutzrichtlinie ist 11 Seiten lang. Sie ist in einer gut verständlichen Sprache geschrieben und ist gut strukturiert.

Zu überprüfendes Datenschutzprinzip
Hat der Verantwortliche innerhalb eines Monats auf die Anfrage des Nutzers zu Artikeln 15 bis 22 reagiert?
Rechtliche Grundlage
Artikel 12 Absatz 3 und 4 DSGVO
Ergebnis
Am 02.04.2019 wurde reagiert und darauf verwiesen, dass man die angefragten Informationen in der Datenschutzerklärung nachlesen kann.

Zu überprüfendes Datenschutzprinzip
Werden Informationen nach Artikeln 13 bis 22 DSGVO unentgeltlich zur Verfügung gestellt?
Rechtliche Grundlage
Artikel 12 Absatz 5 DSGVO
Ergebnis
Informationen, die zur Verfügung gestellt wurden, wurden kostenlos gestellt.

Informationspflicht bei der Erhebung personenbezogener Daten

Zu überprüfendes Datenschutzprinzip	
Teilt der Verantwortliche zum Zeitpunkt der Erhebung personenbezogener Daten des Nutzers folgende Daten mit?	
Rechtliche Grundlage	
Artikel 13 Absatz 1 und 2 DSGVO	
Ergebnis	
Namen und die Kontaktdaten des Verantwortlichen sowie gegebenenfalls seines Vertreters.	ja
Gegebenenfalls Kontaktdaten des Datenschutzbeauftragten.	ja
Zwecke, für die die personenbezogenen Daten verarbeitet werden sollen, sowie die Rechtsgrundlage für die Verarbeitung.	ja
Dauer, für die die personenbezogenen Daten gespeichert werden oder die Kriterien für die Festlegung dieser Dauer.	ja
Bestehen eines Rechts auf Auskunft.	ja
Bestehen eines Rechts auf Berichtigung.	ja
Bestehen eines Rechts auf Löschung.	ja
Bestehen eines Rechts auf Einschränkung der Verarbeitung.	ja
Bestehen eines Widerspruchsrechts gegen die Verarbeitung.	ja
Bestehen des Rechts auf Datenübertragbarkeit.	ja
Bestehen eines Rechts, die Einwilligung jederzeit zu widerrufen.	ja
Bestehen eines Beschwerderechts bei einer Aufsichtsbehörde	ja
Auskunft darüber, ob die Bereitstellung der personenbezogenen Daten gesetzlich oder vertraglich vorgeschrieben oder für einen Vertragsabschluss erforderlich ist.	ja
Auskunft darüber, ob die betroffene Person verpflichtet ist, die personenbezogenen Daten bereitzustellen, und welche möglichen Folgen die Nichtbereitstellung hätte.	ja
Bestehen einer automatisierten Entscheidungsfindung einschließlich Profiling und aussagekräftige Informationen dazu.	nein

Auskunftsrecht

Zu überprüfendes Datenschutzprinzip
Erteilt der Verantwortliche Auskunft über die verarbeiteten personenbezogenen Daten auf Anfrage des Nutzers? Wenn ja, stellt der Verarbeiter folgende Informationen zur Verfügung?
Rechtliche Grundlage
Artikel 15 Absatz 1
Ergebnis
Die Anfrage wurde am 27.03.2019 per E-Mail an das privacy@fitbit.com gestellt. Am 02.04.2019 wurde reagiert und darauf verwiesen, dass man die angefragten Informationen in der Datenschutzerklärung nachlesen kann.

Recht auf Berichtigung

Zu überprüfendes Datenschutzprinzip
Werden personenbezogene Daten auf Anfrage berichtigt?
Rechtliche Grundlage
Artikel 16 DSGVO
Ergebnis
Profilbild, Körpergröße, Körpergewicht, Geburtstag, Standort und Geschlecht können direkt und unverzüglich vom Nutzer in der App geändert werden. Änderung weiterer Daten kann auf der Webseite https://www.fitbit.com/settings/profile durchgeführt werden.

Recht auf Löschung

Zu überprüfendes Datenschutzprinzip
Werden personenbezogene Daten des Nutzers gelöscht, wenn der Nutzer die Einwilligung widerruft?
Rechtliche Grundlage
Artikel 17 Absatz 1 Buchstabe b)
Ergebnis
Personenbezogene Daten des Nutzers können durch das Aufrufen folgender Option in der Samsung Health App gelöscht werden: Konto > Daten verwalten > Konto löschen Das Löschen des Kontos ist auch auf der Webseite https://www.fitbit.com/settings/profile möglich.

Recht auf Datenübertragbarkeit

Zu überprüfendes Datenschutzprinzip
Werden Daten auf Anfrage dem Nutzer in einem strukturierten, gängigen und maschinenlesbaren Format zur Verfügung gestellt?
Rechtliche Grundlage
Artikel 20 DSGVO
Ergebnis
Auf der Webseite https://www.fitbit.com/settings/data/export können Daten im CSV-Format heruntergeladen werden.

Datenschutz durch Technikgestaltung und Voreinstellungen

Zu überprüfendes Datenschutzprinzip
Privacy By Design: Ist die Technik im Sinne der Datenschutzgrundsätze gestaltet?
Rechtliche Grundlage
Artikel 25 Absatz 1 DSGVO
Ergebnis
Beim Koppeln gibt der Nutzer eine auf dem Display des Wearables erschienene IPN ein. Damit wir unautorisiertes Koppeln unterbunden. IN der Fitbit-App gib es keine Möglichkeit das Fitness-Band zurück zu setzen. Das Zurücksetzen direkt am Band ist kompliziert. Man benötigt dafür das Ladekabel und einen USB-Port. Das Zurücksetzen erfolgt mittels einer komplizierter Reihenfolge der Aktionen mit dem Kabel und dem Drücken der Taste am Gerät. Nach dem Koppeln mit einem Gerät ist das Wearable für andere Geräte nicht mehr sichtbar und nicht koppelbar.

Zu überprüfendes Datenschutzprinzip
Privacy By Default: Sind die Voreinstellungen so eingestellt, dass nur die personenbezogenen Daten erhoben werden, deren Verarbeitung für den jeweiligen bestimmten Verarbeitungszweck erforderlich ist?
Rechtliche Grundlage
Artikel 25 Absatz 2 DSGVO
Ergebnis
Zustimmung für Nutzungsbedingungen und Datenschutzerklärung sowie für Übertragung persönlicher Daten in die USA sind per Voreinstellung deaktiviert. Die optionale Zustimmung für Werbung ist aber per Voreinstellung aktiviert.

Sicherheit der Verarbeitung

Zu überprüfendes Datenschutzprinzip
Ergreift der Verantwortliche unter Berücksichtigung der Verhältnismäßigkeit technische und organisatorische Maßnahmen, um Sicherheit der Verarbeitung zu gewährleisten?
Rechtliche Grundlage
Artikel 32 Absatz 1 DSGVO
Ergebnis
Zugang zum Dienst ist passwortgeschützt, zum Wearable jedoch frei. Das Wearable ist nur im Einrichtungsmodus für andere Geräte sichtbar. Nach einer Kopplung mit einem Gerät sind keine weiteren Kopplungen möglich. Laut der Datenschutzrichtlinie werden die Daten mittels TSL verschlüsselt.

Prüfungsprotokoll - Huawei Dienste und Wearables

Allgemeine Beschreibung

- Überprüfung der Datenschutzprinzipien beim Dienst Huawei Health
- Benötigte Komponenten sind die Wear OS by Google App, Huawei Wear App und die Huawei Helth App auf einem Android-Gerät und ein Huawei Wearable
- Die App Wear OS by Google wurde am 27.03.2019 aus dem Google Play Store bezogen. Diese App wurde zu dem Zeitpunkt über 10 Millionen Mal heruntergeladen und hat eine Bewertung von 3,9 von 5 Sternen. Entwickler der App ist Google LLC. Diese App wird benutzt, um das Betriebssystem auf dem Wearable einzurichten und das Google-Konto vom Smartphone auf das Wearable zu kopieren.
- Die App Huawei Wear wurde am 27.03.2019 aus dem Google Play Store bezogen. Diese App wurde zu dem Zeitpunkt über 5 Millionen Mal heruntergeladen und hat eine Bewertung von 3,6 von 5 Sternen. Entwickler der App ist Huawei Internet Service. Diese App wird benutzt, um spezifische Huawei Wear Einstellungen vorzunehmen.
- Die App Huawei Wear wurde am 27.03.2019 aus dem Google Play Store bezogen. Diese App wurde zu dem Zeitpunkt über 100 Millionen Mal heruntergeladen und hat eine Bewertung von 3,9 von 5 Sternen. Entwickler der App ist Huawei Internet Service. Diese App ist der Client für den Fitness-Service von Huawei.

Rechtmäßigkeit der Verarbeitung

Zu überprüfendes Datenschutzprinzip
Wird vor der Erhebung der Daten der Nutzer um eine Einwilligung zu der Verarbeitung der ihn betreffenden personenbezogenen Daten für einen oder mehrere Zwecke gefragt?
Rechtliche Grundlage
Artikel 6 Absatz 1 Buchstabe a) DSGVO
Ergebnis
Beim Starten der Huawei Wear App wird der Nutzer darauf hingewiesen, dass das Wearable personenbezogene Daten, mitunter auch Fitnessdaten erhebt. Per Link gelangt man zur Datenschutzrichtlinie. Man kann nur mit Zustimmung fortfahren. Auf dem Wearable muss man dem Endbenutzerlizenzvertrag zustimmen

Zu überprüfendes Datenschutzprinzip
In welcher Form erfolgt die Einwilligung zur Verarbeitung der personenbezogenen Daten?
Rechtliche Grundlage
Artikel 6 Absatz 1 Buchstabe a) DSGVO
Ergebnis
Mittels eines Weiter-Buttons, der gleichzeitig die Einwilligung zur Datenerhebung bedeutet.

Zu überprüfendes Datenschutzprinzip
Ist die Verarbeitung für die Erfüllung des Vertrages oder zur Durchführung vorvertraglicher Bedingungen erforderlich?
Rechtliche Grundlage
Artikel 6 Absatz 1 Buchstabe b) DSGVO
Ergebnis
Personenbezogene Daten, inklusive besonderer Kategorien personenbezogener Daten werden gebraucht, um Dienstleistungen erfüllen zu können.

Bedingungen für die Einwilligung

Zu überprüfendes Datenschutzprinzip
Betrifft die Einwilligung noch andere Sachverhalte? Wenn Ja, erfolgt das Ersuchen um eine Einwilligung in einer verständlichen und leicht zugänglichen Form in einer klaren und einfachen Sprache und ist diese von anderen Sachverhalten klar zu unterscheiden?
Rechtliche Grundlage
Artikel 7 Absatz 2 DSGVO
Ergebnis
Erhebung der Daten für weitere Sachverhalte kann man separat zustimmen • Beim Start Erhebung zur Verbesserung der Benutzerfreundlichkeit • Werbung per SMS, E-Mail, MMS und Push-Benachrichtigungen

Zu überprüfendes Datenschutzprinzip
Kann der Nutzer die Einwilligung jederzeit widerrufen? Wird die betroffene Person über die Möglichkeit eines Widerrufs vor der Abgabe der Einwilligung in Kenntnis gesetzt?
Rechtliche Grundlage
Artikel 7 Absatz 3 DSGVO
Ergebnis
Durch das Deinstallieren der Health-App beendet man die Datenerfassung.

Zu überprüfendes Datenschutzprinzip
Ist der Widerruf der Einwilligung so einfach wie die Erteilung der Einwilligung?
Rechtliche Grundlage
Artikel 7 Absatz 3 DSGVO
Ergebnis
Nein, da es in der App keine Option zum einfachen Widerruf gibt. Man kann das Konto aber löschen und damit die Einwilligung widerrufen.

Zu überprüfendes Datenschutzprinzip
Muss der Nutzer der Einwilligung der Verarbeitung personenbezogener Daten zustimmen, die für die Erfüllung des Vertrags nicht erforderlich ist?
Rechtliche Grundlage
Artikel 7 Absatz 4 DSGVO
Ergebnis
Nein. Der Nutzer kann vor dem Nutzen des Dienstes und auch später in der App selbst wählen, ob er einer zusätzlichen Verarbeitung seiner Daten zustimmt oder nicht.

Zu überprüfendes Datenschutzprinzip
Wird geprüft, ob der Nutzer mindestens 16 Jahre alt ist?
Rechtliche Grundlage
Artikel 8 DSGVO
Ergebnis
Man muss mindesten 16 Jahre alt sein, um eine Huawei ID erstellen zu können.

Verarbeitung besonderer Kategorien personenbezogener Daten

Zu überprüfendes Datenschutzprinzip
Werden besondere Kategorien personenbezogener Daten Verarbeitet? Wenn ja, hängt diese Verarbeitung von einer expliziten Einwilligung des Nutzers ab? Erfolgt die Verarbeitung aus im Artikel 9 Absatz 2 Buchstaben b) bis j) beschriebenen Ausnahmegründen?
Rechtliche Grundlage
Artikel 9 DSGVO
Ergebnis
Es werden Fitness- und Gesundheitsdaten des Nutzers verarbeitet. Vor dem Nutzen des Dienstes wird darauf hingewiesen. Es wird explizit nach Einwilligung der Verarbeitung dieser Daten gefragt. Vor der Zustimmung werden diese Daten in einem extra Feld explizit erläutert.

Transparenz

Zu überprüfendes Datenschutzprinzip
Werden Informationen und Mitteilungen von Artikeln 13 bis 22 in präziser, transparenter, verständlicher und leicht zugänglicher Form in einer klaren und einfachen Sprache übermittelt?
Rechtliche Grundlage
Artikel 12 Absatz 1 DSGVO
Ergebnis
Im Google App Store, unter dem Link zur Datenschutzerklärung, ist die Huawei Datenschutzrichtlinie in englischer Sprache hinterlegt. Beim Starten der Huawei Health App wird man darüber aufgeklärt, dass besondere Kategorien der personenbezogenen Daten erhoben werden und dass diese Daten auf Servern innerhalb der Europäischen Union verarbeitet werden. Mit dem Fortfahren willigt man diesem Vorgehen ein. Die Datenschutzrichtlinie ist auch in der Huawei Health App abrufbar. Zusätzlich ist die Datenschutzrichtlinie auch im Internet unter der Adresse https://consumer.huawei.com/de/legal/privacy-policy zu finden Die Datenschutzrichtlinie ist 15 Seiten lang. Sie ist in einer gut verständlichen Sprache geschrieben und ist gut strukturiert.

Zu überprüfendes Datenschutzprinzip
Hat der Verantwortliche innerhalb eines Monats auf die Anfrage des Nutzers zu Artikeln 15 bis 22 reagiert?
Rechtliche Grundlage
Artikel 12 Absatz 3 und 4 DSGVO
Ergebnis
Es wurde nach einem Tag reagiert. Jedoch nur in englischer Sprache und nur mit Verweisen auf andere Quellen.

Zu überprüfendes Datenschutzprinzip
Werden Informationen nach Artikeln 13 bis 22 DSGVO unentgeltlich zur Verfügung gestellt?
Rechtliche Grundlage
Artikel 12 Absatz 5 DSGVO
Ergebnis
Informationen, die zur Verfügung gestellt wurden, wurden kostenlos gestellt.

Informationspflicht bei der Erhebung personenbezogener Daten

Zu überprüfendes Datenschutzprinzip	
Teilt der Verantwortliche zum Zeitpunkt der Erhebung personenbezogener Daten des Nutzers folgende Daten mit?	
Rechtliche Grundlage	
Artikel 13 Absatz 1 und 2 DSGVO	
Ergebnis	
Namen und die Kontaktdaten des Verantwortlichen sowie gegebenenfalls seines Vertreters.	ja
Gegebenenfalls Kontaktdaten des Datenschutzbeauftragten.	ja
Zwecke, für die die personenbezogenen Daten verarbeitet werden sollen, sowie die Rechtsgrundlage für die Verarbeitung.	ja
Dauer, für die die personenbezogenen Daten gespeichert werden oder die Kriterien für die Festlegung dieser Dauer.	ja
Bestehen eines Rechts auf Auskunft.	ja
Bestehen eines Rechts auf Berichtigung.	ja
Bestehen eines Rechts auf Löschung.	ja
Bestehen eines Rechts auf Einschränkung der Verarbeitung.	ja
Bestehen eines Widerspruchsrechts gegen die Verarbeitung.	ja
Bestehen des Rechts auf Datenübertragbarkeit.	ja
Bestehen eines Rechts, die Einwilligung jederzeit zu widerrufen.	ja
Bestehen eines Beschwerderechts bei einer Aufsichtsbehörde	ja
Auskunft darüber, ob die Bereitstellung der personenbezogenen Daten gesetzlich oder vertraglich vorgeschrieben oder für einen Vertragsabschluss erforderlich ist.	ja
Auskunft darüber, ob die betroffene Person verpflichtet ist, die personenbezogenen Daten bereitzustellen, und welche möglichen Folgen die Nichtbereitstellung hätte.	ja
Bestehen einer automatisierten Entscheidungsfindung einschließlich Profiling und aussagekräftige Informationen dazu.	nein

Auskunftsrecht

Zu überprüfendes Datenschutzprinzip
Erteilt der Verantwortliche Auskunft über die verarbeiteten personenbezogenen Daten auf Anfrage des Nutzers? Wenn ja, stellt der Verarbeiter folgende Informationen zur Verfügung?
Rechtliche Grundlage
Artikel 15 Absatz 1
Ergebnis
Die Anfrage wurde am 26.03.2019 per E-Mail an das dpo@huawei.com gestellt. Am 27.03.2019 kam eine automatisch erstellte Bestätigungsmail in englischer Sprache. Man wird auf eine englischsprachige Kontaktseite verwiesen.

Recht auf Berichtigung

Zu überprüfendes Datenschutzprinzip
Werden personenbezogene Daten auf Anfrage berichtigt?
Rechtliche Grundlage
Artikel 16 DSGVO
Ergebnis
Profilbild, Körpergröße, Körpergewicht, Geburtstag und Geschlecht können direkt und unverzüglich vom Nutzer in der App geändert werden. Weiterer Daten können auf der Webseite https://hwid7.vmall.com/AMW/portal/userCenter/info.html geändert werden werden.

Recht auf Löschung

Zu überprüfendes Datenschutzprinzip
Werden personenbezogene Daten des Nutzers gelöscht, wenn der Nutzer die Einwilligung widerruft?
Rechtliche Grundlage
Artikel 17 Absatz 1 Buchstabe b)
Ergebnis
Personenbezogene Daten des Nutzers können durch das Aufrufen folgender Option in der Huawei Health App gelöscht werden: Nutzer > Einstellungen > Datenschutzeinstellungen > alle persönlichen Daten aus der Cloud löschen Im Account Center im Internet kann das Komplette Konto gelöscht werden.

Recht auf Datenübertragbarkeit

Zu überprüfendes Datenschutzprinzip
Werden Daten auf Anfrage dem Nutzer in einem strukturierten, gängigen und maschinenlesbaren Format zur Verfügung gestellt?
Rechtliche Grundlage
Artikel 20 DSGVO
Ergebnis
Personenbezogene Daten des Nutzers können in der Huawei Health App durch das Aufrufen der Option Kontoverwaltung > Einstellungen > Daten anfordern angefordert werden. Sie werden per E-Mail in einer verschlüsselten ZIP-Datei verschickt. Diese Anfrage kann der Nutzer auch im Account Center im Internet stellen.

Datenschutz durch Technikgestaltung und Voreinstellungen

Zu überprüfendes Datenschutzprinzip
Privacy By Design: Ist die Technik im Sinne der Datenschutzgrundsätze gestaltet?
Rechtliche Grundlage
Artikel 25 Absatz 1 DSGVO
Ergebnis
Das Löschen aller Daten vom Gerät ist durch das Zurücksetzen auf Werkseinstellungen in der Huawei Wear App und auf dem Wearable durch den Nutzer jederzeit möglich. Synchronisation mit der Cloud und das Senden der Diagnosedaten sind in der App abschaltbar. In der Health-App können folgende Datenflüsse an die Cloud an- und ausgeschaltet werden: • Persönliche Infos • Fitnessdaten • Gesundheitsdaten • Geräte- und App-Nutzungsdaten Das Gerät enthält nur die Sensoren und andere Komponenten, die für seine Funktion oder zur Erbringung des Dienstes benötigt werden. Nach dem Koppeln mit einem Gerät ist das Wearable für andere Geräte nicht mehr sichtbar. Kopplung kann nur vom Wearable gestartet werden.

Zu überprüfendes Datenschutzprinzip
Privacy By Default: Sind die Voreinstellungen so eingestellt, dass nur die personenbezogenen Daten erhoben werden, deren Verarbeitung für den jeweiligen bestimmten Verarbeitungszweck erforderlich ist?
Rechtliche Grundlage
Artikel 25 Absatz 2 DSGVO
Ergebnis
Für weitere optionale Erhebungen sind Zustimmungshäkchen deaktiviert. Das Senden der Diagnosedaten ist in der Wear OS App per Voreinstellung deaktiviert.

Sicherheit der Verarbeitung

Zu überprüfendes Datenschutzprinzip
Ergreift der Verantwortliche unter Berücksichtigung der Verhältnismäßigkeit technische und organisatorische Maßnahmen, um Sicherheit der Verarbeitung zu gewährleisten?
Rechtliche Grundlage
Artikel 32 Absatz 1 DSGVO
Ergebnis
Zugang zum Dienst ist passwortgeschützt, zum Wearable jedoch frei. Das Wearable ist nur im Einrichtungsmodus für andere Geräte sichtbar. Weitere Kopplungen müssen dem Wearable gestartet werden. Alle Verbindungsmöglichkeiten können im Betrieb einzeln aktiviert oder deaktiviert werden. Maßnahmen für Datensicherheit werden in der Datenschutzrichtlinie erläutert.

Prüfungsprotokoll -Samsung Health Dienste und Wearables

Allgemeine Beschreibung

- Überprüfung der Datenschutzprinzipien beim Dienst Samsung Health
- Benötigte Komponenten sind eine Client-App auf einem Android-Gerät und ein Wearable
- Die App Samsung Health wird am 24.03.2019 aus dem Google Store bezogen
- Die App wurde zu diesem Zeitpunkt über 500 Millionen Mal heruntergeladen und hat eine Durchschnittsbewertung von 4,3 von 5 Sternen.
- Entwickler der App ist Samsung Electronics Co., Ltd.
- Aktuelle Datenschutzrichtlinie ist vom 17.10.2018

Rechtmäßigkeit der Verarbeitung

Zu überprüfendes Datenschutzprinzip
Wird vor der Erhebung der Daten der Nutzer um eine Einwilligung zu der Verarbeitung der ihn betreffenden personenbezogenen Daten für einen oder mehrere Zwecke gefragt?
Rechtliche Grundlage
Artikel 6 Absatz 1 Buchstabe a) DSGVO
Ergebnis
Vor der Erstellung eines Nutzerkontos hat man die Möglichkeit mittels eines Links zur Samsung Health-Datenschutzrichtlinie zu gelangen. Beim ersten Anmelden in der App muss man den allgemeinen Geschäftsbedingungen zustimmen. Zustimmung zur Verarbeitung von Gesundheitsdaten ist optional. Man kann den Dienst auch ohne Zustimmung zur Verarbeitung der Gesundheitsdaten nutzen.

Zu überprüfendes Datenschutzprinzip
In welcher Form erfolgt die Einwilligung zur Verarbeitung der personenbezogenen Daten?
Rechtliche Grundlage
Artikel 6 Absatz 1 Buchstabe a) DSGVO
Ergebnis
Mittels eines Zustimmungshäkchens vor der Nutzung in der App.

Zu überprüfendes Datenschutzprinzip
Ist die Verarbeitung für die Erfüllung des Vertrages oder zur Durchführung vorvertraglicher Bedingungen erforderlich?
Rechtliche Grundlage
Artikel 6 Absatz 1 Buchstabe b) DSGVO
Ergebnis
Personenbezogene Daten werden gebraucht, um Dienstleistungen erfüllen zu können.

Bedingungen für die Einwilligung

Zu überprüfendes Datenschutzprinzip
Betrifft die Einwilligung noch andere Sachverhalte? Wenn Ja, erfolgt das Ersuchen um eine Einwilligung in einer verständlichen und leicht zugänglichen Form in einer klaren und einfachen Sprache und ist diese von anderen Sachverhalten klar zu unterscheiden?
Rechtliche Grundlage
Artikel 7 Absatz 2 DSGVO
Ergebnis
In der Samsung Health-Datenschutzrichtlinie werden Sachverhalte erläutert für die Daten des Nutzers gebraucht werden. Vor dem Nutzen des Dienstes kann man jedem Verwendungsbereich einzeln zustimmen. Dazu gehören: • Allgemeine Geschäftsbedingungen • Zustimmung zur Verarbeitung von Gesundheitsdaten (Optional) • Personalisierte Dienste (Optional) • Marketing Informationen (Optional)

Zu überprüfendes Datenschutzprinzip
Kann der Nutzer die Einwilligung jederzeit widerrufen? Wird die betroffene Person über die Möglichkeit eines Widerrufs vor der Abgabe der Einwilligung in Kenntnis gesetzt?
Rechtliche Grundlage
Artikel 7 Absatz 3 DSGVO
Ergebnis
In der Datenschutzrichtlinie wird darauf hingewiesen, dass der Betroffene der Verarbeitung widersprechen kann. Direkter Hinweis auf die Möglichkeit der Wiederrufs der Einwilligung wurde vom Autor nicht entdeckt.

Zu überprüfendes Datenschutzprinzip
Ist der Widerruf der Einwilligung so einfach wie die Erteilung der Einwilligung?
Rechtliche Grundlage
Artikel 7 Absatz 3 DSGVO
Ergebnis
Nein, da es in der App keine Option zum einfachen Widerruf gibt.

Zu überprüfendes Datenschutzprinzip
Muss der Nutzer der Einwilligung der Verarbeitung personenbezogener Daten zustimmen, die für die Erfüllung des Vertrags nicht erforderlich ist?
Rechtliche Grundlage
Artikel 7 Absatz 4 DSGVO
Ergebnis
Nein. Der Nutzer kann vor dem Nutzen des Dienstes und auch später in der App selbst wählen, ob er einer zusätzlichen Verarbeitung seiner Daten zustimmt oder nicht.

Zu überprüfendes Datenschutzprinzip
Wird geprüft, ob der Nutzer mindestens 16 Jahre alt ist?
Rechtliche Grundlage
Artikel 8 DSGVO
Ergebnis
Beim Erstellen eines Benutzerkontos ist nur das Alter von 16 oder höher erlaubt. In der App ist ebenfalls das Alter des Nutzers nur als 16 oder höher einstellbar.

Verarbeitung besonderer Kategorien personenbezogener Daten

Zu überprüfendes Datenschutzprinzip
Werden besondere Kategorien personenbezogener Daten Verarbeitet? Wenn ja, hängt diese Verarbeitung von einer expliziten Einwilligung des Nutzers ab? Erfolgt die Verarbeitung aus im Artikel 9 Absatz 2 Buchstaben b) bis j) beschriebenen Ausnahmegründen?
Rechtliche Grundlage
Artikel 9 DSGVO
Ergebnis
Es werden biometrische und Gesundheitsdaten des Nutzers verarbeitet. Vor dem Nutzen des Dienstes wird darauf hingewiesen. Es wird explizit nach Einwilligung der Verarbeitung dieser Daten gefragt. Vor der Zustimmung werden diese Daten in einem extra Feld explizit erläutert.

Transparenz

Zu überprüfendes Datenschutzprinzip
Werden Informationen und Mitteilungen von Artikeln 13 bis 22 in präziser, transparenter, verständlicher und leicht zugänglicher Form in einer klaren und einfachen Sprache übermittelt?
Rechtliche Grundlage
Artikel 12 Absatz 1 DSGVO
Ergebnis
Im Google App Store ist unter dem Link zur Datenschutzerklärung ein Dokument Samsung Health-Datenschutzrichtlinie in deutscher Sprache zu finden. Die Datenschutzrichtlinie ist vor dem Nutzen der App über einen Link oder jederzeit in der App über den Weg Einstellungen > Info zu Samsung Health > Datenschutzrichtlinie einsehbar. Die Datenschutzrichtlinie ist 8 Seiten lang. Sie ist in einer gut verständlichen Sprache geschrieben und ist gut strukturiert.

Zu überprüfendes Datenschutzprinzip
Hat der Verantwortliche innerhalb eines Monats auf die Anfrage des Nutzers zu Artikeln 15 bis 22 reagiert?
Rechtliche Grundlage
Artikel 12 Absatz 3 und 4 DSGVO
Ergebnis
Die Anfrage wurde am 25.03.2019 über die Webseite www.samsung.com/request-desk an das Samsung Data Protection Team gestellt. Am 17.04.2019 wurde die Anfrage beantwortet, dass keine personenbezogenen Daten vom Anfragesteller bearbeitet werden. Der Account war zu dem Zeitpunkt bereits gelöscht.

Zu überprüfendes Datenschutzprinzip
Werden Informationen nach Artikeln 13 bis 22 DSGVO unentgeltlich zur Verfügung gestellt?
Rechtliche Grundlage
Artikel 12 Absatz 5 DSGVO
Ergebnis
Laut Datenschutzrichtlinie wird die erste Anfrage unentgeltlich beantwortet. Weitere Anfragen können abgelehnt werden.

Informationspflicht bei der Erhebung personenbezogener Daten

Zu überprüfendes Datenschutzprinzip	
Teilt der Verantwortliche zum Zeitpunkt der Erhebung personenbezogener Daten des Nutzers folgende Daten mit?	
Rechtliche Grundlage	
Artikel 13 Absatz 1 und 2 DSGVO	
Ergebnis	
Namen und die Kontaktdaten des Verantwortlichen sowie gegebenenfalls seines Vertreters.	ja
Gegebenenfalls Kontaktdaten des Datenschutzbeauftragten.	ja
Zwecke, für die die personenbezogenen Daten verarbeitet werden sollen, sowie die Rechtsgrundlage für die Verarbeitung.	ja
Dauer, für die die personenbezogenen Daten gespeichert werden oder die Kriterien für die Festlegung dieser Dauer.	ja
Bestehen eines Rechts auf Auskunft.	ja
Bestehen eines Rechts auf Berichtigung.	ja
Bestehen eines Rechts auf Löschung.	ja
Bestehen eines Rechts auf Einschränkung der Verarbeitung.	ja
Bestehen eines Widerspruchsrechts gegen die Verarbeitung.	ja
Bestehen des Rechts auf Datenübertragbarkeit.	ja
Bestehen eines Rechts, die Einwilligung jederzeit zu widerrufen.	nein
Bestehen eines Beschwerderechts bei einer Aufsichtsbehörde	ja
Auskunft darüber, ob die Bereitstellung der personenbezogenen Daten gesetzlich oder vertraglich vorgeschrieben oder für einen Vertragsabschluss erforderlich ist.	ja
Auskunft darüber, ob die betroffene Person verpflichtet ist, die personenbezogenen Daten bereitzustellen, und welche möglichen Folgen die Nichtbereitstellung hätte.	ja
Bestehen einer automatisierten Entscheidungsfindung einschließlich Profiling und aussagekräftige Informationen dazu.	ja

Auskunftsrecht

Zu überprüfendes Datenschutzprinzip
Erteilt der Verantwortliche Auskunft über die verarbeiteten personenbezogenen Daten auf Anfrage des Nutzers? Wenn ja, stellt der Verarbeiter folgende Informationen zur Verfügung?
Rechtliche Grundlage
Artikel 15 Absatz 1
Ergebnis
Antwort auf die Anfrage am 17.04.2019 mit der Benachrichtigung, dass keine personenbezogenen Daten des Antragstellers bearbeitet werden. Zusätzlich kam am 17.04.2019 eine E-Mail mit Informationen, wie im Allgemeinen personenbezogenen Daten bei Samsung bearbeitet werden.

Recht auf Berichtigung

Zu überprüfendes Datenschutzprinzip
Werden personenbezogene Daten auf Anfrage berichtigt?
Rechtliche Grundlage
Artikel 16 DSGVO
Ergebnis
Profilbild, Körpergröße, Körpergewicht und Geschlecht können direkt und unverzüglich vom Nutzer in der App geändert werden. Änderung weiterer Daten kann über die Webseite www.samsung.com/request-desk angefragt werden.

Recht auf Löschung

Zu überprüfendes Datenschutzprinzip
Werden personenbezogene Daten des Nutzers gelöscht, wenn der Nutzer die Einwilligung widerruft?
Rechtliche Grundlage
Artikel 17 Absatz 1 Buchstabe b)
Ergebnis
Personenbezogene Daten des Nutzers können durch das Aufrufen folgender Option in der Samsung Health App gelöscht werden: Einstellungen > Persönliche Daten löschen

Recht auf Datenübertragbarkeit

Zu überprüfendes Datenschutzprinzip
Werden Daten auf Anfrage dem Nutzer in einem strukturierten, gängigen und maschinenlesbaren Format zur Verfügung gestellt?
Rechtliche Grundlage
Artikel 20 DSGVO
Ergebnis
Personenbezogene Daten des Nutzers können in der Samsung Health App durch das Aufrufen der Option Einstellungen > Persönliche Date herunterladen im CSV-Format auf das Smartphone heruntergeladen werden.

Datenschutz durch Technikgestaltung und Voreinstellungen

Zu überprüfendes Datenschutzprinzip
Privacy By Design: Ist die Technik im Sinne der Datenschutzgrundsätze gestaltet?
Rechtliche Grundlage
Artikel 25 Absatz 1 DSGVO
Ergebnis
Das Löschen aller Daten vom Gerät ist durch das Zurücksetzen auf Werkseinstellungen durch den Nutzer jederzeit möglich. Das Wearable verfügt über keine Möglichkeit das Aufzeichnen, Speichern oder Senden der Daten zu unterbinden. Das Gerät enthält nur die Sensoren und andere Komponenten, die für seine Funktion oder zur Erbringung des Dienstes benötigt werden. Nach dem Koppeln mit einem Gerät ist das Wearable für andere Geräte nicht mehr sichtbar und nicht koppelbar.

Zu überprüfendes Datenschutzprinzip
Privacy By Default: Sind die Voreinstellungen so eingestellt, dass nur die personenbezogenen Daten erhoben werden, deren Verarbeitung für den jeweiligen bestimmten Verarbeitungszweck erforderlich ist?
Rechtliche Grundlage
Artikel 25 Absatz 2 DSGVO
Ergebnis
Für alle Zustimmungsoptionen sind die Häkchen per Voreinstellung deaktiviert.

Sicherheit der Verarbeitung

Zu überprüfendes Datenschutzprinzip
Ergreift der Verantwortliche unter Berücksichtigung der Verhältnismäßigkeit technische und organisatorische Maßnahmen, um Sicherheit der Verarbeitung zu gewährleisten?
Rechtliche Grundlage
Artikel 32 Absatz 1 DSGVO
Ergebnis
Zugang zum Dienst ist passwortgeschützt, zum Wearable jedoch frei. Das Wearable ist nur im Einrichtungsmodus für andere Geräte sichtbar. Nach einer Kopplung mit einem Gerät sind keine weiteren Kopplungen möglich. Alle Verbindungsmöglichkeiten können im Betrieb einzeln aktiviert oder deaktiviert werden.

Prüfungsprotokoll - Amazon Alexa Dienste und Wearables

Allgemeine Beschreibung

- Überprüfung der Datenschutzprinzipien beim Dienst Amazon Alexa
- Benötigte Komponenten sind eine Client-App auf einem Android-Gerät und ein Amazon Echo-Gerät.
- Die App Amazon Alexa wird am 25.03.2019 aus dem Google Store bezogen.
- Die App wurde zu diesem Zeitpunkt über 10 Millionen Mal heruntergeladen und hat eine Durchschnittsbewertung von 3,4 von 5 Sternen.
- Entwickler der App ist Amazon Mobile LLC.
- Die im Google App Store hinterlegte Datenschutzerklärung ist vom 29.August 2017 und in englischer Sprache

Rechtmäßigkeit der Verarbeitung

Zu überprüfendes Datenschutzprinzip
Wird vor der Erhebung der Daten der Nutzer um eine Einwilligung zu der Verarbeitung der ihn betreffenden personenbezogenen Daten für einen oder mehrere Zwecke gefragt?
Rechtliche Grundlage
Artikel 6 Absatz 1 Buchstabe a) DSGVO
Ergebnis
Beim Erstellen eines Amazon-Nutzerkontos muss man den Nutzungsbedingungen zustimmen. Ohne Zustimmung kann man mit der Registrierung nicht fortfahren. Zu der Amazon Datenschutzerklärung gelangt man über den Link zu den Nutzerbedingungen, von da auf eine weitere Seite, die auf die Datenschutzerklärung verweist und von da weiter zu der Amazon.de-Datenschutzerklärung.

Zu überprüfendes Datenschutzprinzip
In welcher Form erfolgt die Einwilligung zur Verarbeitung der personenbezogenen Daten?
Rechtliche Grundlage
Artikel 6 Absatz 1 Buchstabe a) DSGVO
Ergebnis
Mittels einer Meldung beim Erstellen des Nutzerkontos, dass man mit dem Fortfahren, den Nutzungsbedingungen zustimmt.

Zu überprüfendes Datenschutzprinzip
Ist die Verarbeitung für die Erfüllung des Vertrages oder zur Durchführung vorvertraglicher Bedingungen erforderlich?
Rechtliche Grundlage
Artikel 6 Absatz 1 Buchstabe b) DSGVO
Ergebnis
Personenbezogene Daten werden benötigt, um Dienstleistungen erfüllen zu können.

Bedingungen für die Einwilligung

Zu überprüfendes Datenschutzprinzip
Betrifft die Einwilligung noch andere Sachverhalte? Wenn Ja, erfolgt das Ersuchen um eine Einwilligung in einer verständlichen und leicht zugänglichen Form in einer klaren und einfachen Sprache und ist diese von anderen Sachverhalten klar zu unterscheiden?
Rechtliche Grundlage
Artikel 7 Absatz 2 DSGVO
Ergebnis
Es wird eine Einwilligung für die Verarbeitung aller Daten eingeholt. Das Ersuchen zum Zugriff auf Kontakte erfolgt separat. Diesen kann man ablehnen, ohne dass der Dienst verweigert wird. Interessenbezogene Werbung kann unter der Adresse https://www.amazon.de/adprefs separat ein- und ausgeschaltet werden.

Zu überprüfendes Datenschutzprinzip
Kann der Nutzer die Einwilligung jederzeit widerrufen? Wird die betroffene Person über die Möglichkeit eines Widerrufs vor der Abgabe der Einwilligung in Kenntnis gesetzt?
Rechtliche Grundlage
Artikel 7 Absatz 3 DSGVO
Ergebnis
Der Nutzer wird nur darüber informiert, dass er seine Einwilligung widerrufen kann, wenn er die Einwilligung für bestimmte Zwecke abgegeben hat.

Zu überprüfendes Datenschutzprinzip
Ist der Widerruf der Einwilligung so einfach wie die Erteilung der Einwilligung?
Rechtliche Grundlage
Artikel 7 Absatz 3 DSGVO
Ergebnis
Nein, da es weder in der App noch auf der Webseite eine Option zum einfachen Widerruf gibt.

Zu überprüfendes Datenschutzprinzip
Muss der Nutzer der Einwilligung der Verarbeitung personenbezogener Daten zustimmen, die für die Erfüllung des Vertrags nicht erforderlich ist?
Rechtliche Grundlage
Artikel 7 Absatz 4 DSGVO
Ergebnis
Der Nutzer muss der Verarbeitung aller Daten zustimmen, um den Dienst Nutzen zu können. Welche Daten für das Erbringen der Dienstleistung erforderlich sind, ist unklar. Beim Hinzufügen von einem Echo-Gerät muss man den Zugriff auf Standortdaten erlauben, sonst kann man mit der Einrichtung nicht fortfahren.

Zu überprüfendes Datenschutzprinzip
Wird geprüft, ob der Nutzer mindestens 16 Jahre alt ist?
Rechtliche Grundlage
Artikel 8 DSGVO
Ergebnis
Alle Amazon Services sind nur für Erwachsene ab 18 Jahre. Minderjährige können dienste nur über Erziehungsberechtigte nutzen. Beim Anmelden wird jedoch das Alter des Nutzers nicht überprüft.

Verarbeitung besonderer Kategorien personenbezogener Daten

Zu überprüfendes Datenschutzprinzip
Werden besondere Kategorien personenbezogener Daten Verarbeitet? Wenn ja, hängt diese Verarbeitung von einer expliziten Einwilligung des Nutzers ab? Erfolgt die Verarbeitung aus im Artikel 9 Absatz 2 Buchstaben b) bis j) beschriebenen Ausnahmegründen?
Rechtliche Grundlage
Artikel 9 DSGVO
Ergebnis
Besondere Kategorien personenbezogener Daten werden nicht explizit erhoben. Diese können aber zufällig von Sprachassistenten aufgenommen werden. Verarbeitung dieser Daten wird von Amazon nicht erwähnt.

Transparenz

Zu überprüfendes Datenschutzprinzip
Werden Informationen und Mitteilungen von Artikeln 13 bis 22 in präziser, transparenter, verständlicher und leicht zugänglicher Form in einer klaren und einfachen Sprache übermittelt?
Rechtliche Grundlage
Artikel 12 Absatz 1 DSGVO
Ergebnis
Im Google App Store sind sowohl die App Amazon Alexa als auch die App Amazon Shopping mit der Datenschutzerklärung vom 29. August 2017 in englischer Sprache verlinkt. In Internet findet man eine Amazon.de-Datenschutzerklärung vom 21. März 2019 in deutscher Sprache. Diese ist auch aus den Amazon-Apps abrufbar. Die Datenschutzerklärung ist 7 Seiten lang und vermittelt Informationen in einer klaren und verständlichen Sprache.

Zu überprüfendes Datenschutzprinzip
Hat der Verantwortliche innerhalb eines Monats auf die Anfrage des Nutzers zu Artikeln 15 bis 22 reagiert?
Rechtliche Grundlage
Artikel 12 Absatz 3 und 4 DSGVO
Ergebnis
Es wurde unverzüglich mit einer Bestätigung des Erhalts der Anfrage reagiert und am 10.04.2019 wurden die Daten zum Download bereitgestellt.

Zu überprüfendes Datenschutzprinzip
Werden Informationen nach Artikeln 13 bis 22 DSGVO unentgeltlich zur Verfügung gestellt?
Rechtliche Grundlage
Artikel 12 Absatz 5 DSGVO
Ergebnis
Informationen, die zur Verfügung gestellt wurden, wurden kostenlos gestellt.

Informationspflicht bei der Erhebung personenbezogener Daten

Zu überprüfendes Datenschutzprinzip	
Teilt der Verantwortliche zum Zeitpunkt der Erhebung personenbezogener Daten des Nutzers folgende Daten mit?	
Rechtliche Grundlage	
Artikel 13 Absatz 1 und 2 DSGVO	
Ergebnis	
Namen und die Kontaktdaten des Verantwortlichen sowie gegebenenfalls seines Vertreters.	ja
Gegebenenfalls Kontaktdaten des Datenschutzbeauftragten.	ja
Zwecke, für die die personenbezogenen Daten verarbeitet werden sollen, sowie die Rechtsgrundlage für die Verarbeitung.	ja
Dauer, für die die personenbezogenen Daten gespeichert werden oder die Kriterien für die Festlegung dieser Dauer.	ja
Bestehen eines Rechts auf Auskunft.	ja
Bestehen eines Rechts auf Berichtigung.	ja
Bestehen eines Rechts auf Löschung.	ja
Bestehen eines Rechts auf Einschränkung der Verarbeitung.	ja
Bestehen eines Widerspruchsrechts gegen die Verarbeitung.	ja
Bestehen des Rechts auf Datenübertragbarkeit.	ja
Bestehen eines Rechts, die Einwilligung jederzeit zu widerrufen.	ja
Bestehen eines Beschwerderechts bei einer Aufsichtsbehörde	ja
Auskunft darüber, ob die Bereitstellung der personenbezogenen Daten gesetzlich oder vertraglich vorgeschrieben oder für einen Vertragsabschluss erforderlich ist.	ja
Auskunft darüber, ob die betroffene Person verpflichtet ist, die personenbezogenen Daten bereitzustellen, und welche möglichen Folgen die Nichtbereitstellung hätte.	ja
Bestehen einer automatisierten Entscheidungsfindung einschließlich Profiling und aussagekräftige Informationen dazu.	ja

Auskunftsrecht

Zu überprüfendes Datenschutzprinzip
Erteilt der Verantwortliche Auskunft über die verarbeiteten personenbezogenen Daten auf Anfrage des Nutzers? Wenn ja, stellt der Verarbeiter folgende Informationen zur Verfügung?
Rechtliche Grundlage
Artikel 15 Absatz 1
Ergebnis
Eine Anfrage auf Datenauskunft wurde am 26.03.2019 über die Webseite gestellt. Am 26.03.2019 kam eine Antwort mit dem Hinweis, dass man Informationen in den Datenschutztexten nachlesen kann und am 10.04.2019 kam ein Link zum Download der gespeicherten Daten.

Recht auf Berichtigung

Zu überprüfendes Datenschutzprinzip
Werden personenbezogene Daten auf Anfrage berichtigt?
Rechtliche Grundlage
Artikel 16 DSGVO
Ergebnis
Name, E-Mail-Adresse, Passwort und Adresse können in den Einstellungen auf der Amazon-Webseite geändert werden. Sprachaufzeichnungen können vom Nutzer gelöscht werden.

Recht auf Löschung

Zu überprüfendes Datenschutzprinzip
Werden personenbezogene Daten des Nutzers gelöscht, wenn der Nutzer die Einwilligung widerruft?
Rechtliche Grundlage
Artikel 17 Absatz 1 Buchstabe b)
Ergebnis
Sprachaufzeichnungen können vom Nutzer jederzeit gelöscht werden. Für eine vollständige Löschung der Daten kann die Löschung des Kundenkontos unter der Webadresse https://www.amazon.de/gp/help/customer/contact-us angefragt werden.

Recht auf Datenübertragbarkeit

Zu überprüfendes Datenschutzprinzip
Werden Daten auf Anfrage dem Nutzer in einem strukturierten, gängigen und maschinenlesbaren Format zur Verfügung gestellt?
Rechtliche Grundlage
Artikel 20 DSGVO
Ergebnis
Datenauskunft kann unter der Webadresse https://www.amazon.de/gp/help/customer/contact-us beantragt werden Die Daten wurden zum Download bereitgestellt. Zu den zur Verfügung gestellten Daten gehören: - Aufgenommene Befehle von Alexa in schrift- und Sprachform in CSV- und MP3-Format - Kontoinformationen im PDF-Format - Geräteinformationen im CSV-Format - Schriftverkehr mit Amazon im PDF-Format - Suchanfragen im CSV-Format

Datenschutz durch Technikgestaltung und Voreinstellungen

Zu überprüfendes Datenschutzprinzip
Privacy By Design: Ist die Technik im Sinne der Datenschutzgrundsätze gestaltet?
Rechtliche Grundlage
Artikel 25 Absatz 1 DSGVO
Ergebnis
Alle Echo-Geräte verfügen über einen Hardware-Knopf, mit dem man das Mithören des Gerätes ausschalten kann. Nach dem Abmelden des Gerätes vom Dienst, bleiben keine Daten des Nutzers auf dem Gerät. Das Echo-Geräte ohne Bildschirm können über die Alexa-App zurückgesetzt werden. Echo Show kann direkt auf dem Gerät in den Einstellungen zurückgesetzt werden.

Zu überprüfendes Datenschutzprinzip
Privacy By Default: Sind die Voreinstellungen so eingestellt, dass nur die personenbezogenen Daten erhoben werden, deren Verarbeitung für den jeweiligen bestimmten Verarbeitungszweck erforderlich ist?
Rechtliche Grundlage
Artikel 25 Absatz 2 DSGVO
Ergebnis
Beim Eingeben des WLAN-Passwortes und des Passwortes für das Amazon-Konto auf einem Echo Show (Generation 1) ist die Sichtbarkeit des Passwortest voreingestellt. Ist ausblendbar.

Sicherheit der Verarbeitung

Zu überprüfendes Datenschutzprinzip
Ergreift der Verantwortliche unter Berücksichtigung der Verhältnismäßigkeit technische und organisatorische Maßnahmen, um Sicherheit der Verarbeitung zu gewährleisten?
Rechtliche Grundlage
Artikel 32 Absatz 1 DSGVO
Ergebnis
Datenübertragungen werden laut der Datenschutzerklärung mit SSL- und PCI DSS-Mechanismen verschlüsselt Zugang zum Dienst ist passwortgeschützt. Zugang zu Funktionen der Echo-Geräten mit Stimmprofile beschränken. Echo-Geräte sind nach dem Koppeln mit einem Amazon-Konto für andere Geräte nicht mehr sichtbar. Alle Echo-Geräte verfügen über einen Hardware-Knopf zum Deaktivieren der Mikrofone. Beim Echo Show kann die Videokamera in Einstellungen deaktiviert werden.

Prüfungsprotokoll - Google Dienste und Wearables

Allgemeine Beschreibung

- Überprüfung der Datenschutzprinzipien beim Dienst Google Home
- Benötigte Komponenten sind eine die Google Home App auf einem Android-Gerät und ein Google Home-Gerät
- Die App Google Home wird am 25.03.2019 aus dem Google Store bezogen
- Die App wurde zu diesem Zeitpunkt über 50 Millionen Mal heruntergeladen und hat eine Durchschnittsbewertung von 4,1 von 5 Sternen.
- Entwickler der App ist Google LLC.
- Aktuelle Datenschutzrichtlinie ist vom 22.01.2019

Rechtmäßigkeit der Verarbeitung

Zu überprüfendes Datenschutzprinzip
Wird vor der Erhebung der Daten der Nutzer um eine Einwilligung zu der Verarbeitung der ihn betreffenden personenbezogenen Daten für einen oder mehrere Zwecke gefragt?
Rechtliche Grundlage
Artikel 6 Absatz 1 Buchstabe a) DSGVO
Ergebnis
Vor dem Anmelden in der App wird man darauf hingewiesen, dass man mit dem Fortfahren den Datenschutzbestimmungen von Google zustimmt. Ohne Zustimmung ist kein Nutzen des Dienstes möglich.

Zu überprüfendes Datenschutzprinzip
In welcher Form erfolgt die Einwilligung zur Verarbeitung der personenbezogenen Daten?
Rechtliche Grundlage
Artikel 6 Absatz 1 Buchstabe a) DSGVO
Ergebnis
Mit dem Fortfahren bei der Anmeldung in der Google Home App.

Zu überprüfendes Datenschutzprinzip
Ist die Verarbeitung für die Erfüllung des Vertrages oder zur Durchführung vorvertraglicher Bedingungen erforderlich?
Rechtliche Grundlage
Artikel 6 Absatz 1 Buchstabe b) DSGVO
Ergebnis
Personenbezogene Daten werden gebraucht, um Dienstleistungen erfüllen zu können.

Bedingungen für die Einwilligung

Zu überprüfendes Datenschutzprinzip
Betrifft die Einwilligung noch andere Sachverhalte? Wenn Ja, erfolgt das Ersuchen um eine Einwilligung in einer verständlichen und leicht zugänglichen Form in einer klaren und einfachen Sprache und ist diese von anderen Sachverhalten klar zu unterscheiden?
Rechtliche Grundlage
Artikel 7 Absatz 2 DSGVO
Ergebnis
Ja, folgende Aktivitäten sind in der Datenschutzerklärung beschrieben und können deaktiviert werden: • Web- und App-Aktivitäten • Standortverlauf • Geräteinformationen • Sprach- & Audioaktivitäten • YouTube-Suchverlauf • YouTube-Wiedergabeverlauf

Zu überprüfendes Datenschutzprinzip
Kann der Nutzer die Einwilligung jederzeit widerrufen? Wird die betroffene Person über die Möglichkeit eines Widerrufs vor der Abgabe der Einwilligung in Kenntnis gesetzt?
Rechtliche Grundlage
Artikel 7 Absatz 3 DSGVO
Ergebnis
Ja, die Möglichkeit des Widerrufs wird in der Datenschutzerklärung beschrieben.

Zu überprüfendes Datenschutzprinzip
Ist der Widerruf der Einwilligung so einfach wie die Erteilung der Einwilligung?
Rechtliche Grundlage
Artikel 7 Absatz 3 DSGVO
Ergebnis
Nein, da es in der App keine Option zum einfachen Widerruf gibt. Wiederruf wird durch Löschung des Accounts realisiert.

Zu überprüfendes Datenschutzprinzip
Muss der Nutzer der Einwilligung der Verarbeitung personenbezogener Daten zustimmen, die für die Erfüllung des Vertrags nicht erforderlich ist?
Rechtliche Grundlage
Artikel 7 Absatz 4 DSGVO
Ergebnis
Der Nutzer kann in der Account-Verwaltung unter der Adresse https://myaccount.google.com/privacycheckup Einwilligungen für Verarbeitung der Daten für andere Sachverhalte aktivieren und deaktivieren.

Zu überprüfendes Datenschutzprinzip
Wird geprüft, ob der Nutzer mindestens 16 Jahre alt ist?
Rechtliche Grundlage
Artikel 8 DSGVO
Ergebnis
Stellt man das Alter von unter 16 ein, wird erkannt, dass es sich um ein Kind handelt. Es folgen Hinweise für Erziehungsberechtigte, wie man mit einem Konto für Minderjährige umgeht.

Verarbeitung besonderer Kategorien personenbezogener Daten

Zu überprüfendes Datenschutzprinzip
Werden besondere Kategorien personenbezogener Daten Verarbeitet? Wenn ja, hängt diese Verarbeitung von einer expliziten Einwilligung des Nutzers ab? Erfolgt die Verarbeitung aus im Artikel 9 Absatz 2 Buchstaben b) bis j) beschriebenen Ausnahmegründen?
Rechtliche Grundlage
Artikel 9 DSGVO
Ergebnis
In der Datenschutzerklärung werden besondere Kategorien der personenbezogenen Daten beschrieben. Bei Sprachassistenten werden besondere Kategorien personenbezogener Daten nicht explizit erhoben. Sie können jedoch zufällig aufgezeichnet werden. Ein Ersuchen um eine Einwilligung zur Verarbeitung dieser Daten findet nicht statt.

Transparenz

Zu überprüfendes Datenschutzprinzip
Werden Informationen und Mitteilungen von Artikeln 13 bis 22 in präziser, transparenter, verständlicher und leicht zugänglicher Form in einer klaren und einfachen Sprache übermittelt?
Rechtliche Grundlage
Artikel 12 Absatz 1 DSGVO
Ergebnis
Im Google App Store ist unter dem Link zur Datenschutzerklärung ein Dokument Google Chrome Privacy Notice in englischer Sprache zu finden. Beim Starten der App Google Home hat man die Möglichkeit per Link zur Google Datenschutzerklärung vom 22. Januar 2019 in deutscher Sprache zu gelangen. Diese Datenschutzerklärung kann man auch aus der Google Home App abrufen. Zusätzlich ist die Datenschutzerklärung auch im Internet unter der Adresse https://policies.google.com/privacy zu finden. Die Datenschutzerklärung ist 32 Seiten lang. Sie ist in einer gut verständlichen Sprache geschrieben und ist gut strukturiert. Aufgrund des großen Umfangs nicht übersichtlich.

Zu überprüfendes Datenschutzprinzip
Hat der Verantwortliche innerhalb eines Monats auf die Anfrage des Nutzers zu Artikeln 15 bis 22 reagiert?
Rechtliche Grundlage
Artikel 12 Absatz 3 und 4 DSGVO
Ergebnis
Ja, es wurde bereits nach 2 Tagen reagiert.

Zu überprüfendes Datenschutzprinzip
Werden Informationen nach Artikeln 13 bis 22 DSGVO unentgeltlich zur Verfügung gestellt?
Rechtliche Grundlage
Artikel 12 Absatz 5 DSGVO
Ergebnis
Informationen, die zur Verfügung gestellt wurden, wurden kostenlos gestellt.

Informationspflicht bei der Erhebung personenbezogener Daten

Zu überprüfendes Datenschutzprinzip	
Teilt der Verantwortliche zum Zeitpunkt der Erhebung personenbezogener Daten des Nutzers folgende Daten mit?	
Rechtliche Grundlage	
Artikel 13 Absatz 1 und 2 DSGVO	
Ergebnis	
Namen und die Kontaktdaten des Verantwortlichen sowie gegebenenfalls seines Vertreters.	ja
Gegebenenfalls Kontaktdaten des Datenschutzbeauftragten.	nein
Zwecke, für die die personenbezogenen Daten verarbeitet werden sollen, sowie die Rechtsgrundlage für die Verarbeitung.	ja
Dauer, für die die personenbezogenen Daten gespeichert werden oder die Kriterien für die Festlegung dieser Dauer.	ja
Bestehen eines Rechts auf Auskunft.	ja
Bestehen eines Rechts auf Berichtigung.	ja
Bestehen eines Rechts auf Löschung.	ja
Bestehen eines Rechts auf Einschränkung der Verarbeitung.	ja
Bestehen eines Widerspruchsrechts gegen die Verarbeitung.	ja
Bestehen des Rechts auf Datenübertragbarkeit.	ja
Bestehen eines Rechts, die Einwilligung jederzeit zu widerrufen.	ja
Bestehen eines Beschwerderechts bei einer Aufsichtsbehörde	ja
Auskunft darüber, ob die Bereitstellung der personenbezogenen Daten gesetzlich oder vertraglich vorgeschrieben oder für einen Vertragsabschluss erforderlich ist.	ja
Auskunft darüber, ob die betroffene Person verpflichtet ist, die personenbezogenen Daten bereitzustellen, und welche möglichen Folgen die Nichtbereitstellung hätte.	ja
Bestehen einer automatisierten Entscheidungsfindung einschließlich Profiling und aussagekräftige Informationen dazu.	nein

Auskunftsrecht

Zu überprüfendes Datenschutzprinzip
Erteilt der Verantwortliche Auskunft über die verarbeiteten personenbezogenen Daten auf Anfrage des Nutzers? Wenn ja, stellt der Verarbeiter folgende Informationen zur Verfügung?
Rechtliche Grundlage
Artikel 15 Absatz 1
Ergebnis
Eine Anfrage auf Datenauskunft wurde am 27.03.2019 über die Webseite https://support.google.com/policies/contact/general_privacy_form gestellt Am 29.03.2019 kam die Antwort per E-Mail, mit dem Verweis, dass die angeforderten Informationen in den Datenschutztexten nachgelesen werden können.

Recht auf Berichtigung

Zu überprüfendes Datenschutzprinzip
Werden personenbezogene Daten auf Anfrage berichtigt?
Rechtliche Grundlage
Artikel 16 DSGVO
Ergebnis
Name, Geburtstag, Profilbild und Geschlecht und Kontaktdaten können direkt und unverzüglich vom Nutzer in der im Google-Konto geändert werden.

Recht auf Löschung

Zu überprüfendes Datenschutzprinzip
Werden personenbezogene Daten des Nutzers gelöscht, wenn der Nutzer die Einwilligung widerruft?
Rechtliche Grundlage
Artikel 17 Absatz 1 Buchstabe b)
Ergebnis
Personenbezogene Daten des Nutzers werden mit dem Löschen des Kontos gelöscht. Sprachaufzeichnungen und andere Aktivitäten sind im Google-Konto löschbar.

Recht auf Datenübertragbarkeit

Zu überprüfendes Datenschutzprinzip
Werden Daten auf Anfrage dem Nutzer in einem strukturierten, gängigen und maschinenlesbaren Format zur Verfügung gestellt?
Rechtliche Grundlage
Artikel 20 DSGVO
Ergebnis
Download ausgewählter Daten im Google-Konto möglich. Die Daten werden im CSV- und TCX-Format zur Verfügung gestellt.

Datenschutz durch Technikgestaltung und Voreinstellungen

Zu überprüfendes Datenschutzprinzip
Privacy By Design: Ist die Technik im Sinne der Datenschutzgrundsätze gestaltet?
Rechtliche Grundlage
Artikel 25 Absatz 1 DSGVO
Ergebnis
Das Löschen aller Daten vom Gerät ist durch das Zurücksetzen auf Werkseinstellungen durch den Nutzer jederzeit möglich. Ansonsten gibt es in der App keine Rechte-Optionen. Alle Home Geräte verfügen über Tasten, mit denen man Mikrofone der Geräte ausschalten kann. Nach dem Koppeln nicht mehr sichtbar und nicht koppelbar.

Zu überprüfendes Datenschutzprinzip
Privacy By Default: Sind die Voreinstellungen so eingestellt, dass nur die personenbezogenen Daten erhoben werden, deren Verarbeitung für den jeweiligen bestimmten Verarbeitungszweck erforderlich ist?
Rechtliche Grundlage
Artikel 25 Absatz 2 DSGVO
Ergebnis
Für optionale Verarbeitungsmöglichkeiten der Daten ist die Voreinstellung auf Einwilligung eingestellt. Diese können im Nachhinein in der Kontoverwaltung deaktiviert werden.

Sicherheit der Verarbeitung

Zu überprüfendes Datenschutzprinzip
Ergreift der Verantwortliche unter Berücksichtigung der Verhältnismäßigkeit technische und organisatorische Maßnahmen, um Sicherheit der Verarbeitung zu gewährleisten?
Rechtliche Grundlage
Artikel 32 Absatz 1 DSGVO
Ergebnis
Zugang zum Dienst ist passwortgeschützt. Zum Sprachassistenten jedoch nicht. Sprachassistenten sind nur im Einrichtungsmodus für andere Geräte sichtbar.

Anlage 3 – Messprotokolle

Messprotokoll - Amazon Echo Dot (3. Generation)

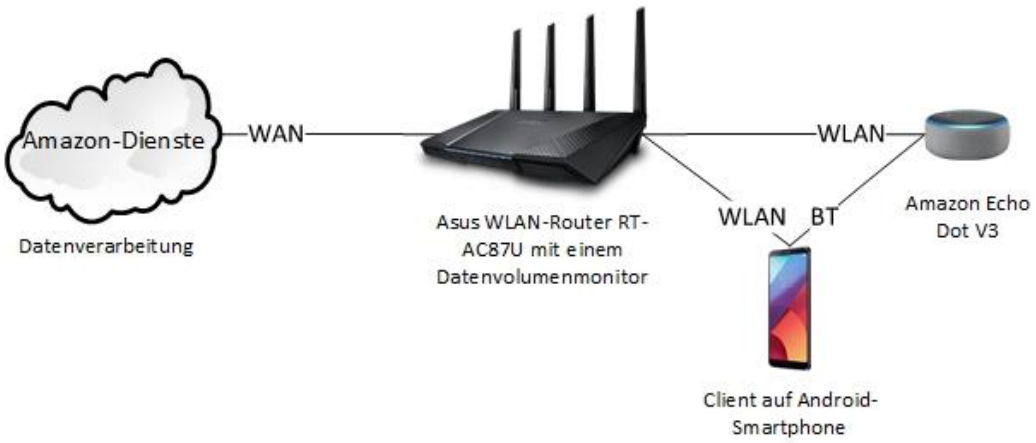
Allgemeine Beschreibung

Amazons Echo-Geräte ohne Display verfügen neben Lautsprecher über Mikrofone für die Aufnahme der Sprachbefehle. Diese lassen sich mittels eines Hardware-Knopfs auf dem Gerät abschalten. Damit wird die im Artikel 25 Absatz 1 DSGVO gestellte Forderung nach der Gestaltung der Technik im Sinne der Datenschutzgrundsätze erfüllt. Bei diesem Test wird überprüft, ob das Betätigen des Knopfes für die Abschaltung der Mikrofone zur Unterbrechung des Datenflusses führt.

Testumgebung

Für den Test werden folgende Komponenten benötigt:

- Amazon Echo Dot der dritten Generation
    - Das Gerät hat die Softwarenummer 1923068932
- Ein Router mit einer Datenflussüberwachungsfunktion
    - In diesem Fall ein Asus WLAN-Router RT-AC87U mit der originalen Firmware der Version 3.0.0.4.382_50702



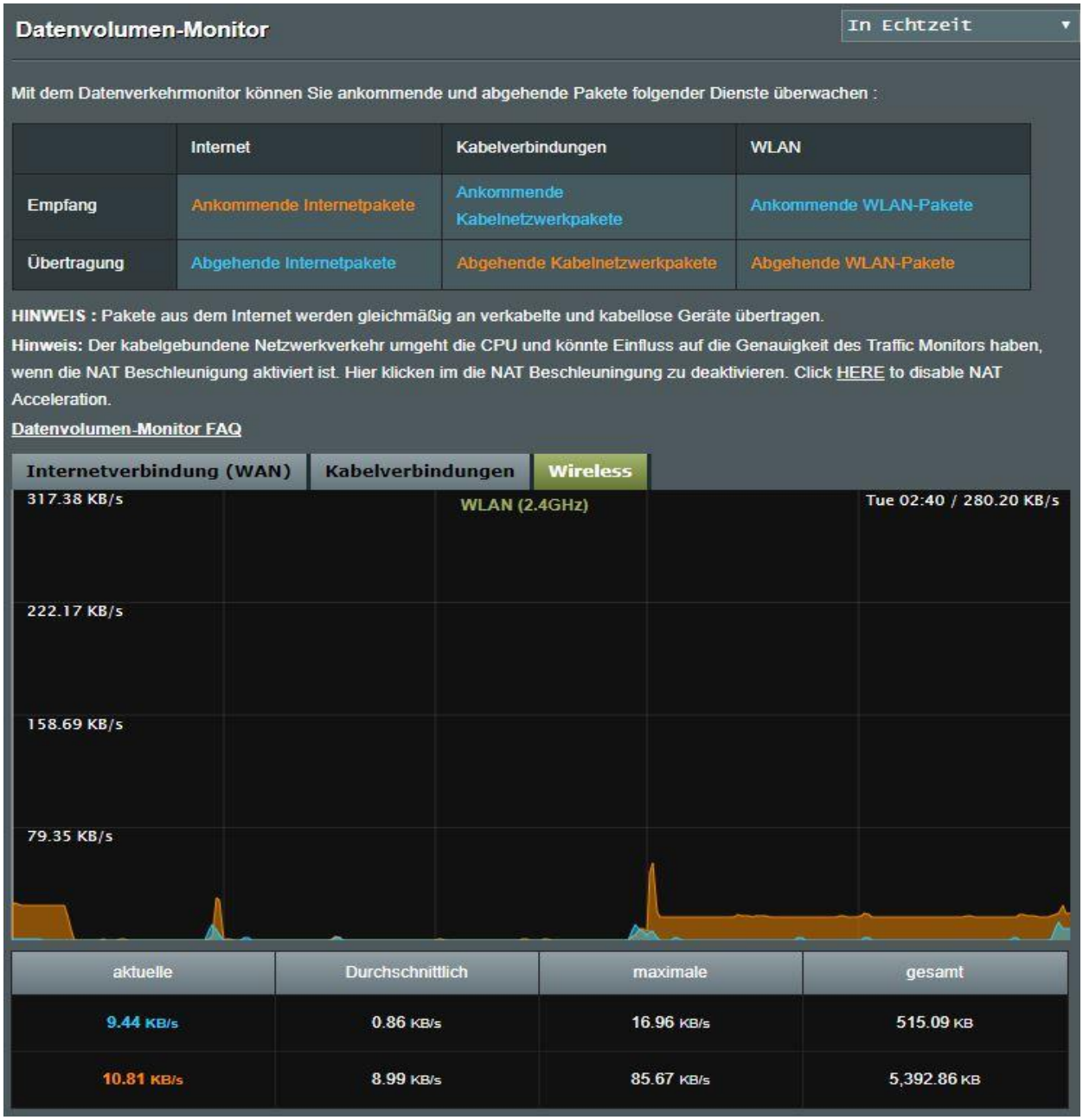
Testverfahren

- Es wird der Datenfluss zwischen dem Sprachassistenten und dem Router gemessen. Da bei diesem Test gemessen werden soll, in welchem Fall die aufgezeichneten Daten vom Sprachassistenten gesendet werden, ist der am Router ankommende Datenfluss zu beachten.
- Das Echo-Gerät und der Router werden mittels eines 2,4 GHz WLANs verbunden.
- Während des Tests sind alle weiteren Geräte von diesem Netzwerk getrennt.

- Die Dauer des Tests beträgt 10 Minuten. Dabei werden ca. alle 2 Minuten folgende Befehle bei jeweils eingeschaltetem und ausgeschaltetem Mikrofon ausgesprochen:
    - Befehl 1: Alexa, wie ist das aktuelle Wetter (Minute 0: AUS, Minute 2: EIN)
    - Befehl 2: Alexa, spiel Ostseewelle (Minute 4: AUS, Minute 6: EIN)
    - Befehl 3: Alexa, spiel Antenne-MV (Minute 8: AUS, Minute 10: EIN)

  Das Mikrofon wird alle vier Minuten vor der Aussprache des Befehls abgeschaltet. In der Zwischenzeit bleibt das Mikrofon eingeschaltet, um zu testen, ob Daten auch ohne des Codewortes Alexa aufgenommen werden.

Testergebnisse



Messprotokoll - Amazon Echo Show

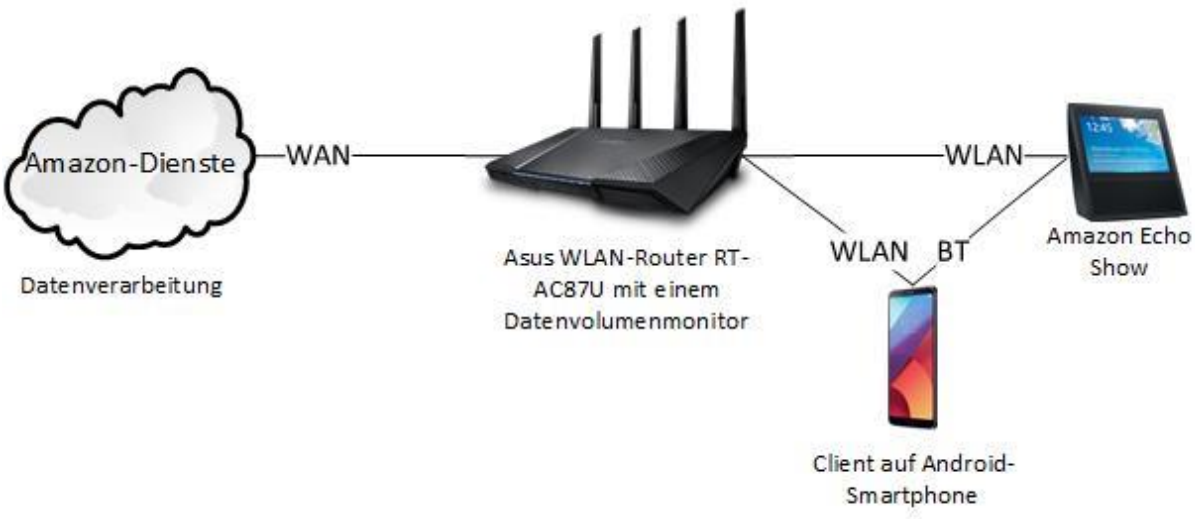
Allgemeine Beschreibung

Amazons Echo-Geräte mit Display verfügen neben Lautsprecher und Display auch über Mikrofone für die Aufnahme der Sprachbefehle. Diese lassen sich mittels eines Hardware-Knopfs auf dem Gerät abschalten. Damit wird die im Artikel 25 Absatz 1 DSGVO gestellte Forderung nach der Gestaltung der Technik im Sinne der Datenschutzgrundsätze erfüllt. Bei diesem Test wird überprüft, ob das Betätigen des Knopfes für die Abschaltung der Mikrofone zur Unterbrechung des Datenflusses führt.

Testumgebung

Für den Test werden folgende Komponenten benötigt:

- Amazon Echo Show der ersten Generation
- Ein Router mit einer Datenflussüberwachungsfunktion
    - In diesem Fall ein Asus WLAN-Router RT-AC87U mit der originalen Firmware der Version 3.0.0.4.382_50702



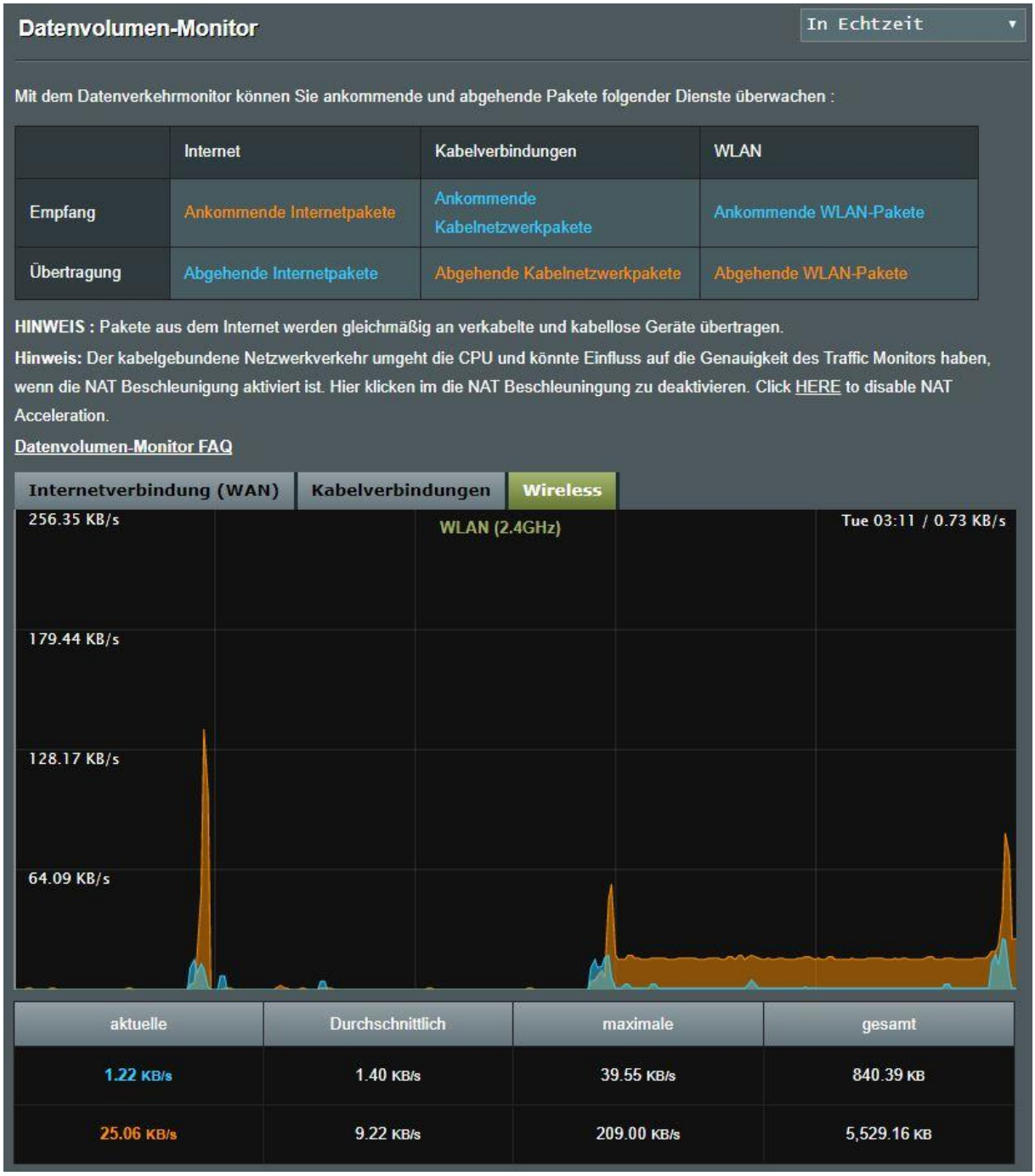
Testverfahren

- Es wird der Datenfluss zwischen dem Sprachassistenten und dem Router gemessen. Da bei diesem Test gemessen werden soll, in welchem Fall die aufgezeichneten Daten vom Sprachassistenten gesendet werden, ist der am Router ankommende Datenfluss zu beachten.
- Das Echo-Gerät und der Router werden mittels eines 2,4 GHz WLANs verbunden.
- Während des Tests sind alle weiteren Geräte von diesem Netzwerk getrennt.
- Die Dauer des Tests beträgt 10 Minuten. Dabei werden ca. alle 2 Minuten folgende Befehle bei jeweils eingeschaltetem und ausgeschaltetem Mikrofon ausgesprochen:

- Befehl 1: Alexa, wie ist das aktuelle Wetter (Minute 0: AUS, Minute 2: EIN)
- Befehl 2: Alexa, spiel Ostseewelle (Minute 4: AUS, Minute 6: EIN)
- Befehl 3: Alexa, spiel Antenne-MV (Minute 8: AUS, Minute 10: EIN)

Das Mikrofon wird alle vier Minuten vor der Aussprache des Befehls abgeschaltet. In der Zwischenzeit bleibt das Mikrofon eingeschaltet, um zu testen, ob Daten auch ohne des Codewortes Alexa aufgenommen werden.

Testergebnisse



Messprotokoll – Google Home Mini

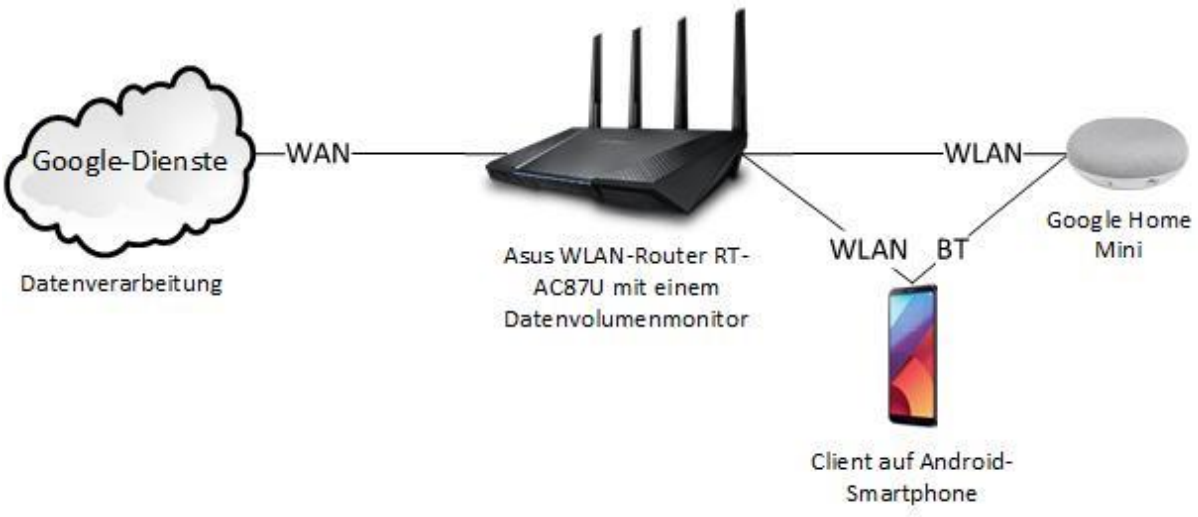
Allgemeine Beschreibung

Googles Home-Geräte ohne Display verfügen neben Lautsprecher über Mikrofone für die Aufnahme der Sprachbefehle. Diese lassen sich mittels eines Hardware-Knopfs auf dem Gerät abschalten. Damit wird die im Artikel 25 Absatz 1 DSGVO gestellte Forderung nach der Gestaltung der Technik im Sinne der Datenschutzgrundsätze erfüllt. Bei diesem Test wird überprüft, ob das Betätigen des Knopfes für die Abschaltung der Mikrofone zur Unterbrechung des Datenflusses führt.

Testumgebung

Für den Test werden folgende Komponenten benötigt:

- Google Home Mini
- Ein Router mit einer Datenflussüberwachungsfunktion
    - In diesem Fall ein Asus WLAN-Router RT-AC87U mit der originalen Firmware der Version 3.0.0.4.382_50702



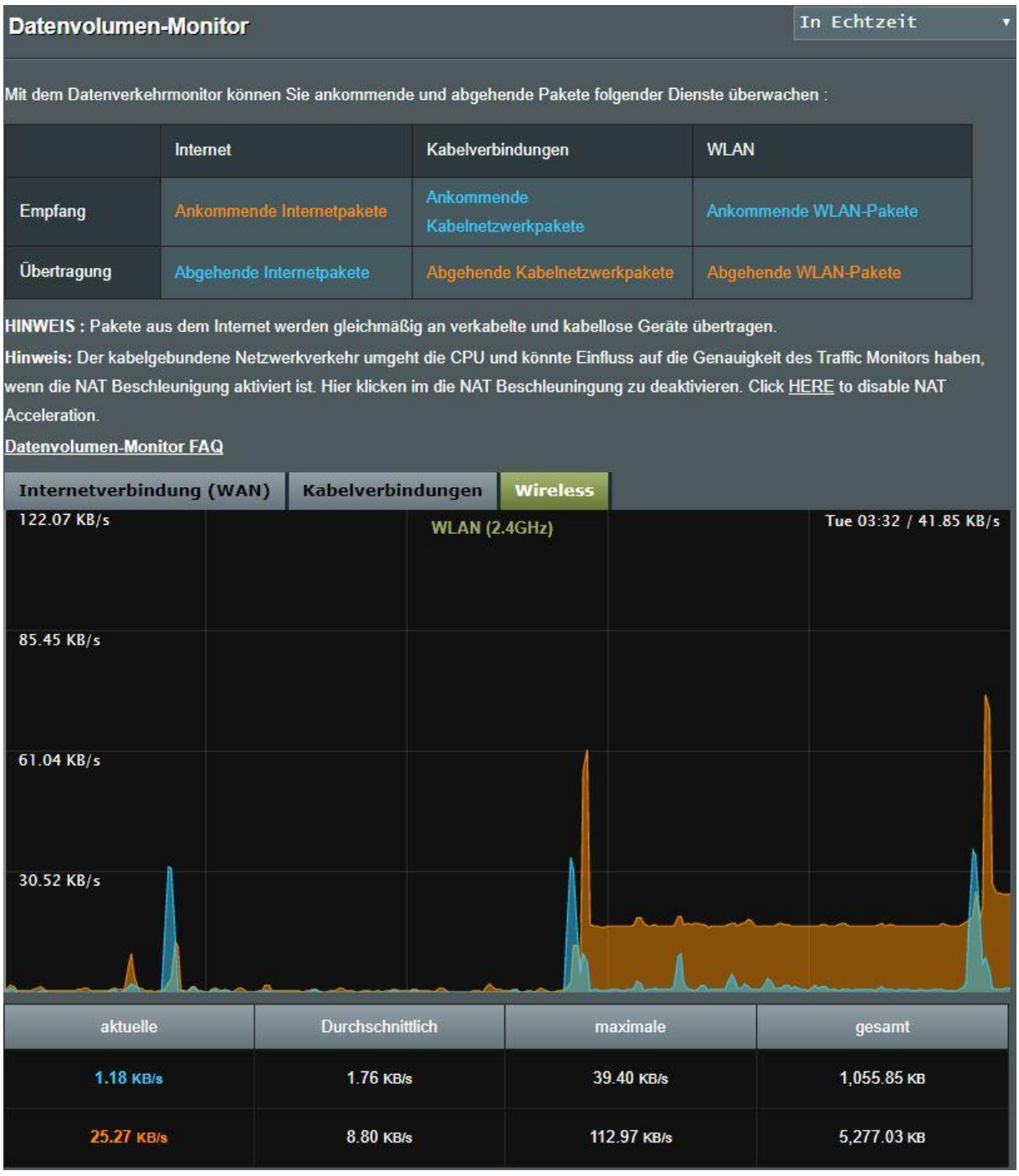
Testverfahren

- Es wird der Datenfluss zwischen dem Sprachassistenten und dem Router gemessen. Da bei diesem Test gemessen werden soll, in welchem Fall die aufgezeichneten Daten vom Sprachassistenten gesendet werden, ist der am Router ankommende Datenfluss zu beachten.
- Das Home-Gerät und der Router werden mittels eines 2,4 GHz WLANs verbunden.
- Während des Tests sind alle weiteren Geräte von diesem Netzwerk getrennt.
- Die Dauer des Tests beträgt 10 Minuten. Dabei werden ca. alle 2 Minuten folgende Befehle bei jeweils eingeschaltetem und ausgeschaltetem Mikrofon ausgesprochen:

- Befehl 1: OK Google, wie ist das aktuelle Wetter (Minute 0: AUS, Minute 2: EIN)
- Befehl 2: OK Google, spiel Ostseewelle (Minute 4: AUS, Minute 6: EIN)
- Befehl 3: OK Google, spiel Antenne-MV (Minute 8: AUS, Minute 10: EIN)

Das Mikrofon wird alle vier Minuten vor der Aussprache des Befehls abgeschaltet. In der Zwischenzeit bleibt das Mikrofon eingeschaltet, um zu testen, ob Daten auch ohne des Codewortes Alexa aufgenommen werden.

Testergebnisse



VIII. ABSTRACT

Ununterbrochen vernetzte intelligente Geräte im privaten Umfeld der Menschen erleichtern das Leben der Nutzer. Sie sind in der Lage, selbstständig und ohne Eingreifen der Menschen, direkt miteinander zu kommunizieren und Daten auszutauschen. Einige dieser Geräte erheben personenbezogene Daten der Nutzer, ohne dass die Nutzer es mitbekommen. Diese Daten werden zur Verarbeitung an die Server der Diensteanbieter gesendet. Die Nutzer haben keinen Einblick darauf, wie und zu welchem Zweck ihre Daten verarbeitet werden. Die Gesetzgebung schützt mit Datenschutzvorschriften die Nutzer vor dem Missbrauch ihrer Daten. Auf Grund der schnellen technischen Entwicklung der im Internet der Dinge agierenden Geräte, ist es für die Gesetzgebung sehr schwer, ihre Vorschriften dieser Entwicklung rechtzeitig anzupassen. Das stellt für den Datenschutz eine Herausforderung dar.

Diese Arbeit befasst sich damit, inwieweit sich die Hersteller und Diensteanbieter für Anwendungssysteme im Internet der Dinge im Verbraucherbereich, an die Datenschutzvorschriften halten. Zu diesem Zweck werden zuerst geeignete Datenschutzvorschriften ermittelt und die bereits vorliegenden Forschungsergebnisse zu diesem Thema ausgewertet. Anschließend werden Anwendungssysteme und die dazugehörigen Datenschutztexte untersucht. Ergebnisse dieser Untersuchungen zeigen den Stand des Datenschutzes in diesem Bereich.

Continuously connected smart devices in the private environment of people make life easier for users of this devices. They are able to communicate and exchange data directly with each other independently and without human intervention. Some of these devices collect users' personal data without the user knowing. These data are sent for processing to the servers of the service providers. Users have no insight into how and for what purpose their data are processed. The legislation protects users against misuse of their data with data protection regulations. Due to the rapid technical development of devices operating on the Internet of Things, it is very difficult for the legislation to adapt their regulations to this development in a timely manner. This poses a challenge to data protection.

This paper looks to what extent manufacturers and service providers of application systems on the Internet of Things in the Consumer Sector comply with data protection regulations. For this purpose, appropriate data protection regulations are first identified and the existing research results on this topic are evaluated. Subsequently, application systems and the associated data protection texts are examined. Results of these investigations show the state of data protection in this area.