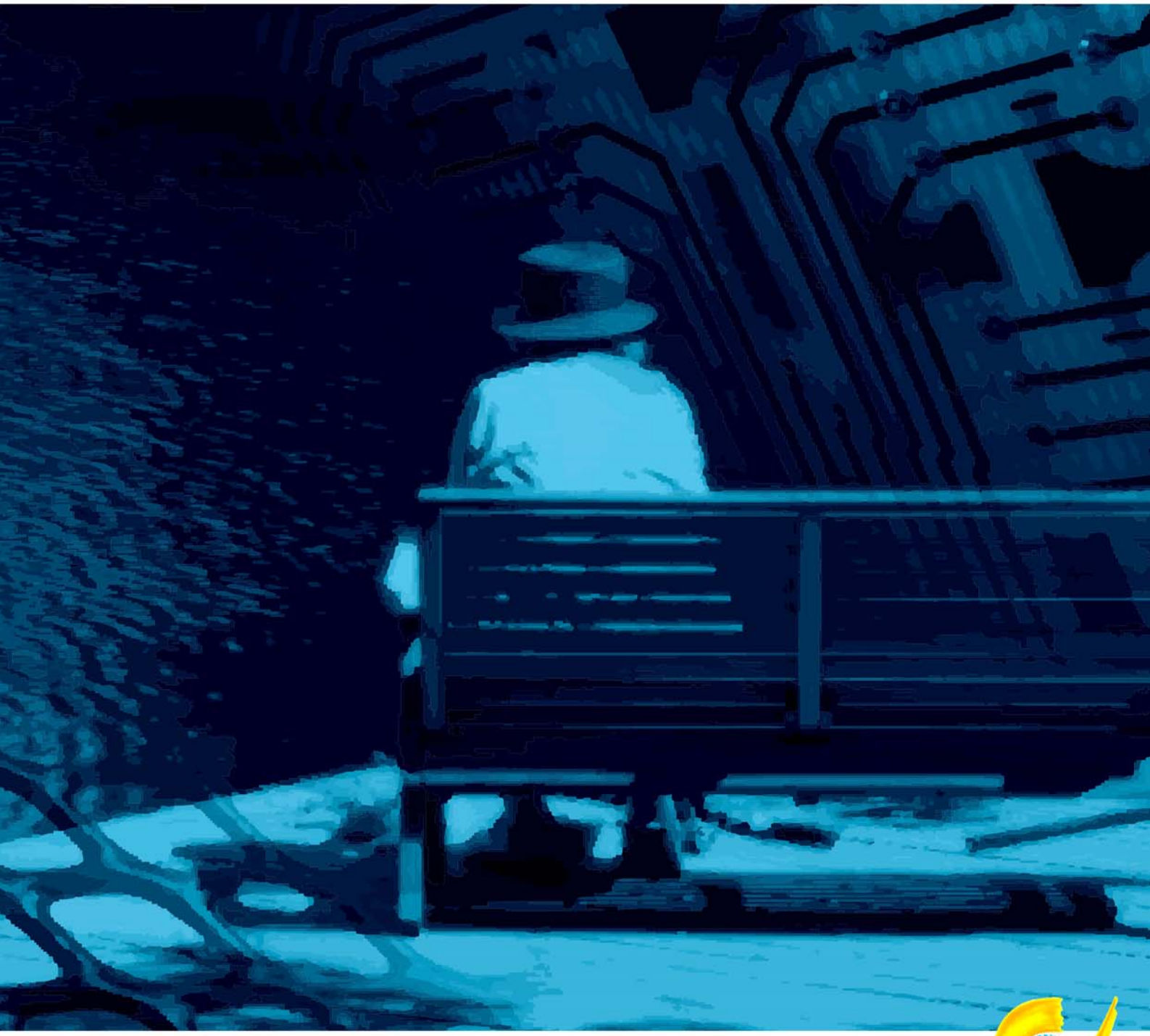
Bundesministerium
für Bildung
und Forschung

VDI|VDE|IT

Juristische Fragen im Bereich Altersgerechter Assistenzsysteme



Vorstudie im Auftrag von VDI/VDE-IT
im Rahmen des BMBF-Förderschwerpunktes
"Altersgerechte Assistenzsysteme für ein gesundes und unabhängiges Leben - AAL"

ULD
Unabhängiges Landeszentrum für
Datenschutz Schleswig-Holstein

Vorstudie

– Juristische Fragen im Bereich altersgerechter Assistenzsysteme –

Im Auftrag vom

VDI/VDE Innovation + Technik GmbH

Steinplatz 1

10623 Berlin

Verfasser:

Unabhängiges Landeszentrum für Datenschutz Schleswig-Holstein (ULD)

Holstenstr. 98, 24103 Kiel

http://www.datenschutzzentrum.de/

Dezember 2010

Zusammenfassung

In unserer Gesellschaft werden altersgerechte Assistenzsysteme, die Menschen gerade im fortschreitenden Alter unterstützen, immer wichtiger. Unter dem Begriff **Ambient Assisted Living (AAL)** werden Konzepte, Produkte und Dienstleistungen diskutiert, die neue Technologien und soziales Umfeld miteinander verbinden, um die Lebensqualität zu erhöhen. Beispielsweise können AAL-Systeme älteren Menschen dazu dienen, ein sicheres und selbstständiges Leben im häuslichen Umfeld zu ermöglichen oder verlängern.

Diese Vorstudie „Juristische Fragen im Bereich altersgerechter Assistenzsysteme“ zeigt die wesentlichen **rechtlichen Fragen und Herausforderungen in Bezug auf altersgerechte Assistenzsysteme** auf. Ein Fokus liegt auf dem Datenschutzrecht, aus dem sich zum einen allgemeine Anforderungen, abgeleitet aus der Verfassung und dem Bundesdatenschutzgesetz, zum anderen spezielle Vorgaben beispielsweise im ärztlichen Bereich oder im Telekommunikations- und Telemedienbereich ergeben. Daneben werden die Bereiche Haftungsrecht, Sozialversicherungsrecht, Delegation von Aufgaben an AAL-Systeme, Einbeziehung internationaler Akteure sowie die Fragen möglicher Zugriffe durch Dritte wie Strafverfolgungsbehörden und Versicherungen erörtert.

Die Analyse zeigt, dass AAL-Technik eine Vielzahl von juristischen Feldern berührt, deren Anforderungen berücksichtigt werden müssen. Gleichzeitig wird deutlich, dass die bestehende Rechtslage, die den Entwicklern und Anwendern von AAL-Techniken Erwartungssicherheit darüber geben soll, was die Gesellschaft von ihnen erwartet, unbefriedigend ist. So fehlt es an passgenauen gesetzlichen Regelungen zum Umgang mit einer Technik, die in den **privatesten Kernbereich** von Menschen eindringen soll.

In den meisten Fällen wird der Einsatz von AAL-Technik auf der Basis einer **Einwilligung** der Betroffenen stattfinden: Eine Einwilligung muss zeitlich vor der Datenerhebung eingeholt werden, die Betroffenen müssen einsichtsfähig sein, sie müssen zuvor ausreichend informiert worden sein, im Regelfall ist die Schriftform erforderlich, jede Einwilligung muss freiwillig und hinreichend bestimmt erfolgen. Hieraus ergibt sich, dass das Instrument der Einwilligung in AAL-Systemen an praktische Grenzen stößt, insbesondere weil angesichts der komplexen Technik vielfach nicht davon auszugehen sein wird, dass alle Betroffenen verstehen, in welche Datenverarbeitung sie einwilligen und welche Risiken vorhanden sein können.

Es bestehen umfangreiche Anforderungen an die **Transparenz** und Kontrollmöglichkeiten für AAL-Systeme und deren Komponenten. Diese Transparenz muss spezifisch sowohl auf die Auffassungsgabe von Betroffenen als auch für die rechtlichen Anforderungen an die verantwortlichen Betreiber zugeschnitten sein. Die anzustrebende Transparenz adressiert u.a. die technischen Systeme, die Informationspflichten der Betreiber und die jeweils klare Regelung der haftungsrechtlichen und datenschutzrechtlichen Verantwortung für Komponenten und Systeme.

Die AAL-Systeme und ihre Komponenten müssen so ausgelegt sein, dass der jeweilige Zweck der mit ihnen erfolgenden Datenverarbeitung feststeht. Eine enge **Zweckbindung** der

technischen Datenverarbeitung kann u.a. dadurch erreicht werden, dass konzeptionell Zwecktrennungen vorgenommen und Systemgrenzen eingezogen, die Grundsätze der Datenvermeidung und Datensparsamkeit eingehalten und die Daten nach Erfüllung des Zwecks gelöscht werden. Eine weitergehende Verwendung von Daten durch Dritte, etwa im Rahmen anonymisierter oder pseudonymisierter Daten zu sozialwissenschaftlicher, medizinischer oder versicherungsmathematischer Forschung, bedarf wegen der Sensibilität der Informationen einer klaren gesetzlichen Regelung: Die Vermessung des Lebens von Menschen in AAL-Umgebungen kann über Profilbildungen und automatisiert feststellbaren Abweichungen von Standardwerten einen Rechtfertigungszwang bei den Betroffenen erzeugen, der das Recht auf informationelle Selbstbestimmung beeinträchtigt.

Sowohl die Vielzahl von Beteiligten in AAL-Kontexten als auch der Umstand, dass AAL-Systeme gerade im Hintergrund funktionieren (sollen), können die **Wahrnehmung der Betroffenenrechte** erschweren. Es ist die Frage zu beantworten, wie Betroffene der Fortsetzung einer AAL-Nutzung in ihrem Privatbereich widersprechen können, ohne dass sie dadurch Nachteile erleiden. Es muss Betroffenen überlassen bleiben, eine selbstbestimmte Kontrolle über ihr Leben und deren Umstände auszuüben. Daneben sind Lösungen für geistig eingeschränkte oder durch die technische Komplexität überforderte Menschen zu konzipieren, bei denen Lotsen, Treuhänder oder Paten eine Rolle spielen können, die bei der Wahrnehmung der Nutzerinteressen zur Seite stehen. Diese dürfen dabei nicht von eigenen Interessen, z.B. als Betreiber des AAL-Systems, geleitet werden.

Die Betroffenen müssen sich auf das korrekte Zusammenwirken einzelner Komponenten im AAL-Gesamtsystem und auf die Erbringung der vereinbarten Dienstleistung verlassen können, insbesondere in den Fällen, in denen bei einem Ausfall oder fehlerhaften Funktionieren eine Gefahr für Leib und Leben bestehen kann. In diesen Fällen besteht für die gesamte Datenverarbeitung, sowohl in den Räumlichkeiten der Betroffenen als auch bei den Betreuungsdienstleistern und eingebundenen IT-Dienstleistern, ein **sehr hoher Schutzbeda**rf, der entsprechende Anforderungen an die Gestaltung der Informationstechnik und des Zusammenspiels der Komponenten stellt.

Bei komplexen IT-Systemen hat jeder Mensch ein Recht auf Gewährleistung der Vertraulichkeit und Integrität informationstechnischer Systeme. Diese **staatliche Pflicht** umfasst zunächst die Schaffung adäquater materieller Regelungen, aber kann sich auch auf Zulassungs- und Kontrollverfahren, bei denen Standards für Infrastrukturen gesetzlich vorgegeben und behördlich sichergestellt werden, erstrecken.

Datenschutz und Datensicherheit sind nicht nur in Deutschland, sondern international Akzeptanzkriterien für IT-Systeme. Normenklare Gesetze, selbstverpflichtende Codes of Conduct sowie insbesondere datenschutzgerecht gestaltete AAL-Systeme können nicht nur national zur Stärkung der Rechtsicherheit bei allen Beteiligten führen, sondern auch ein attraktiver **Wettbewerbsfaktor** auf dem Weltmarkt sein.

Das ärztliche **Berufsrecht** schränkt eine automatische Erhebung und Weitergabe medizinischer Daten relativ stark ein. Eine reine Fernbehandlung ist zurzeit verboten. Dies ist zu überdenken.

Soll AAL-Technik in das Gesundheitssystem integriert werden, muss dies auch im Bereich der **Vergütungsregelungen** der ärztlichen Gebührenordnungen erfolgen.

Bei der Einbindung von **internationalen Akteuren** sind jeweils Fragen nach dem anwendbaren Recht und der Gerichtsbarkeit insbesondere in Bezug auf Datenschutzrecht und ärztliches Berufsrecht zu klären.

Haftungsrechtlich ist angesichts der vielen Teilverantwortlichkeiten die Frage herauszuheben, ob eine **verschuldensunabhängige Haftung** des Datenverarbeiters einzuführen geboten ist oder zumindest Beweislasterleichterungen für die Betroffenen vorgesehen werden sollten.

Mögliche Zugriffsrechte der **Strafverfolgungsbehörden** auf AAL-Daten sollten klar geregelt sein. Hier ist von Bedeutung, inwieweit ein Beschlagnahmeschutz für die Gesundheitsdaten greift.

Eine diskriminierende bzw. missbräuchliche Nutzung von AAL-Datenbeständen im **Versicherungsverhältnis** ist zu verhindern.

Inhaltsverzeichnis

Abbildungsverzeichnis

1 Einleitung

Altersgerechte Assistenzsysteme werden in unserer Gesellschaft immer wichtiger, da sie es Personen aller Altersgruppen ermöglichen, ihren Alltag zu meistern. In dieser Studie beschränkt sich der Blick auf die Unterstützung von Erwachsenen[1], gerade auch im fortgeschrittenen Alter, die einen wachsenden Anteil unserer Gesellschaft ausmachen. Die zum Einsatz kommende Technik wird unter dem Begriff Ambient Assisted Living diskutiert:

Ambient Assisted Living (AAL) ist die situationsabhängige und unaufdringliche Unterstützung des Menschen im alltäglichen Leben. Darunter werden Konzepte, Produkte und Dienstleistungen verstanden, die neue Technologien und soziales Umfeld mit dem Ziel miteinander verbinden, die Lebensqualität zu erhöhen.[2] Je nach Nutzergruppe können sie sehr unterschiedlich aussehen. Während bei jüngeren, gesunden Menschen hauptsächlich Unterhaltung und Lifestyle-Funktionen zur Steigerung der Lebensqualität im Vordergrund stehen, zielt AAL bei älteren Menschen darauf ab, ein sicheres, selbstständiges Leben im häuslichen Umfeld zu ermöglichen bzw. zu verlängern. Diese Ziele ergeben sich aus den veränderten gesellschaftlichen Verhältnissen wie dem demographischen Wandel, dem Trend zum Alleinleben, steigenden Ansprüchen an die Lebensqualität sowie steigenden Bedürfnissen an Komfort und Sicherheit.

Auf der einen Seite geht es um technische und eventuell personale Hilfe im Alter, beispielweise im Fall von Demenz, geistiger Behinderung und sonstigen Handicaps sowie bei sonstiger Pflegebedürftigkeit, z.B. wegen Krankheit oder im Rahmen einer Rehabilitation. Auf der anderen Seite können AAL-Hilfsangebote völlig ohne medizinischen oder sozialen Anlass im Alltag von Menschen in Anspruch genommen und zur Unterstützung bei täglichen Verrichtungen oder als Lifestyle-Angebot zur Erhöhung der Lebensqualität genutzt werden. Sie dienen vorrangig der Kommunikation in der Wohnumgebung zur Verbesserung der Informationslage für Betroffene sowie für professionelle Dienstleister oder helfende Privatpersonen. Im Vordergrund stehen derzeit die unaufdringliche Hilfe im Alter und die Notfallhilfe, beispielsweise durch Mobilisierung von Personen oder durch Auslösung von Prozessen.

Das Bundesministerium für Bildung und Forschung (BMBF) fördert auf der Grundlage des Forschungsprogramms „IKT2020“ 18 anwendungsorientierte Verbundprojekte zum Thema AAL. Um die Technik- und Anwendungsentwicklung in diesen Projekten dabei zu unterstützen, dass wünschenswerte Lösungen entstehen und unerwünschte Entwicklungen frühzeitig erkannt und vermieden werden, wurde eine Begleitforschung implementiert, in der spezifi-

[1] Altersgerechte Assistenzsysteme sind auch für Kinder und Jugendliche denkbar. Viele Ergebnisse dieser Studie lassen sich auf solche Systeme übertragen. Einige Rechtsbereiche wären zusätzlich zu untersuchen, z.B. der Bereich des Jugendschutzes.

[2] Driller et al., Ambient Assisted Living, Technische Assistenz für Menschen mit Behinderung, 2009, S. 32.

sche Studien ausgeschrieben werden, in denen ethische, soziale, ergonomische, rechtliche – darunter datenschutzrechtliche – und ökonomische Aspekte vertieft werden.

In diesem Zusammenhang hat die VDI/VDE Innovation + Technik GmbH (VDI/VDE-IT) das Unabhängige Landeszentrum für Datenschutz Schleswig-Holstein (ULD) beauftragt, eine Vorstudie zu den „Juristischen Fragen im Bereich altersgerechter Assistenzsysteme“ zu erstellen.

1.1 Gegenstand und Ziel der Vorstudie

Gegenstand der Studie „Juristische Fragen im Bereich altersgerechter Assistenzsysteme“, sind AAL-Anwendungen, die primär, aber nicht ausschließlich ältere Menschen unterstützen. Ziel der Vorstudie ist es, die juristischen Fragen, die durch die Durchdringung des unmittelbaren Lebensumfelds von Menschen mit AAL-Technik entstehen, aufzuwerfen. Dabei sollen erste Antworten gegeben bzw. Handlungsempfehlungen für weitere vertiefende juristische Betrachtungen im Kontext der 18 geförderten Verbundprojekte erarbeitet werden. Eine vollständige bzw. abschließende Darstellung der Rechtsfragen ist dabei nicht Gegenstand der Vorstudie.

1.2 Methodik und Aufbau dieser Vorstudie

Diese Vorstudie stellt die Resultate dar, die in fünf aufeinanderfolgenden Arbeitspaketen (AP) erarbeitet wurden (siehe Abb. 1).

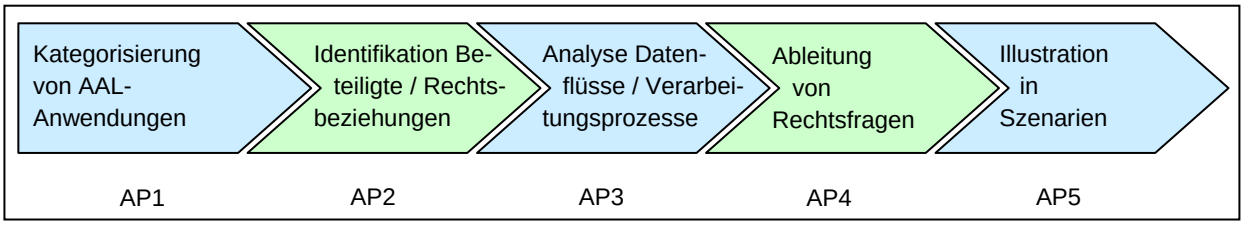


Abb. 1: Arbeitspakete der Vorstudie im Überblick

Der Aufbau der Vorstudie folgt großenteils dem Ablauf der Arbeitspakete. Lediglich die Illustration in Szenarien (AP5) wurde in der Struktur vorgezogen, um bereits zu Beginn der Vorstudie einen Überblick über das Thema und die Einsatzbereiche zu geben. Nach der Einleitung in Kapitel 1 kategorisiert das folgende Kapitel 2 zunächst die typischen AAL-Anwendungen und stellt sie in typischen Szenarien dar. Im Anschluss daran werden die Beteiligten in AAL-Anwendungen identifiziert und deren Rechtsbeziehungen untereinander skizziert. In den Kapiteln 3 bis 9 werden sodann die Rechtsfragen abgeleitet, die in diesen Konstellationen und Rechtsbeziehungen von Relevanz sein können. Der Schwerpunkt liegt dabei auf datenschutzrechtlichen Fragen (in Kapitel 3), ohne dass andere Rechtsbereiche vernachlässigt werden: Dazu gehören die Fragen, die aus den Anforderungen an die Daten-

sicherheit und den technischen Datenschutz resultieren (siehe Kapitel 4), Fragen des Haftungsrechts (siehe Kapitel 5), sozialversicherungsrechtliche Fragen (siehe Kapitel 6), Fragen zu einer möglichen Delegation an AAL-Systeme (siehe Kapitel 7), Fragen aufgrund der Einbeziehung von internationalen Akteuren und grenzüberschreitenden Datenflüssen (siehe Kapitel 8) sowie Fragen zu etwaigen Zugriffsersuchen durch Dritte auf die Daten im AAL-System (siehe Kapitel 9). Die Vorstudie schließt in Kapitel 10 mit einer ausführlichen Zusammenfassung der Ergebnisse und Handlungsempfehlungen.

Während der Erarbeitung der Vorstudie wurde Kontakt zu fünf der vom BMBF geförderten Verbundprojekte aufgenommen. Ziel war es, möglichst praxisrelevante Fragen herauszuarbeiten sowie erste Hinweise aus datenschutzrechtlicher Sicht zu geben. Dabei wurden mit den folgenden Projekten Gespräche geführt:

- SmartAssist

  Plattform zur Unterstützung von sozialen und gesundheitlichen Aspekten bei der Gestaltung eines altersgerechten autonomen Lebens

  Koordinator: Lübecker Wachunternehmen Dr. Kurt Kleinfeldt GmbH

- **SAMDY**

  Sensorbasiertes adaptives Monitoringsystem für die Verhaltensanalyse von Senioren

  Koordinator: Sozialwerk St. Georg e.V.

- **AAL@home**

  Humanzentriertes Assistenzsystem für Sicherheit und Unabhängigkeit älterer, allein lebender Menschen

  Koordinator: Der Paritätische e.V.

Mit den folgenden beiden Projekten erfolgte ein schriftlicher Austausch:

- **SELBST**

  Selbstbestimmt Leben im Alter mit Mikrosystemtechnik

  Koordinator: PME Familienservice

- **DCJ**

  Daily Care Journal – Sensorgestütztes Assistenzsystem für Pflegenetzwerke zur Erfassung von Aktivitäten und existenziellen Erfahrungen des täglichen Lebens

  Koordinator: Euregon AG

2 Anwendungsbereiche, Beteiligte und Datenflüsse

Dieses Kapitel beginnt mit sieben Szenarien, die die Bandbreite von AAL-Anwendungen veranschaulichen. Daneben gibt es einen Überblick über die vielfältigen Anwendungsbereiche von AAL, identifiziert typische Beteiligte sowie die wesentlichen Rechtsbeziehungen untereinander und skizziert Datenflüsse. Mit diesen grundlegenden Informationen stellt es die Basis für die Ableitung der juristischen Fragen in den folgenden Kapiteln dar.

2.1 Typische AAL-Anwendungen, dargestellt in ausgewählten Szenarien

In diesem Abschnitt werden sieben Szenarien des Einsatzes von AAL-Anwendungen vorgestellt. Die Sammlung der Szenarien erlaubt es, die Erfahrungen des fiktiven Paars Alice und Bob als Nutzer von AAL-Anwendungen in diversen Ausprägungen in verschiedenen Lebenssituationen nachzuvollziehen. Die Auswahl der dargestellten AAL-Anwendungen orientiert sich an Angeboten, die bereits jetzt auf dem Markt oder zumindest im Projektstadium existieren.

2.1.1 Szenario 1: „Erleichterung im Haushalt“

Alice und Bob fallen manche Haushaltstätigkeiten schwerer als früher. Es fehlt ihnen insbesondere die Kraft, die schweren Rollläden zu bedienen. Ihre Rollläden haben daher Motoren und Sensoren bekommen, so dass diese entweder auf Knopfdruck, spätestens aber bei Dunkelheit herunter- und bei Helligkeit hochfahren. Auch haben sie beschlossen, ihre Zimmer mit einer automatischen Beleuchtung auszustatten, um Unfälle zu vermeiden. Mit dem Aufschließen der Haustür geht die Beleuchtung im Flur automatisch an. Auch die anderen Zimmer werden bei Dunkelheit dank der Bewegungsmelder automatisch bei Betreten erleuchtet. Dazu haben sie von dem Unternehmen, das ihnen die Motoren, Sensoren und die Bewegungsmelder als Gesamtpaket verkauft hat, eine Fernbedienung erhalten, die es ihnen ermöglicht, die gewünschten Einstellungen vorzunehmen.

Beteiligte: Betroffene(r) Nutzer

2.1.2 Szenario 2: „Notfallhilfe von lieben Verwandten“

Außerdem ist Bob ist aufgrund seines Gesundheitszustands in seiner Mobilität eingeschränkt. Manchmal ist er gezwungen, den ganzen Tag im Bett zu liegen, und kommt dann aus eigener Kraft nicht aus dem Bett. Auch Alice muss für längere Wege einen Rollator benutzen. So beweglich wie noch vor einigen Jahren fühlen sich die beiden nicht mehr. Beiden ist es bereits passiert, dass sie in ihrer Wohnung ins Straucheln geraten sind und beinahe gestürzt wären. Dazu kommt, dass Alice Probleme mit ihrem Blutdruck hat. Bislang hat sie schon drei Mal das Bewusstsein verloren. Glücklicherweise geschah das immer nur dann, wenn sie nach dem ersten Schwindelgefühl schon sicher auf dem Sofa saß. Ihr Sohn **hat**

Alice und Bob daher geraten, ihre Wohnung mit einem Notfallsystem auszustatten (siehe Abb. 2). Denn im Falle eines Sturzes zählt jede Minute, um z.B. im Falle eines Knochenbruches die Chance auf Heilung zu erhöhen. Hantiert Alice gerade mit dem Bügeleisen oder am Herd, kann außerdem auch ein Wohnungsbrand Folge ihrer Bewusstlosigkeit sein. Und was wäre, wenn Alice einmal ausgerechnet dann das Bewusstsein verliert, wenn Bob nicht aus dem Bett aufstehen kann? Das System, für das die beiden sich entschieden haben, heißt „Safe Home“. In Fußmatten auf dem Boden sind Sturzsensoren eingebaut. Diese registrieren die Erschütterung, die bei einem Sturz auftritt. Ein Lesegerät liest über Funk in kurzen Abständen die von den Sensoren gemessenen Werte aus. Wird dabei ein festgelegter **Schwellenwert überschritten, wird ein Alarm ausgelöst**. **Das System informiert selbstständig eine Privatperson (d.h. Kinder, Nachbarn, Freunde)**, die von Alice und Bob bestimmt worden ist, und zwar ihre Tochter. Es ist vereinbart, dass bevor die Tochter einen Krankenwagen ruft, sie zwei Minuten lang versucht, Alice oder Bob telefonisch zu erreichen.[3]

Beteiligte: Betroffene(r) Nutzer, helfende Privatperson

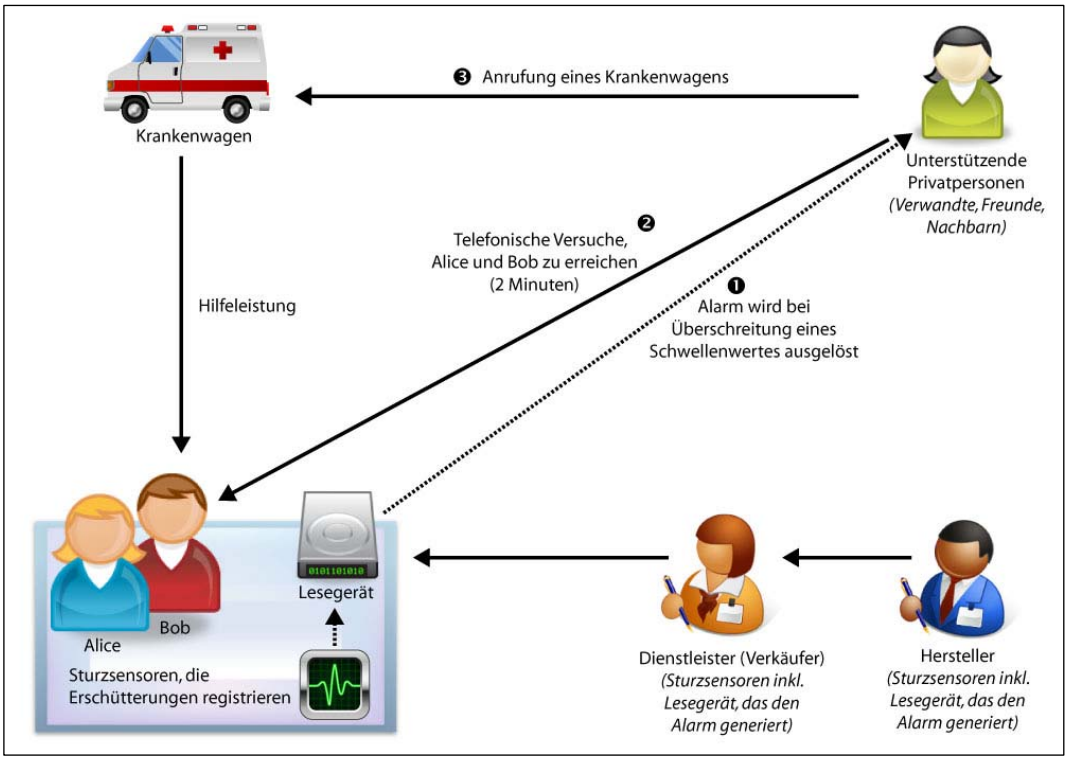


Abb. 2: Szenario 2: „Notfallhilfe von lieben Verwandten“

[3] Dieses und das folgende Szenario sind zu einem guten Teil dem Report „Verkettung digitaler Identitäten“ des Unabhängigen Landeszentrums für Datenschutz in Zusammenarbeit mit der Technischen Universität Dresden im Auftrag des Bundesministeriums für Bildung und Forschung, 2007 (https://www.datenschutzzentrum.de/projekte/verkettung/), S. 202 ff., entnommen. Die weiteren Szenarien haben sich aus der Analyse der Kurzbeschreibungen der 18 geförderten Projekte ergeben.

2.1.3 Szenario 3: „Notfallhilfe durch einen professionellen Dienstleister“

In Fußmatten auf dem Boden sind wie in dem vorherigen Szenario Sturzsensoren eingebaut: Diese registrieren die Erschütterungen, die bei einem Sturz auftreten. Ein Lesegerät liest über Funk in kurzen Abständen die von den Sensoren gemessenen Werte aus. Wird dabei ein festgelegter Schwellenwert überschritten, wird ein Alarm ausgelöst. Das System informiert in diesem Fall **selbstständig die Notfallzentrale des Anbieters**. Durch die übermittelte Kennung wissen die Mitarbeiter sofort, bei welchem Kunden der Alarm ausgelöst wurde. Alice und Bob haben mit dem Anbieter einen abgestuften Alarmierungsplan vereinbart. Bevor dieser einen Krankenwagen ruft, wird zwei Minuten lang versucht, Alice oder Bob telefonisch zu erreichen.

Der Anbieter bestätigt zudem, dass das System nicht zwischen dem Sturz eines Menschen und einem schweren, heruntergefallenen Gegenstand unterscheiden kann. Wenn Alice das Bewusstsein verliert, muss es nicht zwangsläufig zu einem Sturz kommen. Trotzdem wird sie auch in diesen Fällen vielfach dringend auf eine ärztliche Versorgung angewiesen sein. **Deshalb wollen Alice und Bob ihr Notfallsystem um eine Bewegungsfunktion erweitern lassen. Dabei nehmen vier in der Wohnung verteilte Kameras Bewegungen auf** (siehe Abb. 3). Das System ist intelligent und kann die Bewegungsmuster und Tagesabläufe der Bewohner lernen. Auffällige Bewegungen, die auf ein gesundheitliches Problem hindeuten, oder Situationen, in denen sich die Bewohner gar nicht mehr bewegen, erkennt das System selbstständig. Es ist allerdings noch nicht gelungen, Schlaf von Bewusstlosigkeit zu unterscheiden. Daher ist auch für diese Funktion eine Abstufung eingeplant. Bevor bei Bewegungslosigkeit ein Alarm ausgelöst wird, sendet die Anlage ein akustisches Signal. Alice und Bob haben dann zwei Minuten Zeit, die Alarmierung der Zentrale zu verhindern. Dazu können sie entweder einen Knopf am Schaltkasten des „Safe Home“-Systems oder aber einen Knopf an dem zusätzlichen Notrufarmband, das beide tragen, betätigen.

Die Kamerabilder werden nicht an den Anbieter übermittelt und auch nicht aufgezeichnet. Stattdessen findet eine Echtzeitauswertung statt, um auffälliges Verhalten zu erkennen, das von den vom System erlernten Gewohnheiten der Bewohner abweicht. Wie das genau funktioniert, wissen Alice und Bob zwar nicht. Aber sie sind zufrieden, weil sie selbst im Falle eines Alarms eingreifen können, falls das System etwas falsch bewertet hat.

Der Anbieter bietet das System auch in einer zweiten Konfiguration an: Wenn dabei nicht innerhalb von zwei Minuten die Alarmübermittlung verhindert wird, werden die von den Kameras erfassten Bilder an die Zentrale übertragen, damit die Mitarbeiter sehen können, ob ein Notfall vorliegt. Damit soll eine Fehlalarmierung von Sicherheitskräften verhindert werden. Die Vorstellung, dass unvermittelt Fremde einen Blick in ihr Wohnzimmer werfen können, gefiel Alice und Bob nicht, weshalb sie sich dagegen entschieden.

Beteiligte: Betroffene(r) Nutzer, unterstützendes Dienstleistungsunternehmen

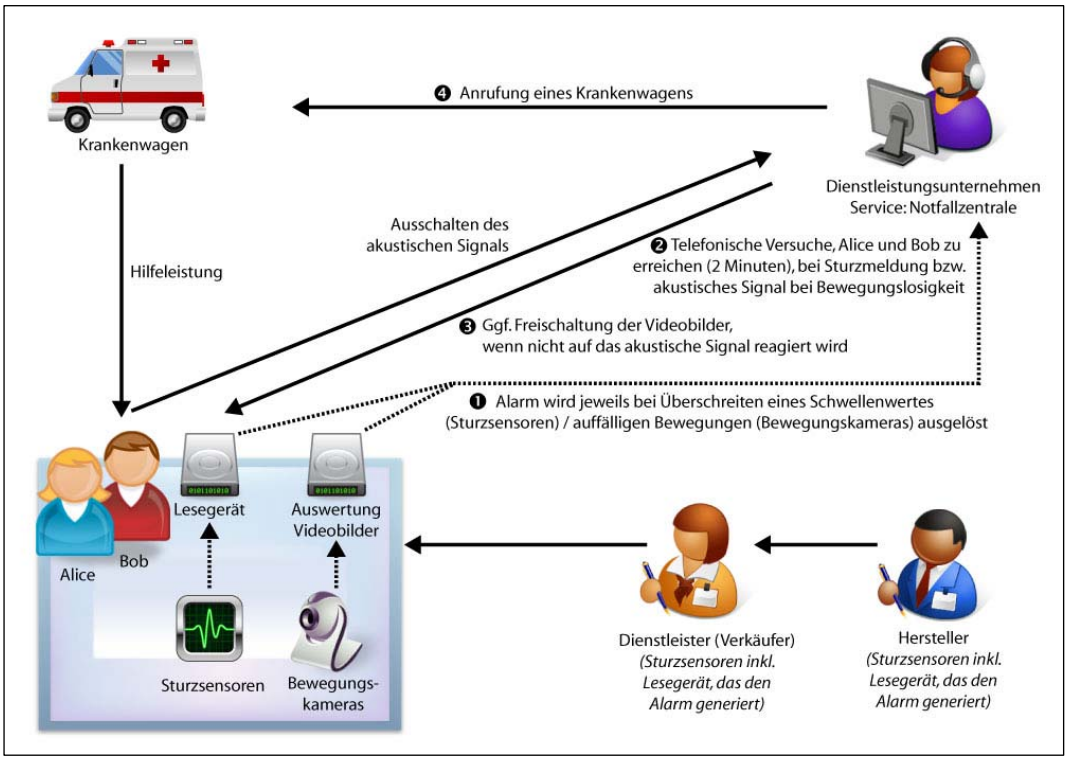


Abb. 3: Szenario 3: „Notfallhilfe durch einen professionellen Dienstleister“

2.1.4 Szenario 4: „Fernbetreuung durch den Hausarzt“

Bob leidet in letzter Zeit vermehrt unter gesundheitlichen Beschwerden. Deshalb hat ihm sein Hausarzt vorgeschlagen, **Vitalsensoren zu nutzen**, die die Werte seines Blutdrucks, seines Gewichts und seines Blutzuckers laufend aufzeichnen.[4] Als Steuerungsgerät dient das Fernsehgerät. Über das Fernsehgerät wird ein rückkanalfähiges Breitbandkabel mit der Service-Plattform des Dienstleistungsanbieters verbunden (siehe Abb. 4). Hier werden die gemessenen und automatisch übermittelten Daten mit Einwilligung von Bob in einer elektronischen Gesundheitsakte abgelegt. Dort stehen sie für den Zugriff durch den Hausarzt sowie das medizinische Betreuungscenter, in dem sein Hausarzt arbeitet, zur Verfügung.[5] Dadurch bleibt die vorhandene Patient-Arzt-Beziehung zu seinem Hausarzt bestehen, nur der Kontakt wird verstetigt und vereinfacht. Hinzu kommt eine Alarmierungsfunktion, wenn die gemessenen und automatisierten Daten bestimmte Schwellenwerte überschreiten. In einem solchen Fall wird zum einen Bob selbst durch das System automatisiert unterrichtet und an ggf. fehlende Medikamenteneinnahme erinnert. Bei bestimmten Werten, die Anlass für ein schnelles Einschreiten eines Arztes geben, wird außerdem der Hausarzt alarmiert.

---

[4] Hartmann / Fiebig, in: BUS-Systeme, Berlin, 17. Jahrgang, 2010, S. 252 ff.: Dabei werden funkbasierte Techniken z.B. Bluetooth oder ZigBee, GSM oder GPRS genutzt. Der Aufsatz ist abrufbar unter: http://www.wohnselbst.de/downloads/WohnSelbst%20in%20Bussysteme%201_2010_Hartmann_Fiebig.pdf.

[5] Hartmann / Fiebig, in: BUS-Systeme, Berlin, 17. Jahrgang, 2010, S. 252 ff.

Beteiligte: Betroffene(r) Nutzer, Unterstützer aus dem medizinischen Bereich

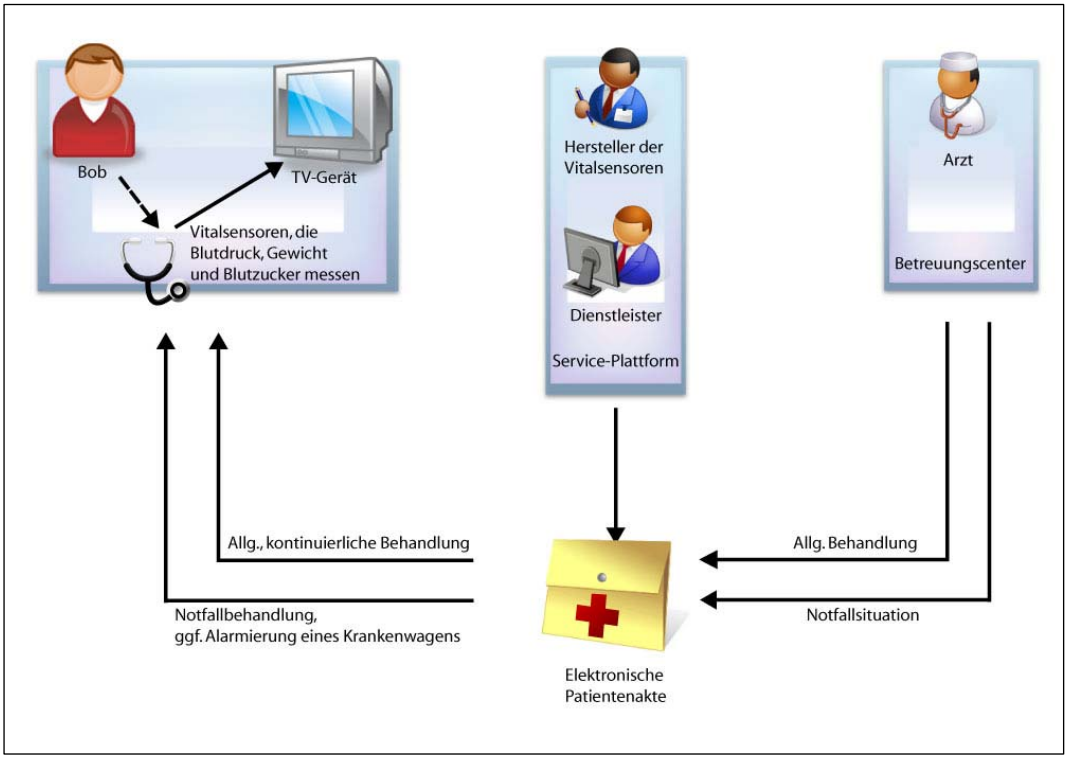


Abb. 4: Szenario 4: „Fernbetreuung durch den Hausarzt“

2.1.5 Szenario 5: „Betreuung im Pflegeheim mit Fernbetreuung durch den Hausarzt, finanzierbar dank der Übernahme der Kosten durch die Pflegekasse“

Alice und Bob sind mittlerweile in eine Pflegeeinrichtung umgezogen. Dort haben sie zusammen ein Apartment und fühlen sich rundum gut betreut. In ihrem Apartment und in ihren Betten werden **Sensoren installiert, die drahtlos das Schlaf- und Wachverhalten und die Bedienung der Haushaltsgeräte erfassen sowie Atmung und Puls messen** (siehe Abb. 5). Die Daten werden von einer Home-Station aufbereitet und über eine Kommunikationsverbindung an das Pflegepersonal weitergeleitet. So hat das Pflegepersonal jederzeit einen Überblick über schleichende gesundheitliche Veränderungen. Zugleich kann es im Notfall rechtzeitig eingreifen. Um den Dokumentationsprozess und die Abrechnung von pflegerischen Leistungen zu verbessern, werden von den gemessenen Daten automatisch die abrechnungsrelevanten Daten in einer gesonderten Abrechnungsdokumentation erfasst. Das Pflegepersonal ergänzt diese manuell um zusätzlich erforderliche Daten, bevor die Dokumentation zwecks Kostenersatzes bei der Pflegekasse von Alice und Bob eingereicht wird.

Beteiligte: Betroffene(r) Nutzer, Unterstützer aus dem pflegerischen Bereich, Pflegekasse

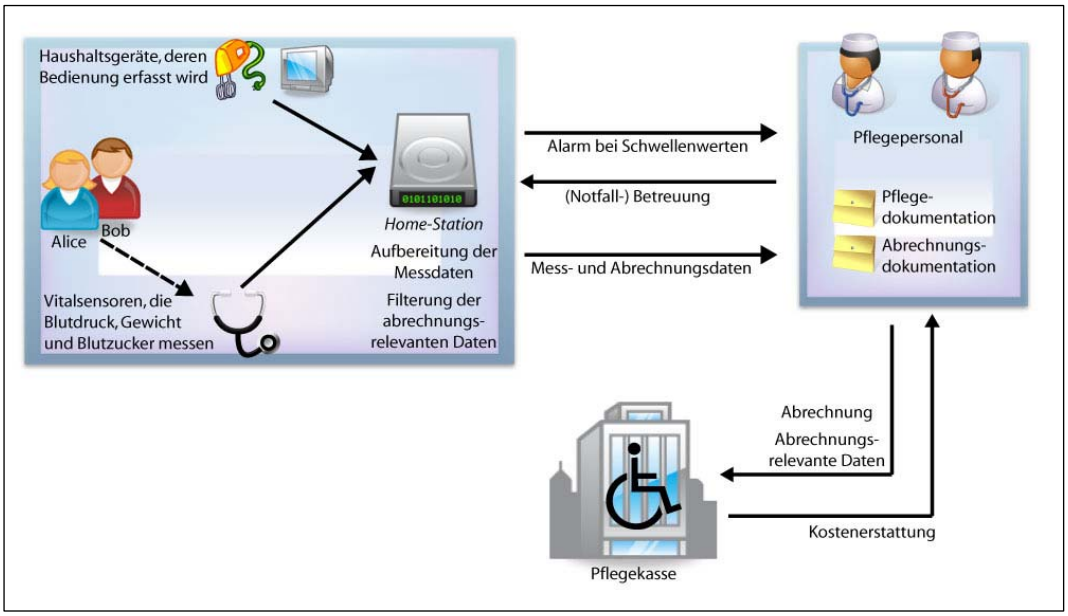


Abb. 5: Szenario 5: „Betreuung im Pflegeheim mit Fernbetreuung durch den Hausarzt“

2.1.6 Szenario 6: „In der Freizeit gut versorgt – zu Hause und unterwegs – und nicht mehr einsam“

Alices und Bobs Gesundheitszustand erlaubt es ihnen wieder, in ihrem Haus zu leben. Bob nutzt weiterhin Vitalsensoren, die die Werte seines Blutdrucks, seines Gewichts und seines Blutzuckers laufend aufzeichnen.[6] Die Datenauswertung erfolgt auf einem Minicomputer, der die Daten an die Service-Plattform ihres Dienstleistungsanbieters überträgt. Neuerdings haben Alice und Bob von ihrem Dienstleistungsanbieter das Angebot erhalten, weitere Dienstleistungen zu nutzen. Alice und Bob gehen aufgrund ihrer abnehmenden Mobilität immer seltener aus dem Haus, so dass sie angefangen haben, die **Service-Plattform auch für andere Online-Dienste**, z.B. für Bestellungen von Waren über ein Portal, zu nutzen (siehe Abb. 6). Außerdem möchten sie das Angebot nutzen, sich in einem sozialen Netzwerk für Senioren (genannt „SeniorenVZ“) anzumelden, um Kontakt mit anderen Senioren zu erhalten und vielleicht alte Bekannte ausfindig zu machen, die sie im Laufe des Lebens aus den Augen verloren haben. Da ihr Freundeskreis in letzter Zeit kleiner geworden ist, haben sich Alice und Bob von ihrer Tochter einen Account auf dem Portal „SeniorenVZ“ einrichten lassen. Darüber haben sie bereits viele Kontakte geknüpft.

[6] Hartmann / Fiebig, in: BUS-Systeme, Berlin, 17. Jahrgang / 2010, S. 252 ff.

Da sie von dieser Art der Kommunikation begeistert waren, haben sie sich auch eine bildgestützte Kommunikation einrichten lassen. Zwischenzeitlich haben sie zwar keine Bilder empfangen können, aber ihr Dienstleister hat dieses Problem per Ferndiagnose umgehend gelöst. Alice und Bob haben sich außerdem über ihren Telekommunikationsanbieter bei einem Service angemeldet, der ihnen auf ihr Handy Produktinformationen zu den Läden übermittelt, in deren Nähe sie sich gerade befinden. Weiterhin haben sie einen Service beantragt, mit dem sie über ihr Handy direkt ohne explizite Angabe einer Adresse jederzeit ein Taxi bestellen können – die notwendigen Informationen über ihren Standort werden automatisch mit Hilfe des Handys ermittelt. So sind Alice und Bob sich sicher, dass sie bei ihren Unternehmungen immer wieder sicher nach Hause kommen.[7] Allerdings stört sie, dass sie, seit sie sich bei dem Service angemeldet haben, ständig Werbe-SMS auf ihr Handy erhalten.

Beteiligte: Betroffene(r) Nutzer, Telediensteanbieter, Telekommunikationsanbieter, Auftragnehmer der Dienstleister

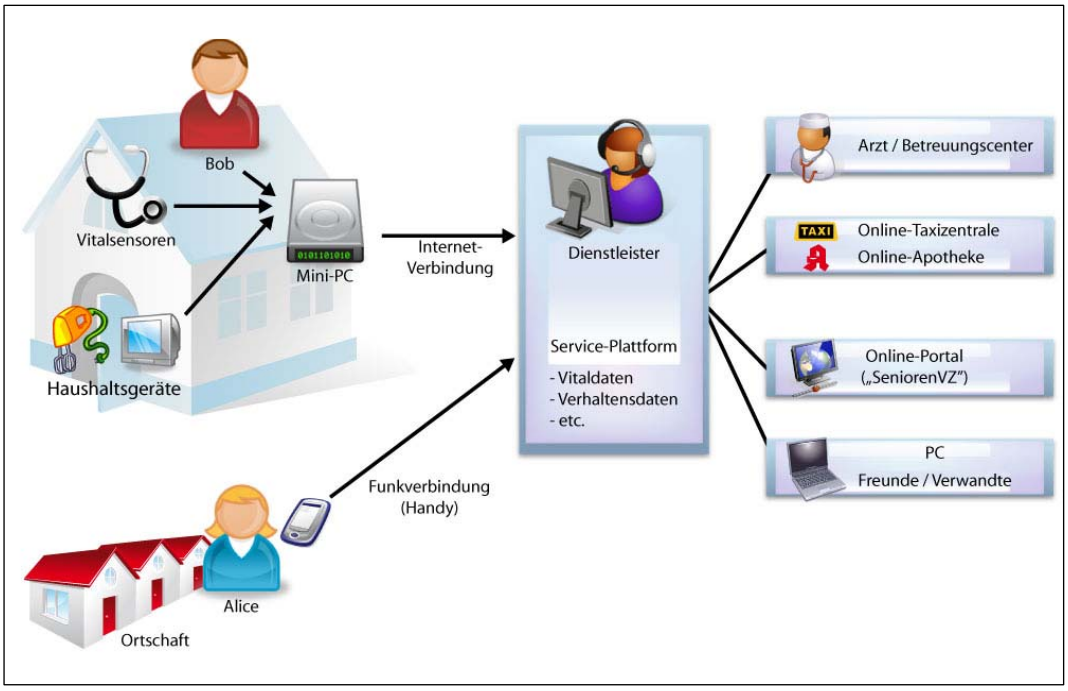


Abb. 6: Szenario 6: „In der Freizeit gut versorgt, zu Hause und unterwegs“

[7] Siehe z.B. das im Rahmen der BMBF-Fördermaßnahme „Altersgerechte Assistenzsysteme für ein gesundes und unabhängiges Leben – AAL“ geförderte Projekt SmartAssist – Plattform zur Unterstützung von sozialen und gesundheitlichen Aspekten bei der Gestaltung eines altersgerechten autonomen Lebens. Koordinator: Lübecker Wachunternehmen Dr. Kurt Kleinfeldt GmbH, Homepage: http://www.itm.uni-luebeck.de/projects/smartassist/.

2.1.7 Szenario 7: „Anfragen von Strafverfolgungsbehörden, Versicherungen und Forschungseinrichtungen“

Alice und Bob nehmen regelmäßig an virtuellen Kaffeerunden teil, bei denen die Teilnehmer durch Videokonferenz miteinander verbunden sind und sich über die verschiedensten Themen austauschen. Einer ihrer neuen Bekannten ist jedoch etwas eigenwillig und unbeherrscht. In den Diskussionen kommt es wiederholt zu hitzigen Wortgefechten, in denen dieser Bekannte schon mal unhöflich und (fast) beleidigend wird. Eines Tages erhalten Alice und Bob die Mitteilung, dass die Videoaufnahmen von der Kaffeerunde an einem bestimmten Tag von den Strafverfolgungsbehörden beschlagnahmt wurden, weil ein Teilnehmer Strafanzeige wegen Beleidigung gestellt hat.

Auch haben Alice und Bob ein Schreiben von ihrer Hausratsversicherung bekommen. Denn im letzten Urlaub ist bei ihnen eingebrochen worden. Die Versicherung fordert nun einen Nachweis darüber, dass die Rollläden auch im Urlaub heruntergelassen worden waren, und verlangt die Übersendung der diesbezüglich in ihrem Hausautomationssystem gespeicherten Daten. Außerdem haben sie noch ein Schreiben von einem Forschungsinstitut erhalten, das sie um die Teilnahme an einer Studie bittet, die die Verhaltensdaten von AAL-Nutzern auswertet – in personenbezogener oder in anonymer Form (siehe Abb. 7). An dem Forschungsprojekt beteiligt sind auch die Krankenkassen, die sich durch die Auswertungen Erkenntnisse für die Steuerung der Gesundheitsvorsorge erhoffen.

Beteiligte: Betroffene(r) Nutzer, Strafverfolgungsbehörden, Versicherungen, Forschungseinrichtungen

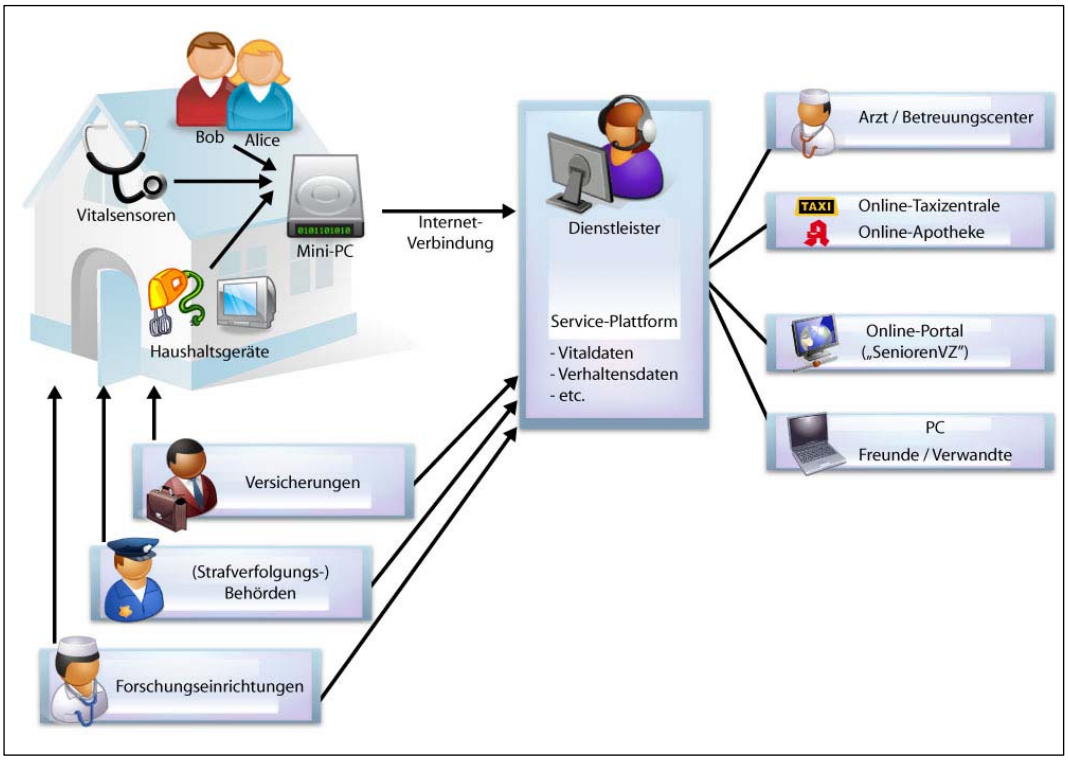


Abb. 7: Szenario 7: „Anfragen von Strafverfolgungsbehörden, Versicherungen und Forschungseinrichtungen“

2.2 Anwendungsbereiche

Wie die oben dargestellten Szenarien illustrieren, reicht die Bandbreite technischer Assistenz von kleineren Erleichterungen beim Verrichten der alltäglichen Dinge des Lebens bis hin zu komplexen technischen und vernetzten Systemen. Dabei kann in ihrer Funktionalität und Komplexität zwischen Low-, Medium- und High-Technology-Systemen unterschieden werden.[8] Die Vernetzung innerhalb des häuslichen Bereichs kann sich auf wenige oder aber eine Vielzahl von Gegenständen einbeziehen. Der Wirkungsbereich der Anwendung kann sich auf den häuslichen Bereich beschränken oder auch eine Vielzahl von außerhäuslichen Dritten einbeziehen. Eine Vernetzung nach außen kann eine Telefonverbindung zum Nachbarn bedeuten, eine Kommunikationsverbindung zu Service-Einrichtungen oder zu globalen Systemen wie dem Internet. Entsprechend vielfältig sind die Anwendungsbereiche. Unter den möglichen Anwendungsbereichen haben die folgenden eine große Relevanz:

1. Sicherheit

Bereits Alarmsysteme und andere Schutzvorrichtungen gegen Einbrüche können zum AAL-Bereich gehören. Hier geht es um die Erkennung von und Warnung vor Gefahren, ohne dass die Privatsphäre oder Bewegungsfreiheit der Bewohner eingeschränkt werden.

2. Haushalt

Steuerungssysteme für häusliche Komponenten zur kontextabhängigen Beleuchtung oder Raumtemperatur, die auch im „Smart Living“ eine Rolle spielen, können im Sinne des AAL die Bewohner unterstützen.

3. Gesundheit

Menschen werden dabei unterstützt, möglichst unabhängig zu Hause leben zu können, auch wenn sie gesundheitlich temporär oder permanent eingeschränkt sind. Zu den eingesetzten AAL-Systemen gehören Anwendungen zur Teleüberwachung für Notfälle, Telemedizin oder Roboter zur Unterstützung im Alltag.

4. Pflege

Auch hier geht es darum, Menschen dabei zu unterstützen, möglichst unabhängig zu Hause bleiben zu können. Im Vordergrund stehen jedoch vermehrt die Entlastung der Betreuenden sowie ein Einsatz in Pflegeeinrichtungen, wobei die Anwendungen ähnlich wie im medizinischen Bereich konzipiert sind (z.B. Notrufsystem, Monitoringsystem).

---

[8] Driller et al., Ambient Assisted Living, Technische Assistenz für Menschen mit Behinderung, 2009, S. 33.

5. Prävention und Rehabilitation

Menschen werden hier zumeist mit einem Bewegungs- und Ernährungsprogramm unterstützt. Zum Beispiel können Aktivitätsmonitore und Waagen mit einem direkten Feedback zu mehr Bewegung und besserer Ernährung motivieren. Mit Hilfe von Softwareprogrammen und Heimtrainern kann eine Datenübertragung an ein Kompetenzzentrum erfolgen und die stationäre Rehabilitation fortgesetzt werden.

6. Soziales Umfeld

AAL-Assistenzsysteme können auch Menschen bei der Teilnahme am gesellschaftlichen Leben und in ihrem sozialen Umfeld unterstützen. Dazu gehören beispielsweise das Management der persönlichen Kontakte, Hilfe bei der Kommunikation mit anderen und das Nutzen kollaborativer Möglichkeiten über das Internet wie E-Learning, E-Demokratie, lokale Kommunikationsportale oder soziale Netzwerke.

7. Lifestyle

Hierbei geht es im Wesentlichen um die Nutzung von Diensten, die über die modernen Kommunikationswege erreichbar sind, so zum Beispiel die Bestellung von Waren über Online-Portale oder die Bestellung eines Taxis mit Hilfe von Standortdaten.

2.3 Die Beteiligten

Je nach Anwendungsbereich und technischer Realisierung der AAL-Anwendung sind verschiedene Beteiligte involviert. Im Folgenden werden typische beteiligte Rollen aufgeführt, die auch in den weiteren Ausführungen von Relevanz sind:

- **Die unmittelbaren Nutzer,** d.h. Personen, die in ihrer häuslichen Umgebung oder in ihrem nahen Umfeld AAL-Anwendungen in Anspruch nehmen möchten. Dazu gehören sowohl Personen, die auf diese Anwendungen angewiesen sind, als auch solche, die nicht darauf angewiesen sind, oder aber Nutzer, die auf diese Anwendungen angewiesen sind **(ältere Menschen).**
- **Die Unterstützenden aus dem privaten Bereich,** d.h. Personen, die eine Verbesserung oder Erleichterung ihrer Betreuung/Hilfestellung durch die AAL-Anwendung erfahren **(Angehörige, Freunde, Nachbarn).**
- **Die Unterstützenden aus dem medizinischen Bereich,** d.h. Personen, die eine Verbesserung oder Erleichterung ihrer medizinischen Arbeit/Dienstleistung durch die AAL-Anwendung erfahren **(Ärzte oder Arztpraxen, Krankenhäuser und Apotheken).** Die medizinischen Leistungserbringer haben eine zentrale Rolle bei der Versorgung von Pa-

tienten/Kunden mit AAL-Anwendungen, die medizinische Hilfsmittel und Dienstleistungen darstellen, die jedoch, damit eine Abrechnung mit den Sozialversicherungen möglich ist, zuvor entsprechend anerkannt sein müssen.[9]

- **Die Unterstützenden aus dem pflegerischen Bereich,** d.h. Personen, die eine Verbesserung oder Erleichterung ihrer pflegerischen Arbeit/Dienstleistung durch AAL-Anwendungen erfahren (Pflegedienste und Pflegeeinrichtungen). In diesem Bereich ist besonders die hohe Arbeitsbelastung Motivation dafür, AAL-Anwendungen einzusetzen (z.B. Notruf- und Monitoringsysteme, die die Pflegekräfte entlasten sollen).
- **Die Unterstützenden aus dem allgemeinen Dienstleistungssektor,** d.h. Personen, die über die AAL-Anwendungen ihre nicht-medizinischen und nicht-pflegerischen Dienstleistungen anbieten, z.B.
  - Wachunternehmen, die einen Notfallservice anbieten,
  - Wohnungseigentümer, die ihre Wohnungen mit AAL-Anwendungen anbieten,
  - Unternehmen, die ihre Waren online anbieten oder Kommunikationsplattformen zur Verfügung stellen.
- **Die Unterstützenden der Dienstleister (also Dienstleister der Dienstleister),** häufig Planer, Architekten, Ingenieure, Handwerker und insb. Techniker, d.h. Personen, die die AAL-Infrastruktur, d.h. oftmals die Heimvernetzung planen, einrichten und pflegen und damit „Dienstleister der AAL-Dienstleister“ sind.
- **Die Sozialversicherungen (Krankenversicherung, Pflegeversicherung, aber auch Unfall- und Rentenversicherung),** die ggf. die Kosten der Anwendungen tragen und von einer eventuellen Kostenreduzierung durch AAL-Anwendungen insbesondere im medizinischen und pflegerischen Bereich profitieren. AAL-Anwendungen, die älteren Menschen ermöglichen, länger zu Hause leben zu können und medizinische Leistungen zu Hause erhalten, können dabei die Gesundheitsversorgung verbessern und kostengünstiger machen. Die Sozialversicherungen könnten daneben unabhängig von der Frage der Kostenerstattung auch Interesse an Daten und Auswertungen im Zusammenhang mit AAL-Anwendungen haben, um Erkenntnisse für die Steuerung des Gesundheitssystems zu gewinnen.
- **Technik- und Gerätehersteller,** die die AAL-Anwendung konzipieren und entwickeln. Sie kommen insbesondere aus den Bereichen Medizingeräte, Haushaltsgeräte, Kommunikationssysteme und Mikrosysteme.
- Unternehmen und Behörden, die ein Interesse an den durch AAL-Anwendungen gewonnenen Daten haben (Versicherungen, Strafverfolgungsbehörden).

[9] Siehe dazu Kapitel 6 zu Sozialversicherungsrecht.

- **Einrichtungen von Wissenschaft und Forschung:** AAL-Anwendungen erzeugen eine bisher nicht verfügbare Vielzahl von Daten, die für die Forschung (u.a. soziologische, medizinische, versicherungswissenschaftliche Forschung) von hoher Bedeutung sein können. Zugleich erfordert bereits der Einsatz von AAL-Anwendungen wissenschaftliche Begleitung, so im ethischen, rechtlichen und sozialwissenschaftlichen Bereich.[10]

Zusätzliche Beteiligte, deren Aufgaben und Interessen in der weiteren Betrachtung dieser Vorstudie nicht vertieft erörtert werden, sind beispielsweise die folgenden:

- **Sozial- und Seniorenverbände** als Interessenvertreter der die AAL-Anwendungen nutzenden Personen.
- **Politik** als Förderer der Entwicklung altersgerechter Assistenzsysteme und Verantwortlicher, gesetzliche Rahmenbedingungen für den Einsatz von AAL-Anwendungen zu schaffen.

2.4 Die Rechtsbeziehungen der Beteiligten untereinander

Die Rechtsbeziehungen der o.g. Beteiligten können vielfältig sein. So kann der Einsatz allein zwischen dem Nutzer und einem AAL-Dienstleister vereinbart sein. Dabei kann sich der Dienstleister bei der Erbringung seiner Leistung eines Dritten, z.B. zwecks Installation oder Wartung des Systems, bedienen. Auf Seiten des Nutzers kann die angebotene Leistung z.B. die Anbindung an das Internet voraussetzen, wenn diese nicht in dem Angebot des Dienstleisters inbegriffen ist. Hinzu kommt in diesem Fall auf Seiten des Nutzers eine Rechtsbeziehung zu einem Telekommunikationsanbieter. Eine AAL-Dienstleistung kann auch Privatpersonen und weitere Dienstleister einbeziehen, so dass Mehrpersonenverhältnisse entstehen.

Im medizinischen und pflegerischen Bereich kommen die Besonderheiten des Gesundheitssystems hinzu. Hier besteht eine vertragliche Beziehung zum Arzt, zum Krankenhaus und/oder zur Pflegeeinrichtung, wobei das jeweilige zivilrechtliche Verhältnis von den Vorschriften des Sozialgesetzbuches (SGB) überlagert wird.

Es sind daher exemplarische Beziehungen gewählt worden, anhand derer die relevanten Fragen aufgeworfen werden. Die Rechtsbeziehungen werden im Folgenden aufgeteilt in grundlegende Rechtsbeziehungen (siehe Abschnitt 2.4.1), Rechtsbeziehungen in Bezug auf die telekommunikative Infrastruktur (siehe Abschnitt 2.4.2) sowie Rechtsbeziehungen im medizinischen oder pflegerischen Bereich (siehe Abschnitt 2.4.3).

[10] Vgl. auch: Das AALmagazin, Informationen zu intelligenten Assistenzsystemen für ein selbstbestimmtes Leben im Alter, Heft 1/2010, Beitrag „AAL geht viele an“, S. 10 f. sowie BMBF/VDE, Innovationspartnerschaft AAL, Zielgruppen für AAL-Technologien und -Dienstleistungen, abrufbar unter: http://www.vde.de/de/Technik/AAL/Publikationen/Kongress-undFachbeitraege/documents/zielgruppen%20f%C3%BCr%20aal%20_tabelle_.pdf.

2.4.1 Grundlegende Rechtsbeziehungen der Nutzer

Zu den wichtigsten grundlegenden Rechtsbeziehungen aus Sicht der Nutzer gehören die Verhältnisse „Nutzer – AAL-Diensteanbieter“ (hier zunächst beschränkt auf den nicht-medizinischen und nicht-pflegerischen Bereich), „Nutzer – Hersteller“ sowie „Nutzer – unterstützende Privatperson“, wie im Folgenden erläutert.

- **Verhältnis „Nutzer – AAL-Diensteanbieter“ im nicht-medizinischen und nicht-pflegerischen Bereich**

  Der Nutzer entscheidet sich für eine AAL-Dienstleistung bei einem Anbieter und schließt mit diesem direkt einen Vertrag ab. Die konkrete vertragsrechtliche Einordnung hängt von der angebotenen Leistung ab. In Betracht dürfte im Regelfall ein Kauf-, Werk-, Dienstleistungs- oder Mietvertrag kommen. Geht es dem Nutzer wie im Szenario 1 um den Erwerb und Einsatz einer Heimautomation, so liegt ein Kaufvertrag nach § 433 Bürgerliches Gesetzbuch (BGB) vor mit den sich daraus anschließenden rechtlichen Folgen.[11]

  Für einen AAL-Dienstleistungsanbieter gilt dagegen Werkvertragsrecht, wenn er sich verpflichtet, eine Sache herzustellen, zu verändern oder einen anderen Erfolg, wie das Funktionieren eines technischen Systems, herbeizuführen. Unter die typischen Einsatzgebiete des Werkvertrags fallen beispielsweise die Herstellung eines den individuellen Bedürfnissen des Nutzers entsprechenden Programms, die Anpassung von (gekaufter) Standardsoftware an die individuellen Bedürfnisse des Nutzers, die Herstellung und Einrichtung eines EDV-Terminals mit Standardprogrammen, das Erfassen von betrieblichen Daten sowie die Reparatur und Wartung von Hard- und Software. Liegt der Hauptteil der vertraglich vereinbarten Leistung daher in der Erstellung und Implementierung eines „AAL-Konzepts“ für eine Wohnung mit Einbindung in ein Netz, so bekommt der Vertrag einen werkvertraglichen Charakter.[12] Soweit jedoch die Lieferung der herzustellenden Sache im Vordergrund steht, findet wiederum Kaufrecht Anwendung (§ 651 BGB).

  Ein Dienstvertrag liegt dagegen vor, wenn die Erbringung von Diensten durch eine Vertragspartei geschuldet ist. Denkbar ist auch ein Mietvertrag zwischen dem Nutzer und dem Anbieter, wenn die Leistung in der vorübergehenden Überlassung von Geräten wie Sensoren und Lesegeräten liegt.

  Erfolgt der Vertragsschluss zwischen dem Nutzer und dem Anbieter unter ausschließlicher Verwendung von Fernkommunikationsmitteln, dann gelten die Vorschriften der §§ 312b ff. BGB. Die rechtliche Einordnung der Vertragsform hängt auch hier von der

[11] Beispiele: „Heimautomation“, „Sturzüberwachung bei einem Wachunternehmen“.

[12] Vgl. dazu im Zusammenhang mit der Installation einer Netzinfrastruktur: LG Köln, Urteil vom 16.07.2003, 90 O 68/01.

Ausgestaltung im Einzelfall ab. Ist beispielsweise der Vertrag auf das Lesen des Inhalts der Datenbank auf dem Bildschirm beschränkt, kann dies dem „Kauf" von Informationen entsprechen (z.B. bei einem Informationsangebot für pflegende Personen) mit der Folge der Einordnung unter den Vorschriften des Kaufrechts nach §§ 433 ff. BGB. Verpflichtet sich der Anbieter jedoch zum dauerhaften Bereithalten der Daten zum Abruf, steht der Dienstleistungs- und Dauerschuldcharakter im Vordergrund, weshalb eine Anwendung des Dienstvertragsrechts nach §§ 611 ff. BGB gerechtfertigt sein kann. In Betracht kommt wiederum auch ein Werkvertrag nach §§ 631 ff. BGB, wenn es um die Herbeiführung eines bestimmten Erfolges geht.

Zusätzlich finden jeweils die § 312b ff. BGB Anwendung, d.h. die besonderen Bestimmungen zu den sog. Fernabsatzverträgen. Dies hat zur Folge, dass der Nutzer ein Widerrufs- und besonderes Rückgaberecht hat und dem Händler besondere Informationspflichten obliegen. Ferner finden die Vorschriften des Telemediengesetzes Anwendung, die u.a. besondere Informationsregeln, Datenschutznormen und Haftungsvorschriften enthalten.[13]

- **Verhältnis „Nutzer – Hersteller"**

  Mit dem Hersteller der AAL-Technik besteht seitens des Nutzers nur dann eine vertragliche Beziehung, wenn er mit diesem direkt eine Rechtsbeziehung eingeht, z.B. direkt mit diesem ein Kaufvertrag abschließt. Im Regelfall dürfte jedoch keine vertragliche Beziehung vorliegen, da die Anwendung zumeist vom Verkäufer/Händler/Dienstleister erworben wird.[14] Der Hersteller kann jedoch haftungsrechtlich dem Nutzer verpflichtet sein, wenn dieser wegen eines Konstruktions- bzw. Fabrikationsfehlers der gelieferten Geräte einen Schaden erleidet oder der Hersteller seine Instruktionspflichten oder Produktbeobachtungspflichten verletzt.

- **Verhältnis „Nutzer – unterstützende Privatperson"**

  Mit der unterstützenden Privatperson, d.h. beispielsweise mit der Tochter oder der Nachbarin, besteht ein Gefälligkeitsverhältnis. Eine Gefälligkeit im unverbindlichen Sinn ist das Bereiterklären zur Vornahme einer Handlung aus freundschaftlichen, nachbarschaftlichen oder familiären Motiven, ohne dass für den anderen ein vertraglicher Anspruch begründet wird. Kennzeichnend für eine Gefälligkeit ist, dass kein **Rechtsbindungswille** besteht.[15] Das Fehlen des Rechtsbindungswillens ist anhand **objektiver** Kriterien im Einzelfall zu ermitteln. Indizien dafür sind die Art der Gefällig-

---

[13] Zusammenfassend: Hoeren, Das Telemediengesetz, NJW 2007, S. 801 ff.

[14] In Betracht kommt eine verschuldensunabhängige Haftung auf Schadensersatz aus dem Produkthaftungsgesetz, welche keine vertragliche Beziehung des Herstellers zum Kunden voraussetzt (Herstellerhaftung) sowie verschuldensabhängige Schadensersatzansprüche aus § 823 BGB.

[15] BGHZ 21, 102.

keit, ihr Grund und Zweck, die wirtschaftliche und rechtliche Bedeutung für die Beteiligten, die Interessenlage der Beteiligten, die dem Begünstigten drohenden Gefahren und Schäden bei fehlerhafter Leistung sowie ein unverhältnismäßiges Haftungsrisiko des Leistenden.[16]

Die Auferlegung bzw. Vereinbarung einer Interventionspflicht mit einer Privatperson in Form eines zivilrechtlichen Auftrages oder Gefälligkeits**vertrags** ist weder anzuraten noch sachgerecht, weil die Privatperson insbesondere haftungsrechtlich in einer unzumutbaren Verantwortung wäre.

2.4.2 Rechtsbeziehungen für die Bereitstellung der Telekommunikationsinfrastruktur

Die für AAL-Anwendungen notwendige Datenfernübertragung bedarf einer telekommunikativen Infrastruktur, d.h. einer Übertragung über das Telefonnetz oder eine Funkverbindung.

- **Verhältnis „Nutzer – Anbieter von Telekommunikationsdienstleistungen“**

  AAL-Anwendungen setzen grundsätzlich eine Vernetzung zu Service-Einrichtungen und damit eine Anbindung an Kommunikationssysteme wie z.B. das Internet voraus. Diese Anbindung kann in der Leistung des AAL-Dienstleistungsanbieters enthalten sein oder wird beim Nutzer vorausgesetzt. Hinzu kommt eine Rechtsbeziehung des Nutzers zu einem Telekommunikationsanbieter. Im Hinblick auf die Rechtsnatur des Vertrags zwischen einem Endkunden und dem Anbieter von Telekommunikationsdienstleistungen werden verschiedene Vertragstypen diskutiert. Es könnte sich um einen Werkvertrag nach §§ 635 ff. BGB handeln, um einen Mietvertrag nach §§ 535 ff. BGB, einen Dienstvertrag nach § 611 BGB oder einen Vertrag „sui generis“. Bei Festnetzverträgen handelt es sich zum Beispiel um sogenannte gemischt-typische Verträge, weil sie keinem im BGB geregelten Vertragstyp alleine zugeordnet werden können. So weist ein Festnetzvertrag mietvertragsähnliche Elemente hinsichtlich der Überlassung des Telefonanschlusses auf. Andererseits besteht eine werksvertragsähnliche Natur hinsichtlich der Herstellung von Telefonverbindungen (erfolgreicher Verbindungsaufbau wird geschuldet). Daneben findet Telekommunikationsrecht Anwendung, das zahlreiche Verbraucherschutzvorschriften enthält, die beispielsweise die Art und Weise der Rechnung, die Sperrung von Telefonanschlüssen und den Datenschutz betreffen. Das Telekommunikationsrecht ist auf alle Übertragungswege anzuwenden. Auch hier stellen sich Haftungsfragen beim Auftreten von Fehlern auf dem Übertragungsweg.

Zusätzlich bestehen ähnliche Rechtsbeziehungen der anderen Beteiligten mit Anbietern von Telekommunikationsdienstleistungen.

---

[16] BGH NJW 74, 1705.

2.4.3 Rechtsbeziehungen im medizinischen und pflegerischen Bereich

Speziell im medizinischen und pflegerischen Bereich sind weitere Rechtsbeziehungen relevant, die juristisch gesondert zu betrachten sind.

- **Verhältnis „Nutzer – Arzt“**

  Bei der Aufnahme einer ärztlichen Behandlung kommt es in der Regel zu vertraglichen Beziehungen zwischen dem niedergelassenen Arzt und dem Patienten. Dieser Vertrag ist ein Dienstvertrag (§ 611 BGB)[17], in dem sich der Arzt verpflichtet, seine Dienste zu erbringen, d.h. die Behandlung durchzuführen. Dagegen verspricht er keinen bestimmten Erfolg.

  Außer der Behandlungspflicht ergeben sich aus dem Arztvertrag für diesen noch eine Reihe von Nebenpflichten, so die rechtzeitige Aufklärung des Patienten über Risiken der Behandlung, die Dokumentation der Behandlung und Pflege, das Gewähren von Einsicht in die Krankenunterlagen sowie die Verschwiegenheitsverpflichtung hinsichtlich anvertrauter Geheimnisse und Daten des Patienten.

  Setzt der Arzt im Rahmen seiner Behandlung AAL-Anwendungen ein, so wird im Regelfall dieser Einsatz Bestandteil des Behandlungsvertrags. Denn das Fernbehandlungsverbot, auf das noch einzugehen ist, gebietet die Einbettung der Anwendung von AAL-Technik in eine Gesamtbehandlung. Der Arzt wird sich im Regelfall an einen AAL-Anbieter wenden, um diese Leistungen seinen Patienten anbieten zu können. Er wird dann Vertragspartner des AAL-Anbieters, um seiner Leistungspflicht seinem Patienten gegenüber nachkommen zu können. Denkbar ist jedoch auch die Konstellation, dass sowohl der Patient als auch der Arzt in eine vertragliche Beziehung mit einem AAL-Dienstleistungsanbieter treten. So kann z.B. zwischen dem Nutzer und dem Dienstleister vereinbart werden, dass dieser ihm die Sensorik zur Verfügung stellt, die Daten (auch) an seinen Arzt weiterleitet und selbst die Veranlassung von Notfallmaßnahmen übernimmt.

  Das Patient-Arzt-Verhältnis wird durch das System der gesetzlichen Krankenversicherung (GKV) überlagert, wenn der Patient dort Mitglied ist[18] und der Arzt der Kassenärztlichen Vereinigung (KV) als Mitglied angehört. Die Behandlungskosten werden dann direkt mit der Krankenkasse abgerechnet, die daher die Krankenversicherungsleistungen im Regelfall als Sachleistung erbringt. Rechtsgrundlage ist im Wesentlichen das Fünfte Buch Sozialgesetzbuch – Gesetzliche Krankenversicherung (SGB V).

---

[17] Die rechtliche Einordnung der Beziehung zwischen Vertragsarzt und sozialversichertem Patienten ist umstritten. Die oben dargestellte Meinung entspricht der des BGH. Eine andere Meinung verneint das Zustandekommen eines Dienstvertrags: Der Vertragsarzt soll die ärztliche Behandlung kraft öffentlich-rechtlicher Verpflichtung gegenüber der Kassenärztlichen Vereinigung schulden. Die zivilrechtlichen Beziehungen seien vom öffentlich-rechtlich ausgestatteten Sozialversicherungsrecht überlagert.

[18] Ca. 90 % der Bevölkerung in Deutschland sind Mitglied der GKV.

Durchbrochen wird dieses Prinzip dann, wenn Eigenanteile zu zahlen sind oder wie bei Zahnersatz ein Erstattungsprinzip eingeführt wurde, nach welchem der Patient zunächst nur eine Rechtsbeziehung zum Arzt / Zahnarzt hat und die von ihm verauslagten Kosten von der Krankenkasse erstattet bekommt. Dies ist ansonsten ein typisches Strukturmerkmal der privaten Krankenversicherung, wird aber auch dort bisweilen durch Kostenzusagen direkt an Ärzte und Krankenhäuser durchbrochen. Daneben kommt es im Bereich der GKV immer mehr zum Abschluss sog. Selektivverträge, bei denen die Krankenkassen mit einzelnen Leistungserbringern besondere Bedingungen aushandeln. In die Abrechnung ist die KV dann oft nicht mehr eingebunden.

Der Vertragsarzt ist dem Patienten gegenüber durch die Übernahme der Behandlung öffentlich-rechtlich zur Sorgfalt nach den Vorschriften des bürgerlichen Rechts verpflichtet.[19] Ist dem Vertragsarzt ein Behandlungsfehler unterlaufen, haftet er zivilrechtlich aus Vertrag (§ 280 Abs. 1 BGB) und daneben aus unerlaubter Handlung nach § 823 BGB, wenn eine rechtswidrige und schuldhafte Verletzung von Leben, Körper oder Gesundheit vorliegt.

Bei einer privatärztlichen Behandlung werden im Rahmen Allgemeiner Geschäftsbedingungen (AGB) meist die Gebührenordnung für Ärzte (GOÄ) bzw. die Gebührenordnung für Zahnärzte (GOZ) zugrunde gelegt. Nach diesen Grundsätzen erstatten private Krankenversicherungen und staatliche Beihilfestellen Krankenbehandlungskosten.

- **Verhältnis „Nutzer – Krankenhaus“**

  Der im Krankenhaus beschäftigte Arzt wird aufgrund seines Arbeitsvertrags mit dem Krankenhausträger (z.B. einer Kommune, einem Zweckverband oder einem privatrechtlichen Unternehmen) tätig; der Patient schließt in der Regel mit dem Krankenhausträger einen gemischten Vertrag, der vorwiegend Dienstvertrag ist und die ärztliche Behandlung einschließt (sog. totaler Krankenhausvertrag).

- **Einschaltung weiterer Ärzte und Verhältnis der Ärzte untereinander**

  Bei dem Einsatz von AAL-Anwendungen kommt es häufig zu einem arbeitsteiligen Zusammenwirken mit anderen Ärzten. Hier gilt, dass ein Vertragsschluss zwischen dem Patienten und den hinzugezogenen Ärzten nur anzunehmen ist, wenn die Hinzuziehung jeweils im Einzelfall mit Zustimmung des Patienten geschieht. Anderenfalls besteht ausschließlich eine vertragliche Beziehung des Patienten mit dem Primärbehandler. Hinzu kommt eine vertragliche / haftungsrechtliche Beziehung unter den arbeitsteilig tätigen Ärzten.[20]

---

[19] § 76 Abs. 4 SGB V.

[20] Vgl. dazu auch Link, Telemedizinische Anwendungen in Deutschland und in Frankreich, 2009, S. 112.

- **Rechtsbeziehung des Arztes / des Pflegedienstes zur Krankenkasse / Pflegekasse**

  Das Rechtsverhältnis zwischen den Leistungserbringern (Ärzten, Krankenhäusern, Apotheken, Pflegediensten) und den Kranken- bzw. Pflegekassen ist in den jeweiligen Büchern des SGB geregelt.

2.5 Bedeutung einer Datenflussanalyse bei AAL-Anwendungen

Die Beschreibung der Datenflüsse in einer konkreten AAL-Anwendung stellt das Herzstück einer jeden Analyse dar, die die Bestimmung der Rechtskonformität und des Datensicherheitsniveaus zum Ziel hat. In diesem Abschnitt wird lediglich ein Überblick über Bereiche gegeben, die typische Datenflüsse bei AAL-Anwendungen umfassen.

In Anlehnung an sich von innen nach außen öffnende Sphären kann der AAL-Datenfluss folgende Bereiche erfassen: Im Zentrum steht die Datenerhebung in der Wohnung oder am Körper. Über diese Datenverarbeitung soll zunächst und vorrangig der Betroffene selbst Verfügungsmacht und -befugnis haben. Informationen können auch an Freunde, Eltern, Kinder, sonstige Familienangehörige oder Nachbarn gegeben werden, denen aber in keinem Fall eine Interventionspflicht auferlegt, sondern allenfalls eine solche Möglichkeit gegeben werden sollte. Eine entsprechende Pflicht kann gegenüber externen Dienstleistern begründet werden; zu unterscheiden ist dabei zwischen medizinischen und nicht-medizinischen Angeboten. Darüber qualitativ hinausgehend und für die Privatsphäre der Betroffenen invasiver sind die akute Notfallbearbeitung und zeitlich umfangreichere Hilfen. Dabei können medizinische und Pflegeeinrichtungen einbezogen sein, evtl. aber auch Krankenkassen oder sonstige professionelle medizinische Helfer. In einer äußeren Schale können Daten aus AAL zu weiteren unterschiedlichen Bedarfsträgern gelangen: von der Forschung über Versicherungen bis zu Anbietern von Informationstechnik (IT).

Diese abstrahierende Darstellung ist für eine umfassende juristische und sicherheitstechnische Evaluation von realen AAL-Systemen und ihrer Einbettung in andere Datenverarbeitungssysteme nicht geeignet; dafür wären die genauen Datenflüsse in zweckmäßiger Form darzustellen, beispielsweise in UML-Diagrammen[21], und mit detaillierten Informationen über die einzelnen Bearbeitungsschritte bei den verschiedenen Systemkomponenten und Akteuren zu versehen. Notwendig wäre auch die Transparenz darüber, welche Daten genau verarbeitet werden, z.B. um feststellen zu können, inwieweit ein Personenbezug der Daten gegeben ist oder besondere Schutzbedarfe bestehen. Dies wird im Einzelnen in Kapitel 4 im Rahmen der Anforderungen an die Datensicherheit und den technischen Datenschutz erläutert.

[21] UML: Unified Modeling Language.

2.6 Ableitung von Anforderungen und Rechtsfragen

Die anhand der geschilderten Szenarien sichtbar gemachte Durchdringung des unmittelbaren Lebensumfelds von Menschen mit AAL-Technik und AAL-Dienstleistungen wirft viele juristische Fragen auf. Im Vordergrund dieser Vorstudie stehen die datenschutzrechtlichen Fragen, die sich bei Planung, Einsatz und Betrieb eines AAL-Systems stellen. Auch aus den Anforderungen an die Datensicherheit und den technischen Datenschutz resultieren weitere Fragen. Daneben ergeben sich insbesondere haftungsrechtliche und sozialversicherungsrechtliche Fragen sowie besondere Konstellationen bei Einbeziehung von internationalen Akteuren oder bei Zugriffsersuchen durch Dritte auf die Daten im AAL-System.

In den folgenden Kapiteln 3 bis 9 werden die wesentlichen Anforderungen an AAL-Systeme und daraus resultierenden Fragenkomplexe erörtert. Grundlage für die Ausführungen in dieser Vorstudie ist stets das in Deutschland geltende Recht.

3 Datenschutzrechtliche Anforderungen und Fragestellungen

AAL-Systeme sammeln üblicherweise Daten aus ihrer Umgebung, die sie in ihren Aktionen berücksichtigen. In den meisten Fällen werden diese Daten an verschiedene Beteiligte weitergeleitet, z.B. wenn medizinisches Personal die Daten auswertet und diese als Handlungsgrundlage für Maßnahmen und Interaktionen mit dem Betroffenen dienen. Ein Teil der Daten, die über AAL-Systeme erhoben und verarbeitet werden, sind personenbezogen, spätestens dann, wenn diese einen Dritten (den Unterstützenden) zu einer konkreten Hilfeleistung veranlassen sollen. Die Ansammlung, Auswertung und mögliche Weiterleitung der Daten kann in die Privatsphäre der Nutzer einwirken. Auch die Privatsphäre anderer Betroffener – z.B. im Fall von Besuchern oder Pflegedienstmitarbeitern – kann tangiert werden. Hier kommt dem Datenschutzrecht eine wesentliche Bedeutung zu. Betroffenenrechte auf Auskunft, Berichtigung und Löschung müssen umgesetzt werden können. Auch den weiteren Anforderungen des Datenschutzrechts, z.B. in Bezug auf Datensparsamkeit, Zweckbindung und Transparenz, muss nachgekommen werden. Weitere Konkretisierungen des Rechts auf informationelle Selbstbestimmung sind das Recht auf Nichtwissen, das Verbot des Erstellens von Persönlichkeitsprofilen, das Verbot der Vorratsdatenverarbeitung sowie das Verbot einer Rundumüberwachung. Mit der Entscheidung zur Online-Durchsuchung 2008 hat das Bundesverfassungsgericht[22] analog zum räumlichen Schutz der Wohnung und dem sozialen Schutz der Familie eine digitale persönliche Privatsphäre der eigengenutzten IT-Systeme definiert und mit dem Grundrecht auf Gewährleistung der Vertraulichkeit und Integrität informationstechnischer Systeme einem starken Schutz unterworfen. Adressat dieser Pflichten ist stets die Daten verarbeitende Stelle[23], mithin auch jede private Stelle. Dies können Betreiber und Anbieter der AAL-Systeme sein, aber auch die Nutzer selbst können in diese Rolle geraten, wenn ihre Systeme personenbezogene Daten über andere verarbeiten.

Im Folgenden werden zunächst die verfassungsrechtlichen (siehe Abschnitt 3.1) und einfachgesetzlichen Rechtsgrundlagen des Datenschutzes (siehe Abschnitt 3.2) dargestellt, bevor die Grundprinzipien des Datenschutzes (siehe Abschnitt 3.3) erläutert werden, die für jedes AAL-System zu beachten sind. Anschließend wird auf besonderes Datenschutzrecht, insbesondere im Medien- und im Medizinbereich, eingegangen (siehe Abschnitt 3.4). Schließlich fasst Abschnitt 3.5 die Ergebnisse und offenen Fragen zusammen.

3.1 Verfassungsrechtliche Grundlagen

In Bezug auf die verfassungsrechtlichen Grundlagen für datenschutzrechtliche Anforderungen an AAL-Systeme spielen insbesondere das Recht auf informationelle Selbstbestimmung

[22] BVerfG, Urteil vom 27.02.2008, 1 BvR 370/07.

[23] Auch „verantwortliche Stelle“, siehe § 3 Abs. 7 Bundesdatenschutzgesetz (BDSG), näher erläutert in Abschnitt 3.3.7.

(siehe Abschnitt 3.1.1) und das Fernmeldegeheimnis (siehe Abschnitt 3.1.2) eine Rolle. Aus diesen Grundrechten resultieren zunächst Schutzpflichten des Staates; sie können aber auch Wirkung in privatrechtlichen Verhältnissen entfalten, wie in Abschnitt 3.1.3 dargestellt. Schließlich führt Abschnitt 3.1.4 weitere Grundrechte auf, die möglicherweise tangiert werden.

3.1.1 Das Recht auf informationelle Selbstbestimmung

Grundlage des deutschen Datenschutzrechts ist das Verfassungsrecht. Das Bundesverfassungsgericht hat erstmals in seinem Volkszählungsurteil, durch das das deutsche Datenschutzrecht entscheidend geprägt worden ist, ein Grundrecht auf informationelle Selbstbestimmung anerkannt[24] und nachfolgend immer wieder bestätigt und weiterentwickelt. Das von Art. 2 Abs. 1 i.V.m. Art. 1 Abs. 1 Grundgesetz (GG) gewährleistete allgemeine Persönlichkeitsrecht umfasst auch die aus dem Gedanken der Selbstbestimmung folgende Befugnis des Einzelnen, grundsätzlich selbst zu entscheiden, wann und innerhalb welcher Grenzen persönliche Lebenssachverhalte offenbart werden. Dies setzt voraus, dass dem Einzelnen eine Entscheidungsfreiheit über vorzunehmende oder zu unterlassende Handlungen einschließlich der Möglichkeit verbleibt, sich auch entsprechend dieser Entscheidung tatsächlich zu verhalten. Wer nicht mit hinreichender Sicherheit überschauen kann, welche ihn betreffenden Informationen in bestimmten Bereichen seiner sozialen Umwelt bekannt sind, und wer das Wissen möglicher Kommunikationspartner nicht einigermaßen abzuschätzen vermag, kann in seiner Freiheit wesentlich gehemmt sein, aus eigener Selbstbestimmung zu planen oder zu entscheiden.[25]

Daneben ist ein Recht auf Nichtwissen, das insbesondere im Medizinbereich und in der genetischen Forschung Bedeutung erlangt, allgemein anerkannt.[26] Die Kenntnis z.B. einer unheilbaren Krankheit oder einer nicht verhinderbaren genetischen Disposition beeinträchtigt u.U. die Gesundheit des Betroffenen. Zur Selbstbestimmung gehört daher auch die Befugnis auf Nichtkenntnis persönlicher Daten. Man darf dem Betroffenen Ergebnisse einer Analyse nicht aufdrängen, wenn dieser dieses Wissen nicht haben will.[27]

Wie bereits dargelegt, hat das Bundesverfassungsgericht in der oben genannten Entscheidung eine digitale persönliche Privatsphäre der eigengenutzten IT-Systeme definiert und mit

---

[24] BVerfGE 65, 1 = NJW 1984, 419.

[25] BVerfGE 65, 42 f.

[26] Vgl. auch Stümper, in: DuD 1995, S. 511 ff.; Laufs / Kern, Handbuch des Arztrechts, 4. Auflage, 2010, Rn. 82; Weichert / Kilian, in: Kilian / Heussen (Hrsg.), Computerrechts-Handbuch, Ergänzungslieferung 2009, Verfassungsrechtliche Grundlagen des Datenschutzes, Rn. 44.

[27] Weichert, Gentests und Persönlichkeitsrecht, Datenschutz und Datenhoheit, Vortrag im Rahmen des Wintersymposiums 2001/2002, „Von der Durchsichtigkeit des Menschen – Rechtsprobleme der Gendiagnostik“, abrufbar unter: https://www.datenschutzzentrum.de/material/themen/gendatei/gentests.htm#2c.

dem Grundrecht auf Gewährleistung der Vertraulichkeit und Integrität informationstechnischer Systeme einem starken Schutz unterworfen.[28] Es ist wie das Recht auf informationelle Selbstbestimmung Ausfluss aus Art. 2 Abs. 1 i.V.m. Art. 1 Abs. 1 GG und ergänzt den bisher lückenhaften anderweitigen Grundrechtsschutz, um neuartigen Gefährdungen zu begegnen. Die allgegenwärtig gewordene Nutzung eigener IT-Systeme – dazu gehören nicht nur der heimische Computer, sondern auch kleine, leistungsfähige mobile Endgeräte wie Personal Digital Assistants (PDAs) und Smartphones (Handys mit Zusatzfunktionen wie z.B. einem E-Mail-Programm),[29] die typischerweise zum Speichern auch personenbezogener Daten mit gesteigerter Sensibilität genutzt werden – führt zu einem umfangreichen Datenbestand über die persönlichen Verhältnisse und Lebensführung des Betroffenen.[30] Anknüpfungspunkte für das Bundesverfassungsgericht (BVerfG) in seiner Entscheidung waren sowohl die potenziell große Menge und der potenzielle Gehalt der Daten, die angesichts ihrer Herkunft persönlicher Art sind und damit von gesteigerter Sensibilität sein können,[31] als auch die besondere Verletzlichkeit informationstechnischer Systeme.[32] Das neue Grundrecht dient daher insbesondere dem Schutz vor einer „Ausforschung der Persönlichkeit des Betroffenen“ auch im Vorfeld eines Personenbezugs und schützt somit vor Persönlichkeitsgefährdungen, die sich daraus ergeben, dass der Einzelne zu seiner Persönlichkeitsentfaltung auf die Nutzung informationstechnischer Systeme angewiesen ist und dabei dem System persönliche Daten anvertraut oder schon allein durch dessen Nutzung zwangsläufig liefert.[33] Das Bundesverfassungsgericht hat damit seine Rechtsprechung konsequent fortgesetzt, dass es die Notwendigkeit eines solchen Freiheitsschutzes namentlich auch im Hinblick auf moderne Entwicklungen und die mit ihnen verbundenen neuen Gefährdungen für den Schutz der menschlichen Persönlichkeit angenommen hat. Geschützt sind das Interesse der Betroffenen an der Vertraulichkeit der erzeugten, verarbeiteten und gespeicherten Daten sowie die Integritätserwartungen der Betroffenen.

3.1.2 Das Fernmeldegeheimnis

Art. 10 GG schützt die private Fernkommunikation. Das Fernmeldegeheimnis gewährleistet die Vertraulichkeit der individuellen Kommunikation, wenn diese wegen der räumlichen Distanz zwischen den Beteiligten auf eine Übermittlung durch andere angewiesen ist und des-

---

[28] Dieser verfassungsrechtliche Grundrechtsschutz gilt analog spätestens seit dem Inkrafttreten der Europäischen Grundrechtecharta im Dezember 2009 EU-weit; dort ist das Grundrecht auf Datenschutz in Art. 8 normiert.

[29] Vgl. Fox, in: DuD 2007, S. 827.

[30] BVerfG, Urteil vom 27.02.2008, 1 BvR 370/07, Rn. 171 ff.

[31] Petri, in: DuD 2008, S. 444 ff.

[32] NJW 2008, 1043.

[33] BVerfG, Urteil vom 27.02.2008, 1 BvR 370/07, Rn. 199 f.

halb in besonderer Weise einen Zugriff Dritter – einschließlich staatlicher Stellen – ermöglicht. Brief-, Post- und Fernmeldegeheimnis sind wesentlicher Bestandteil des Schutzes der Privatsphäre; sie schützen vor ungewollter Informationserhebung und gewährleisten eine Privatheit auf Distanz.[34] Das Fernmeldegeheimnis schützt damit die unkörperliche Übermittlung von Informationen an individuelle Empfänger mit Hilfe des Telekommunikationsverkehrs.[35] Es hat seine einfachgesetzliche Ausprägung in § 88 Telekommunikationsgesetz (TKG) gefunden und wird dort legaldefiniert. Demnach unterliegen dem Fernmeldegeheimnis „der Inhalt der Telekommunikation und ihre näheren Umstände, insbesondere die Tatsache, ob jemand an einem Telekommunikationsvorgang beteiligt ist oder war“ sowie „die näheren Umstände erfolgloser Verbindungsversuche“. Es schützt daher die Vermittlung von Informationen[36] an individuelle Empfänger und mithin auch die sog. Verkehrsdaten.[37] Nach Abschluss des Kommunikationsvorgangs unterliegen die beim Teilnehmer gespeicherten Daten nicht mehr dem Schutzbereich des Fernmeldegeheimnisses. Diese Daten sind dann in den Herrschaftsbereich des Teilnehmers in der Weise übergegangen, dass ihm das Löschen der Kommunikationsinhalte und Verkehrsdaten eigenständig möglich ist, so dass eine Gefahrenlage aufgrund der Kommunikation über eine räumliche Distanz nicht mehr besteht.[38] Jedoch kommt dann der Schutzbereich des Rechts auf informationelle Selbstbestimmung aus Art. 2 Abs. 1 i.V.m. Art. 1 Abs. 1 GG zum Tragen.

3.1.3 Drittwirkung der Grundrechte und Schutzpflichten des Staates

In privatrechtlichen Rechtsverhältnissen haben die Grundrechte nach der Rechtsprechung des Bundesverfassungsgerichts zwar keine unmittelbare Geltung. Als Ausdruck einer objektiven Wertordnung strahlen sie jedoch auf die Auslegung und Anwendung privatrechtlicher Vorschriften aus (sog. mittelbare Drittwirkung).[39] Weiterhin kann sich aus den Grundrechten auch eine Pflicht für den Staat herleiten, die jeweils betroffene grundrechtliche Sphäre aktiv zu schützen – insbesondere vor Beeinträchtigungen durch andere Privatrechtsubjekte. Solche staatlichen Schutzpflichten wurden vom Bundesverfassungsgericht zunächst in Bezug

---

[34] BVerfGE, Urteil vom 02.03.2006, 2 BvR 2099/04, Rn. 65.

[35] BVerfGE 67, 157.

[36] Dabei ist jede Übermittlung von Informationen mit Hilfe der verfügbaren Telekommunikationstechniken erfasst, ohne dass es auf die konkrete Übermittlungsart (Kabel oder Funk, analoge oder digitale Vermittlung) und Ausdrucksform (Sprache, Bilder, Töne, Zeichen oder sonstige Daten) ankommt.

[37] BVerfGE, Urteil vom 02.03.2006, 2 BvR 2099/04, Rn. 67; vgl. auch BVerfGE 106, 28, 36.

[38] Eckhardt, in: DuD 2006, S. 365 ff.

[39] Ständige Rechtsprechung seit BVerfGE 7, 198.

auf das Schutzgut Leben und körperliche Unversehrtheit entwickelt[40] und später auf andere Freiheitsgrundrechte ausgedehnt.[41]

Die informationelle Selbstbestimmung ist in erheblichem Maße auch Beeinträchtigungen durch die Aktivitäten privater Dritter ausgesetzt. Hieraus folgt eine verfassungsrechtlich gebotene Risikovorsorge im Sinne einer Schutzpflicht des Staates ebenfalls in Hinblick auf das Verhalten Privater mit Auswirkungen für den von diesem Grundrecht geschützten Schutzbereich. Soweit das Grundrecht von Seiten privater Dritter beeinträchtigt werden kann, hat der Gesetzgeber durch den Einsatz straf-, zivil- und verwaltungsrechtlicher Instrumente für einen effektiven Schutz Sorge zu tragen. Hinzu kommen organisatorische und verfahrensmäßige Vorkehrungen, welche die Beachtung materieller Regelungen sichern müssen.[42] Auch Art. 10 GG beschränkt sich nicht auf die Abwehr staatlicher Eingriffe, sondern ist ein Element der Gesamtrechtsordnung, so dass dem Geheimnisschutz ebenso Bedeutung für die Rechtsbeziehungen zwischen Privaten zukommt.

3.1.4 Sonstige Grundrechte

Bei AAL geht es nicht allein um den Persönlichkeitsschutz i.S.d. Art. 2 Abs. 1 i.V.m. Art. 1 Abs. 1 GG. Vielmehr können auch andere Grundrechte einen direkten Bezug zur AAL-Datenverarbeitung haben: Art. 2 Abs. 2 Satz 1 GG schützt das Leben und die körperliche Unversehrtheit. Diesem Schutz dient u.a. AAL; dem Einsatz von Körpersensoren geht i.d.R. ein einwilligungsbedürftiger Eingriff in dieses Grundrecht voraus. Weiterhin verbietet der grundgesetzliche Gleichheitsgrundsatz Diskriminierung generell, Art. 3 Abs. 3 Satz 2 GG insbesondere die Benachteiligung wegen einer Behinderung. Art. 5 GG gewährt Informations- und Meinungsfreiheit; ein Aspekt ist insofern der Anspruch auf Informationszugang zu Daten aus der eigenen Umwelt. Da bei AAL oft nicht nur eine Person, sondern auch ein Ehepartner oder eine ganze Familie miterfasst werden, wird durch AAL der Schutz von Ehe und Familie nach Art. 6 GG tangiert. Zumeist betroffen ist auch die Unverletzlichkeit der Wohnung nach Art. 13 GG, wenn die Daten hieraus erhoben werden. Schließlich schützt die Berufsfreiheit des Art. 12 GG die Vertraulichkeit in besonderen beruflichen Beziehungen, insbesondere das Sozial- und das Patientengeheimnis.

---

[40] Vgl. BVerfGE 39, 1.

[41] Vgl. z.B. BVerfGE 52, 357; BVerfGE 81, 242.

[42] Theißen, Risiken informations- und kommunikationstechnischer (IKT-)Implantate im Hinblick auf Datenschutz und Datensicherheit, 2009, S. 248.

3.2 Einfachgesetzliche Grundlagen

Auf einfachgesetzlicher Ebene richten sich das Erheben[43], das Verarbeiten[44] und das Nutzen[45] personenbezogener Daten durch private Stellen nach dem Bundesdatenschutzgesetz (BDSG) bzw. den vorrangigen spezialgesetzlichen Regelungen des Datenschutzrechts, die gem. § 1 Abs. 3 Satz 1 BDSG den Vorschriften des Bundesdatenschutzgesetzes vorgehen.[46] Die gesetzlichen Verarbeitungsgrundlagen des AAL finden sich vorrangig im vierten Abschnitt des BDSG (§§ 27 ff.); Grundlage ist im Hinblick auf AAL i.d.R. die Abwicklung eines Vertrags bzw. die Einwilligung des Betroffenen nach § 4a BDSG.

§ 3 Abs. 9 BDSG unterwirft Gesundheitsdaten einem besonderen Regime mit der Folge, dass Einwilligungen sich hierauf explizit beziehen müssen oder dass die Verarbeitung nach § 28 Abs. 6 bis 9 BDSG entweder dem Schutz lebenswichtiger Interessen, der Gesundheitsvorsorge, der medizinischen Diagnostik, der Gesundheitsversorgung, der Behandlung oder der Verwaltung von Gesundheitsdaten dienen muss. Eine wichtige Aufgabe wird es sein festzulegen, welche AAL-Daten zu den nach § 3 Abs. 9 BDSG besonders geschützten Gesundheitsdaten gehören.

Spezialgesetzliche Regelungen zum Datenschutz finden sich unter anderem in den Sozialgesetzbüchern, dem Telemediengesetz und dem Telekommunikationsgesetz.

3.3 Grundbegriffe und Grundprinzipien des Datenschutzes

Zu den Grundprinzipien des Datenschutzrechts gehören die Grundsätze der Rechtmäßigkeit der Datenverarbeitung, der Zweckbindung, der Erforderlichkeit, der Datenvermeidung und der Datensparsamkeit, der Transparenz, der Grundsatz der klaren Verantwortung und der Kontrolle sowie die Gewährleistung der Betroffenenrechte. Weitere Konkretisierungen des Rechts auf informationelle Selbstbestimmung sind das Verbot des Erstellens von Persönlichkeitsprofilen, das Verbot der Vorratsdatenverarbeitung sowie das Verbot einer Rundumüberwachung. Sind AAL-Anwendungen auf das automatisierte Auslösen von Prozessen ausgerichtet, so ist § 6a BDSG anwendbar, wonach automatisierte Entscheidungen, bei denen einzelne Persönlichkeitsmerkmale automatisiert bewertet werden, unter Nennung bestimmter Ausnahmen grundsätzlich verboten sind.

---

[43] Gemäß § 3 Abs. 3 BDSG bedeutet „Erheben“ das Beschaffen von Daten über den Betroffenen.

[44] Gemäß § 3 Abs. 4 Satz 1 BDSG umfasst der Begriff „Verarbeiten“ „das Speichern, Verändern, Übermitteln, Sperren und Löschen personenbezogener Daten“. Es ist zu beachten, dass der Begriff „Datenverarbeitung“ in dieser Studie in dem umfassenderen Sinn verwendet wird, wie es in der Informatik üblich ist. Die jeweilige Bedeutung ergibt sich aus dem jeweiligen Kontext.

[45] Gemäß § 3 Abs. 5 BDSG ist „Nutzen“ jede Verwendung personenbezogener Daten, soweit es sich nicht um Verarbeitung (siehe Erklärung in Fußnote 44) handelt.

[46] Ihre europäische Grundlage hat das nationale Datenschutzrecht v.a. in der europäischen Datenschutzrichtlinie 95/46/EG und in der E-Privacy-Richtlinie (2002/58/EG zuletzt geändert durch die Richtlinie 2009/136/EG) für den Bereich der Telekommunikation und der Telemedien.

Bevor jedoch auf die Grundprinzipien eingegangen werden kann, sind die Fragen der Anwendbarkeit der Datenschutzgesetze und damit auch der Einschlägigkeit der Grundprinzipien des Datenschutzes zu klären. Daher beschäftigt sich Abschnitt 3.3.1 mit dem Vorliegen des Personenbezugs und untersucht anonymisierte und pseudonymisierte Daten. Abschnitt 3.3.2 beschreibt die Anforderungen an die Rechtmäßigkeit der Datenverarbeitung. Anschließend werden die Grundprinzipien des Datenschutzes vorgestellt, d.h. die Grundsätze der Zweckbindung (siehe Abschnitt 3.3.3), der Erforderlichkeit (siehe Abschnitt 3.3.4), der Datenvermeidung und Datensparsamkeit (siehe Abschnitt 3.3.5), der Transparenz (siehe Abschnitt 3.3.6), der klaren Verantwortlichkeit (siehe Abschnitt 3.3.7), der Kontrolle (siehe Abschnitt 3.3.8), der Gewährleistung der Betroffenenrechte (siehe Abschnitt 3.3.9), des Verbots der Profilbildung (siehe Abschnitt 3.3.10), des Verbots der Datensammlung auf Vorrat (siehe Abschnitt 3.3.11) und schließlich des Verbots der automatisierten Einzelentscheidung (siehe Abschnitt 3.3.12).

3.3.1 Personenbezogene und anonymisierte oder pseudonymisierte Daten

Grundsatz

Der Anwendungsbereich der Datenschutzbestimmungen ist eröffnet, wenn personenbezogene Daten durch öffentliche oder nicht-öffentliche Stellen erhoben, verarbeitet oder genutzt werden.[47] Personenbezogene Daten sind nach den Datenschutzgesetzen „Einzelangaben über persönliche oder sachliche Verhältnisse einer bestimmten oder bestimmbaren natürlichen Person (Betroffener)“.[48] Ob Daten personenbezogen sind oder nicht, hängt folglich davon ab, ob diese Aussagen zu bestimmten oder bestimmbaren Personen zulassen. Zu den personenbezogenen Angaben gehören demnach u.a. Informationen zur Anschrift, zum Beruf und zu privaten Aktivitäten. Auch Bild- und Tonaufnahmen können personenbezogene Daten darstellen. Für AAL-Anwendungen von Bedeutung sind daneben insbesondere Daten zum Nutzungsverhalten, technische Kennungen wie z.B. IP-Adressen, unter denen ein Endgerät mit dem Internet kommuniziert, sowie Gesundheitsdaten, die zu den besonderen Arten personenbezogener Daten[49] zählen, für die spezielle Verarbeitungsregeln gelten.[50]

Die Datenschutzgesetze gelten dagegen nicht für nicht-personenbezogene Daten, so dass bei diesen die datenschutzrechtlichen Vorgaben nicht beachtet werden müssen. Um den Personenbezug aus vormals personenbezogenen Daten zu entfernen, ist in vielen Fällen die

---

47 Vgl. z.B. § 1 BDSG, § 1 TMG.

48 § 3 Abs. 1 BDSG.

49 „Besondere Arten personenbezogener Daten sind Angaben über die rassische und ethnische Herkunft, politische Meinungen, religiöse oder philosophische Überzeugungen, Gewerkschaftszugehörigkeit, Gesundheit oder Sexualleben.“, § 3 Abs. 9 BDSG.

50 Zum Beispiel § 13 Abs. 2, 14 Abs. 5, § 28 Abs. 6-9, § 29 Abs. 5 BDSG.

Methode des Anonymisierens möglich: Anonymisieren ist das Verändern personenbezogener Daten derart, dass die Einzelangaben über persönliche oder sachliche Verhältnisse nicht mehr oder nur mit einem unverhältnismäßig großen Aufwand an Zeit, Kosten und Arbeitskraft einer bestimmten oder bestimmbaren natürlichen Person zugeordnet werden können.[51] Allerdings sind auch bei anonymisierten Daten Vorkehrungen zu treffen, damit ein Personenbezug nicht mit Zusatzwissen oder durch andere Methoden wiederhergestellt werden kann.[52] Ähnliches gilt für pseudonymisierte Daten: Pseudonymisieren ist das Ersetzen des Namens und anderer Identifikationsmerkmale durch ein Kennzeichen zu dem Zweck, die Bestimmung des Betroffenen auszuschließen oder wesentlich zu erschweren.[53,54] Während es sich beim Anonymisieren und Pseudonymisieren um Methoden handelt, die die Daten verarbeitende Stelle auf in der Regel bereits vorhandene Daten mit Personenbezug anwenden kann, können auch Daten anonym oder unter Pseudonym vorliegen, deren Personenbezug der Daten verarbeitenden Stelle gar nicht bekannt ist. Beispielsweise ist es möglich, dass ein Betroffener selbst unter Pseudonym auftritt, ohne dass die Daten verarbeitende Stelle hier pseudonymisieren müsste.

Nicht anwendbar ist das BDSG außerdem bei Datenerhebungen, -nutzungen und -verarbeitungen, die ausschließlich für persönliche und familiäre Tätigkeiten erfolgen (§ 1 Abs. 2 Nr. 3 BDSG),[55] d.h. im Fall einer rein privaten Verarbeitung.[56] Etwas anderes gilt, wenn die Tätigkeit aus dem persönlich-familiären Bereich herausragt, so z.B. bei Werbeangeboten, auch wenn diese an und für sich privater Natur sind.[57]

---

51 § 3 Abs. 6 BDSG.

52 Roßnagel / Scholz, Datenschutz durch Anonymität und Pseudonymität, in: MMR 2000, S. 721 ff.

53 § 3 Abs. 6a BDSG.

54 Schwierig wird eine Anonymisierung oft z.B. im medizinischen Bereich, da der Arzt zur Erstellung einer Diagnose in der Regel auch zusätzliche Daten, wie etwas das Alter des Patienten oder bereits erfolgte Operationen etc. benötigt, die sodann die Informationen personenbeziehbar machen. Gleiches gilt für eine Speicherung im Rahmen der Dokumentation und der Aufbewahrung dieser Daten. Der Patient bleibt damit stets zumindest bestimmbar, so dass die Datenschutzvorschriften eingreifen. Die insbesondere in der Praxis der medizinischen Forschung vielfach angewandte Methode, den direkten Patientenbezug durch Pseudonyme zu ersetzen, führt nicht zu einer faktischen Anonymisierung im Sinne der Datenschutzgesetze. Bei dieser sog. Pseudonymisierung bleibt eine Zuordnungsfunktion erhalten, mit deren Hilfe der Personenbezug wiederhergestellt werden kann. Pseudonymisierte Daten fallen daher unter den Anwendungsbereich der Datenschutzgesetze. Dies gilt nach hiesiger Auffassung auch dann, wenn die pseudonymisierten Daten von einer Stelle verarbeitet werden, die selbst nicht über die Zuordnungsfunktion verfügt.

55 Der Gesetzgeber will damit in Umsetzung des Art. 3 Abs. 2-3 Datenschutzrichtlinie 95/46/EG klarstellen, dass lediglich solche Erhebungen, Verarbeitungen oder Nutzungen der personenbezogenen Daten in den Anwendungsbereich der Datenschutzbestimmungen fallen, die kommerzielle Verarbeitungen, mithin geschäftsmäßig für berufliche oder gewerbliche Zwecke erfolgende Verarbeitungen zum Gegenstand haben.

56 Dammann, in: Simitis (Hrsg.), BDSG, 6. Auflage, 2006, § 1 Rn. 116.

57 Weichert, in: Däubler / Klebe / Wedde / Weichert (Hrsg.), Bundesdatenschutzgesetz Kompaktkommentar, 3. Auflage, 2010, § 1 Rn. 9.

Herausforderungen

AAL-Anwendungen dürften sich in Teilbereichen auch mit anonymisierten oder pseudonymisierten Daten durchführen lassen. Beispielsweise kann die Datenerhebung im räumlichen Bereich und die Übermittlung der Daten so lange anonym bzw. unter Pseudonym erfolgen, bis ein Dritter eingeschaltet wird, der in eine konkrete Interaktion mit dem Betroffenen treten soll oder muss. Soll zum Beispiel bei Überschreitung eines zuvor festgelegten Schwellenwertes bei Dritten ein Alarm ausgelöst werden, so könnten zunächst Daten in anonymer Weise bzw. unter Pseudonym ausgewertet und bei Unauffälligkeit zeitnah wieder gelöscht werden. Erst im Falle der Alarmierung des Dritten würden diese Daten einer bestimmten Person zugeordnet werden. Auch bei AAL-Anwendungen, die einen Erfahrungsaustausch über ein soziales Netzwerk zum Ziel haben, kann eine Datenverarbeitung unter Pseudonym in Betracht kommen oder sogar geboten sein.[58] Beteiligte derartiger Verfahren sollten daher immer prüfen, ob bzw. bis zu welchem Zeitpunkt die gewünschte Funktionalität auch ohne personenbezogene Daten erreicht werden kann.

Ist eine anonymisierte Verarbeitung der Daten vorgesehen, ist darauf zu achten, dass eine Personenbeziehbarkeit nicht durch die Auswertung der Daten oder Zusatzwissen von Beteiligten wieder- oder neu hergestellt wird. Hier liegt wiederum eine wesentliche Herausforderung in Bezug auf AAL: Eine elektronische Auswertbarkeit und Verknüpfbarkeit von Daten erhöht die Wahrscheinlichkeit des Vorliegens und die Möglichkeiten der Zuordnung von Zusatzwissen, das eine Identifizierung der Betroffenen ermöglicht und ehemals anonyme Daten wieder zuordenbar macht.[59] Die für AAL-Anwendungen typische enge Verknüpfung von Sensordaten mit realen Ereignissen erlaubt selbst bei konsequenter Verwendung von Pseudonymen unter Umständen eine Personenidentifikation beispielsweise durch Zurückverfolgung pseudonymisierter Bewegungsdaten mit bekannten bevorzugten Aufenthaltsorten oder einer Kombination mit anderen Identifizierungsmethoden.[60] Zudem liegen alle Daten ohne Medienbruch elektronisch vor, was eine automatisierte Auswertung erheblich erleichtert. Über eine Person, deren Daten über eine AAL-Anwendung erhoben werden, entsteht somit eine umfangreiche und aussagekräftige, zunächst noch anonyme oder pseudonyme Datensammlung, die jedoch bei der Verwendung weiterer Daten durch Zusatzwissen, Veränderungen des Aufwandes von Aufdeckungsanstrengungen oder durch Fortentwicklung der techni-

[58] Siehe dazu Abschnitt 3.4.1.

[59] Vgl. auch Weichert, Cloud Computing und Datenschutz, Vortrag auf dem 4. Österreichischen IT-Rechtstag INFOLAW, 18.06.2010, Wien.

[60] Roßnagel, Datenschutz in einem informatisierten Alltag, Gutachten im Auftrag der Friedrich-Ebert-Stiftung, 2007, S. 186, abrufbar unter: http://library.fes.de/pdf-files/stabsabteilung/04548.pdf.

schen Analyse- und Auswertungsinstrumente dann doch dieser Person zugeordnet werden kann. Die Grenze zwischen Personenbezug und fehlendem Personenbezug verschwimmt.[61]

Kommt es zu einer Aufdeckung des Personenbezugs, so können auf einen Schlag ganze Bewegungs- und Verhaltensprofile personenbeziehbar werden, die vorher als anonym galten. Im Fall von wirklich anonymen Daten wäre es der Daten verarbeitenden Stelle grundsätzlich gestattet, diese Daten nach Belieben aufzuzeichnen bzw. zu speichern, auszuwerten und an Dritte zu übermitteln. Es könnten also Daten auf Vorrat gesammelt werden, ohne dass die Betroffenen etwas darüber erfahren, da auch keine Benachrichtigungspflichten greifen. Zwar wird bei fehlender Rechtsgrundlage die Datenverwendung nach Aufhebung der Anonymität rechtswidrig, so dass unzulässig gespeicherte Daten zu löschen sind. Damit lassen sich jedoch nicht unerwünschte Konsequenzen verhindern, die etwa durch vorherige Übermittlung der Daten entstanden sein können.

Offene Fragen

Zu klären und festzulegen ist, unter welchen Bedingungen Daten, die für bestimmte Entitäten möglicherweise bereits zum aktuellen Zeitpunkt oder sonst zu einem späteren Zeitpunkt personenbezogen sein können, auf welche Weise verarbeitet werden dürfen. Beispielsweise könnten bei solchen Daten „im Vorfeld des Personenbezugs“ Übermittlungen oder Veröffentlichungen eingeschränkt werden, es könnte das Vorhandensein von möglicherweise verkettenden Elementen unterbunden oder in ihrer zeitlichen Gültigkeit limitiert werden, und die zu treffenden Vorsorgemaßnahmen[62] gegen eine unerwünschte Herstellung des Personenbezugs und für den Umgang mit einem verbleibenden Risiko könnten konkretisiert werden. Hier bedarf es zum einen einer genaueren Prüfung der Risiken und zum anderen der Festlegung von spezifischen Regeln.

3.3.2 Rechtmäßigkeit der Datenverarbeitung

Da jede Verwendung von personenbezogenen Daten einen Eingriff in das Recht auf informationelle Selbstbestimmung darstellt, steht die Verarbeitung personenbezogener Daten unter einem Gesetzesvorbehalt (Verbot mit Erlaubnisvorbehalt).[63] § 4 Abs. 1 BDSG erklärt die Verarbeitung personenbezogener Daten ausnahmsweise für zulässig, wenn sie von einer Rechtsvorschrift erlaubt oder angeordnet wird oder der Betroffene eingewilligt hat.[64] Für jede Phase der Verwendung der Daten – Erhebung, Speicherung, Nutzung, Übermittlung – ist

---

61 Theissen, Risiken informations- und kommunikationstechnischer (IKT-)Implantate im Hinblick auf Datenschutz und Datensicherheit, 2009, S. 305; Roßnagel, Handbuch des Datenschutzrechts, 2003, Kapitel 4.1, Rn. 22, BT-Drs. 16/7891.

62 Roßnagel / Scholz, Datenschutz durch Anonymität und Pseudonymität, in: MMR 2000, S. 721 ff.

63 Tinnefeld / Ehmann / Gerling, Einführung in das Datenschutzrecht, 4. Auflage, 2005, S. 316.

64 Simitis, in: Simitis (Hrsg.), BDSG, 6. Auflage, 2006, § 4a Rn. 1.

dabei ein gesonderter Erlaubnistatbestand notwendig, dessen Vorliegen von dem Verwender vorab zu prüfen ist. Im Ergebnis ist demnach eine Verwendung personenbezogener Daten ohne Gestattung durch eine gesetzliche Rechtsgrundlage (siehe Abschnitt 3.3.2.1) oder durch die Einwilligung des Betroffenen (siehe Abschnitt 3.3.2.2) unzulässig.

3.3.2.1 Gesetzliche Rechtsgrundlagen

Je nachdem, welche Art von Daten verarbeitet wird, können das BDSG oder bereichsspezifische Rechtsgrundlagen einschlägig sein. Grundsätzlich gilt, dass für eine durch vernetzte und allgegenwärtige Datenverarbeitung technisch mögliche unbemerkte Erfassung von Personen und deren Verhaltensweisen sowie einer damit einhergehenden Profilbildung eine Einwilligung des Betroffenen erforderlich ist. Eine solche Datenverarbeitung dürfte sich häufig weder durch § 28 Abs. 1 Nr. 1 BDSG rechtfertigen lassen – weil kein entsprechender Vertrag besteht – noch durch § 28 Abs.1 Nr. 2 BDSG, weil das schutzwürdige Interesse des Betroffenen bei einer im Hintergrund laufenden Datenerhebung und damit „unbewussten" Überwachung und Auswertung seines Verhaltens das Interesse der Daten verarbeitenden Stelle überwiegt.[65]

Eine Datenverarbeitung auf der Grundlage des § 28 Abs. 1 Nr. 1 BDSG i.V.m. einem Vertrag ist nur dann gestattet, wenn von einem Betreiber oder Verkäufer einer einfach gehaltenen AAL-Anwendung oder -Dienstleistung dem Nutzer eine Leistung angeboten wird, die keine Gefahr der Intransparenz beinhaltet.[66] So kommt im zweiten Szenario als Rechtsgrundlage der Datenverarbeitung § 28 Abs. 1 Nr. 1 BDSG in Betracht, wenn ein Vertrag über das Erbringen der Leistung „Notfallsystem" geschlossen wird und an der Art und Weise der Überwachung durch das System für die Betroffenen kein Transparenzdefizit besteht. Dies dürfte anzunehmen sein, wenn die Betroffenen sich für die grundsätzlich weniger invasive Nutzungsvariante entscheiden, die keine Übertragung von Kamerabildern an Mitarbeiter der „Safe Home"-Notfallzentrale vorsieht.

Nach § 28 Abs. 1 Nr. 2 BDSG ist das Erheben, Speichern, Verändern oder Übermitteln personenbezogener Daten oder ihre Nutzung als Mittel für die Erfüllung eigener Geschäftszwecke zwar zulässig, soweit es zur Wahrung berechtigter Interessen der verantwortlichen Stelle erforderlich ist und kein Grund zu der Annahme besteht, dass das schutzwürdige Interesse des Betroffenen an dem Ausschluss der Verarbeitung oder Nutzung überwiegt. Grundsätzlich überwiegt aber bei einer im Hintergrund laufenden Datenerhebung und damit „unbe-

---

65 Report „Verkettung digitaler Identitäten" des Unabhängigen Landeszentrums für Datenschutz in Zusammenarbeit mit der Technischen Universität Dresden im Auftrag des Bundesministeriums für Bildung und Forschung, 2007, S. 202 ff.

66 Report „Verkettung digitaler Identitäten" des Unabhängigen Landeszentrums für Datenschutz in Zusammenarbeit mit der Technischen Universität Dresden im Auftrag des Bundesministeriums für Bildung und Forschung, 2007, S. 202 ff.

wussten“ Überwachung und Auswertung seines Verhaltens immer das schutzwürdige Interesse des Betroffenen. Im Ergebnis sollte im Zweifelsfall stets eine Einwilligung der Betroffenen nach § 4a BDSG der Betroffenen eingeholt werden.

Für die Verarbeitung personenbezogener Gesundheitsdaten im Zusammenhang mit einer ärztlichen Behandlung ist im Regelfall § 28 Abs. 7 Satz 1 BDSG einschlägig. Danach dürfen die für die Erfüllung der Verpflichtung aus dem Behandlungsverhältnis notwendigen Daten vom Arzt erhoben und verarbeitet werden, auch ohne dass hierzu eine ausdrückliche Einwilligung des Patienten vorliegt. Überschreitet die Datenverarbeitung hingegen die Grenzen des Erforderlichen oder das Maß des Üblichen, gemessen an den Erwartungen des Patienten, ist eine gesonderte Einwilligung des Patienten erforderlich. Im telemedizinischen Bereich ist anerkannt, dass telemedizinische Dienstleistungen, die sich im Regelfall noch nicht standardmäßig etabliert haben, grundsätzlich einer gesonderten schriftlichen Einwilligung des Patienten entsprechend den Anforderungen des § 4a BDSG bedürfen. Diese Erwägungen gelten aufgrund der Komplexität der Verfahren und der bisher fehlenden Standardisierung erst recht für AAL-Anwendungen und -Dienstleistungen.

3.3.2.2 Einwilligung

Angesichts der zurzeit sehr beschränkten gesetzlichen Befugnisse zur Datenverarbeitung im Bereich AAL kommt der Einwilligung in der Praxis besondere Bedeutung zu. Die formellen und inhaltlichen Anforderungen an eine wirksame datenschutzrechtliche Einwilligungserklärung sind in § 4a BDSG geregelt. Zu den formalen Anforderungen gehört, dass die Einwilligung zeitlich vor der Datenerhebung erfolgt, der Betroffene einsichtsfähig ist, er zuvor ausreichend informiert und im Regelfall die Schriftform gewahrt wird. Inhaltlich muss jede Einwilligung freiwillig und hinreichend bestimmt erfolgen. Da, wie dargestellt, die Einwilligung vor dem in Rede stehenden Datenverarbeitungsvorgang erfolgen muss, kann eine nachträglich erteilte Zustimmung die zuvor erfolgte rechtswidrige Datenverarbeitung nicht rechtfertigen.[67]

Im Folgenden werden die Anforderungen an die Einsichtsfähigkeit des Betroffenen (siehe Abschnitt 3.3.2.2.1), die Schriftform der Einwilligung (siehe Abschnitt 3.3.2.2.2), deren Freiwilligkeit (siehe Abschnitt 3.3.2.2.3), die Informationspflicht der verantwortlichen Stelle (siehe Abschnitt 3.3.2.2.4) und die Bestimmtheit der Einwilligung (siehe Abschnitt 3.3.2.2.5) erläutert. Daneben finden Besonderheiten in Bezug auf den öffentlichen Bereich (siehe Abschnitt 3.3.2.2.6) und auf die wissenschaftliche Forschung (siehe Abschnitt 3.3.2.2.7) Erwähnung.

[67] Däubler, in: Däubler / Klebe / Wedde / Weichert (Hrsg.), Kompaktkommentar, 3. Auflage, 2010, § 4a Rn. 4.

3.3.2.2.1 Einsichtsfähigkeit

Die Erhebung und Verarbeitung von personenbezogenen Daten stellt einen Eingriff in das Persönlichkeitsrecht des Betroffenen dar, so dass es bei der Legalisierung des Eingriffs darauf ankommt, ob der Betroffene die Konsequenzen seines Handelns übersehen kann, mithin einsichtsfähig ist. Auf die Geschäftsfähigkeit kommt es nicht an.[68] Man kann insoweit bei der datenschutzrechtlichen Einwilligung von einer geschäftsähnlichen Handlung sprechen. Abstrakte Aussagen darüber, wann die Einsichtsfähigkeit gegeben ist, können nicht getroffenen werden. Es ist vielmehr der jeweilige Verwendungszusammenhang zu betrachten, d.h. erst in Kenntnis der konkreten Verarbeitungsabsichten und Verarbeitungsbedingungen lässt sich verlässlich beurteilen, inwieweit der Betroffene selbst entscheiden kann, was mit seinen Daten geschehen soll.[69] Eine bestimmte Altersgrenze ist hier nicht relevant.

Fehlt es an einer entsprechenden Einsicht aufgrund einer Erkrankung, muss der Betreuer oder gesetzliche Vertreter zustimmen.[70] Aus dem Umstand, dass es allein auf die Einsichtsfähigkeit des Betroffenen ankommt, schließen einige Autoren, dass die Einwilligung notwendigerweise höchstpersönlichen Charakter habe und eine Stellvertretung daher ausscheide.[71] In Betracht komme lediglich die Einschaltung eines gesetzlichen Vertreters. Der gesetzliche Vertreter wird auch ein autonomes Tätigwerden von AAL-Systemen für den Betroffenen genehmigen können, so dass eine Übermittlung von personenbezogenen Daten an z.B. Lieferanten möglich ist (zur Delegation an AAL-Systeme siehe Kapitel 7). Die Einordnung als höchstpersönliches Recht darf indes nicht dazu führen, dem Betroffenen die Möglichkeit zu entziehen, eine Vertrauensperson zu bestimmen, um die datenschutzrechtlich gewährten Kontrollrechte wahrzunehmen und die Einhaltungen von Vorgaben auch gegenüber gesetzlichen Vertretern zu kontrollieren. Insgesamt vorzugswürdig erscheint die Auffassung, die Wahrnehmung der sich aus der informationellen Selbstbestimmung ergebenden Rechte an einen selbst gewählten Vertreter überantworten zu können.[72] Für die Möglichkeit, Datenschutzrechte auch durch Dritte wahrnehmen zu lassen, sprach sich auch die 31. Internationale Konferenz der Datenschutzbeauftragten in Madrid aus.[73] Schließlich wurde unlängst ebenfalls in anderen Rechtsgebieten, namentlich im Medizinrecht, vertreten, dass eine Stell-

---

[68] Däubler, in: Däubler /Klebe / Wedde / Weichert (Hrsg.), Kompaktkommentar, 3. Auflage, 2010, § 4a Rn. 5; Gola / Schomerus, Bundesdatenschutzgesetz, 10. Auflage, 2010, § 4a Rn. 10.

[69] Simitis, in: Simitis (Hrsg.), BDSG, 6. Auflage, 2006, § 4a Rn. 21.

[70] Däubler, in: Däubler / Klebe / Wedde / Weichert (Hrsg.), Bundesdatenschutzgesetz Kompaktkommentar, 3. Auflage, 2010, § 4a Rn. 5, der auch auf die Sondervorschrift des § 36 SGB I hinweist, der die Handlungsfähigkeit bei Beantragung von Sozialleistung durch Minderjährige gilt.

[71] Däubler, in: Däubler / Klebe / Wedde / Weichert (Hrsg.), Bundesdatenschutzgesetz Kompaktkommentar, 3. Auflage, 2010, § 4a Rn. 6.

[72] Hansen / Raguse / Storf / Zwingelberg, 2010, S. 29.

[73] Siehe Anmerkung 19 in: Madrid Resolution of the 31st International Conference of the Data Protection and Privacy Commissioners, adopted on 5 November, 2009,

vertretung auch dann in Frage kommt, wenn es um die Einwilligung in Bezug auf Eingriffe in höchstpersönliche Rechte geht.[74]

Davon zu unterscheiden ist die im weiteren Verlauf zu klärende Frage, ob bei der Aufklärung und Information der Betroffenen im Sinne von § 4a BDSG auf die spezifische Nutzergruppe eingegangen werden muss.

3.3.2.2.2 Schriftform

Die Einwilligung ist zum Schutz des Betroffenen grundsätzlich schriftlich zu erklären.[75] Soll die Einwilligung zusammen mit anderen Erklärungen abgegeben werden, so ist sie im jeweiligen Schriftstück besonders zu kennzeichnen, da der Warnfunktion der Schriftform nur Genüge getan wird, wenn der Betroffene auch deutlich erkennen kann, dass er gerade in die Verarbeitung seiner Daten einwilligt. Der Betroffene kann seine bereits erteilte Einwilligung widerrufen.

Soweit Daten im Rahmen einer elektronischen Kommunikation erhoben, verarbeitet oder genutzt werden, ist eine Einwilligung auch in dieser Form möglich. Die Form der Einwilligung muss allerdings sicherstellen, dass der Betroffene seine Einwilligung bewusst und eindeutig erteilt, die Einwilligung protokolliert wird, der Betroffene den Inhalt der Einwilligung jederzeit abrufen und mit Wirkung für die Zukunft widerrufen kann.[76]

Soweit besondere Arten personenbezogener Daten (§ 3 Abs. 9 BDSG, z.B. Gesundheitsdaten) erhoben, verarbeitet oder genutzt werden, muss sich die Einwilligung darüber hinaus ausdrücklich auf diese Daten beziehen, § 4a Abs. 3 BDSG.

3.3.2.2.3 Freiwilligkeit der Einwilligung

Grundsatz

Eine Einwilligung ist nur wirksam, wenn sie auf der freien Entscheidung des Betroffenen beruht.[77] Das bedeutet, sie muss frei von jedem (inneren oder äußeren) Zwang abgegeben werden. Danach ist es nicht ausreichend, auf die Einwilligung zu verweisen, sondern es kommt gleichermaßen auf den Einwilligungskontext an. Eine freie Entscheidung kann nur

---

[74] Perau, Betreuungsverfügung und Vorsorgevollmacht, in: MittRhNotK 1996, S. 285, 293 ff. Zur Vollmachtserteilung auch bei lebensverlängernden Maßnahmen: Füllmich, Zur Ablehnung künstlich lebensverlängernder medizinischer Maßnahmen durch nicht entscheidungsfähige Patienten, in: NJW 1990, S. 2301, 2303.

[75] Vgl. § 4a Abs. 1 Satz 3 BDSG.

[76] Vgl. § 13 Abs. 2 TMG.

[77] Vgl. § 4a Abs. 1 Satz 1 BDSG.

dann vorliegen, wenn der Betroffenen sich nicht in einer Situation befindet, die ihn faktisch dazu zwingt, sich mit der angetragenen Datenverarbeitung einverstanden zu erklären.[78]

Fraglich ist die Freiwilligkeit aus diesem Grund oftmals im Bereich der öffentlichen Leistungsgewährung, mithin im Krankenversicherungsbereich sowie im Behandlungs- und Pflegeverhältnis. Die Betroffenen haben in diesen Bereichen häufig nicht die Wahl, ihr Einverständnis zu verweigern, weil ihnen anderenfalls die benötigte Leistung oder Behandlung nicht bewilligt oder erteilt wird. In den Fällen der öffentlichen Leistungsgewährung erschwert die hinzukommende staatliche Autorität eine freie Entscheidungsmöglichkeit des Betroffenen.[79] Im Gesundheitsbereich befindet sich der Patient in einer ähnlichen Lage: Er befürchtet, nicht die optimale Behandlung zu erhalten, wenn er nicht in die Erhebung seiner Daten einwilligt.[80] Im Grundsatz besteht bei allen ärztlichen Leistungen die Gefahr, dass aufgrund der Unentbehrlichkeit der Leistung der Patient jedenfalls subjektiv nicht frei in seiner Entscheidung für oder gegen die Einwilligung ist.[81]

Hinzu kommt, dass der Patient unter Umständen nicht in der gesundheitlichen Verfassung ist, die nötige Energie und Zeit für eine freie Entscheidung aufzubringen. Während für gesunde Personen in der Regel die Wahrung ihrer informationellen Selbstbestimmung und persönlichen Intimsphäre im Vordergrund steht, tritt dieser Gesichtspunkt bei (Schwer-)Kranken schnell in den Hintergrund und wird durch den Wunsch nach einer möglichst optimalen, effizienten und schnellen Heilbehandlung ersetzt.[82] Einerseits hoffen die Betroffenen auf neue Techniken in der Medizin, andererseits wollen sie gerade in diesem sensiblen Bereich selbst darüber bestimmen können, wer was unter welchen Umständen über ihre Gesundheitsprobleme erfährt. Die Technik weckt nicht nur Hoffnungen, sondern angesichts der in immer mehr Lebensbereichen anfallenden Daten und deren Auswertungsmöglichkeiten auch Ängste.

Die Notwendigkeit der Freiwilligkeit bei einer Einwilligung impliziert, dass die Erbringung von Leistungen nicht von der Einwilligung in die Verarbeitung oder Nutzung von Daten abhängig gemacht werden darf, die nicht in einem sachlichen Zusammenhang mit der Leistung stehen und für die Erbringung der Leistung erforderlich sind. Dieses sog. Koppelungsverbot ist explizit in § 28 Abs. 3b BDSG sowie spezialgesetzlich im Telekommunikationsgesetz und Telemediengesetz vorgesehen.[83] Gemäß § 28 Abs. 3b BDSG darf die verantwortliche Stelle den Abschluss eines Vertrags nicht von einer Einwilligung des Betroffenen in die Verwendung seiner Daten für Werbe- oder Markforschungszwecke abhängig machen, wenn dem

---

78 Simitis, in: Simitis (Hrsg.), BDSG, 6. Auflage, 2006, § 4a Rn. 62.

79 Simitis, in: Simitis (Hrsg.), BDSG, 6. Auflage, 2006, § 4a Rn. 16.

80 BSG, Urteil vom 10.12.2008, B 6 KA 37/07, Rn. 36.

81 BSG, Urteil vom 10.12.2008, B 6 KA 37/07, Rn. 36.

82 Theißen, Risiken informations- und kommunikationstechnischer (IKT-)Implantate im Hinblick auf Datenschutz und Datensicherheit, 2009, S. 163.

83 Zu den Vorschriften den TKG und TMG siehe Abschnitt 3.4.1.

Betroffenen ein anderer Zugang zu gleichwertigen vertraglichen Leistungen ohne die Einwilligung nicht oder nicht in zumutbarer Weise möglich ist. Dadurch soll u.a. die Situation erfasst werden, dass an sich nicht marktbeherrschende Unternehmen aufgrund von Absprachen marktweit ihre Leistungen nur anbieten, wenn der Betroffene seine Zustimmung erteilt.[84] Darüber hinaus enthält das BDSG mit dem Grundsatz der Erforderlichkeit im Zusammenhang gesehen mit der Anforderung der Freiwilligkeit bei Abgabe einer datenschutzgerechten Einwilligung ein generalisiertes Koppelungsverbot.[85] Die verantwortliche Stelle ist zwar einerseits berechtigt, die jeweils erforderlichen Daten zu verarbeiten, § 28 Abs. 1 Nr. 1 BDSG, darf aber andererseits ihre Leistungen nicht mit dem Zugriff auf weitere konkret nicht benötige Angaben verknüpfen. Daher besteht auch im BDSG, wie im Telekommunikations- und Telemedienrecht ausdrücklich vorgesehen, ein Koppelungsverbot, da jede Koppelung an eine Datenerhebung von nicht erforderlichen Daten die „freie Entscheidung" der Betroffenen in Frage stellt und damit unzulässig macht. Einwilligungen, die gegen das Koppelungsverbot verstoßen, sind daher unwirksam.[86]

Zur Freiwilligkeit gehört auch die Widerruflichkeit der Einwilligung**.** Die Widerruflichkeit der Einwilligung sichert den Betroffenen eine Einflussnahme auf den Umgang mit ihren Daten nach Beginn des Verarbeitungsvorgangs. Ein Verzicht auf das Widerrufsrecht ist nicht möglich.[87]

Herausforderungen

Problematisch kann die Einwilligung daher aus dem oben dargestellten Gründen immer dann sein, wenn die AAL-Anwendung im Rahmen einer ärztlichen Behandlung oder im Rahmen einer Pflegesituation eingesetzt wird und eine Kostenerstattung über die Kranken- bzw. Pflegeversicherung im Raum steht.

Das o.g. Koppelungsverbot steht dann im Raum, wenn unangemessene Vorteile bei der Teilnahme am AAL versprochen werden oder eine medizinische Grundversorgung im Fall der Einwilligungsverweigerung vorenthalten wird.

Offene Fragen

Offen ist, wie der Betroffene vor entsprechenden Zwangslagen und unfreiwilligen Erklärungen ausreichend geschützt werden kann bzw. muss. Hier ist zu untersuchen, inwieweit zu den allgemeinen Wirksamkeitsvoraussetzungen des § 4a BDSG zusätzliche Voraussetzun-

---

84 Patzak / Beyerlein, in: MMR 2009, S. 525.

85 Simitis, in: Simitis (Hrsg.), BDSG, 6. Auflage, 2006, § 4a Rn. 63.

86 Simitis, in: Simitis (Hrsg.), BDSG, 6. Auflage, 2006, § 4a Rn. 63 und 64.

87 Simitis, in: Simitis (Hrsg.), BDSG, 6. Auflage, 2006, § 4a Rn. 94.

gen oder Schutzvorkehrungen erforderlich sind, um einen angemessenen Schutz der Betroffenen zu erreichen, ohne in der Praxis unüberwindbare Hürden aufzustellen.

Beim Einsatz von AAL-Anwendungen stellt sich damit auch die Frage, inwieweit eine zeitlich befristete Aussetzung („Widerruf auf Zeit“) der Anwendung zwingend ermöglicht werden muss. Erhält der in seiner Wohnung Betreute z.B. Besuch, so berührt die Aufzeichnung von Daten über Sensoren auch die Persönlichkeitsrechte des Besuchers, wenn eine Unterscheidung der sich in der Wohnung aufhaltenden Personen nicht möglich ist. Hinzu kommt, dass der Nutzer selbst das Bedürfnis haben kann, seinen Besuch „ungestört“ zu empfangen, z.B. weil sein Tagesablauf sich aufgrund des Besuches so verändert, dass dies u.U. Einfluss auf die Auswertung seiner Daten und die daraus folgenden Meldungen hat oder weil ein Notrufsystem im Falle eines Besuches aufgrund dessen Anwesenheit überflüssig ist. Ein zeitliches Aussetzen der Anwendung müsste daher auf Veranlassung des Nutzers möglich sein.

3.3.2.2.4 Informationspflicht der verantwortlichen Stelle

Grundsatz

Nach § 4a Abs. 1 Satz 2 BDSG ist die verantwortliche Stelle verpflichtet, den Betroffenen rechtzeitig und umfassend über die beabsichtigte Verwendung seiner Daten zu unterrichten. Die Betroffenen müssen vor der Einwilligung alle Informationen bekommen, die notwendig sind, um Anlass, Ziel und Folgen der Verarbeitung korrekt und konkret abzuschätzen. Ein bloßes Informationsangebot oder eine Beschränkung auf weniger Informationen ist in diesem Zusammenhang nicht ausreichend:[88] Sowohl die Verarbeitungsziele als auch die Verarbeitungsfolgen lassen sich erst abschätzen, wenn die jeweils gewünschten Daten genauso wie die Verarbeitungsbedingungen und die potenziellen Übermittlungsempfänger angegeben werden. Kann ein Verarbeitungszweck nicht ausreichend spezifiziert werden, weil sich ein solcher erst aus dem Ergebnis der Datenverarbeitung ergibt, dann ist eine Legitimation der Verarbeitung durch Einwilligung nicht möglich. Raum für eine rechtsgültige Einwilligung bleibt nur dann, wenn die geplanten Datenverarbeitungsvorgänge präzise beschrieben werden, d.h., es muss klar sein, auf welche Informationen sich die Datenverarbeitung stützt, nach welchen Kriterien die Daten gespeichert und ausgewertet werden, welche Gewichtung die einzelnen Kriterien haben und was die Folge von einzelnen Auswertungen ist.[89]

Eine Einwilligung sollte immer in Kenntnis der bestehenden Risiken erfolgen, einschließlich der mittel- und langfristigen Auswirkungen auf die Persönlichkeit und die Risikoverteilung in dem sozialen Umfeld, in dem die Erklärung abgegeben wird. Je sensibler die bearbeiteten Daten sind und je weiter der Zugriffsbereich auf diese Daten ausgedehnt wird, desto höhere

88 Simitis, in: Simitis (Hrsg.), BDSG, 6. Auflage, 2006, § 4a Rn. 70 ff.

89 Roßnagel, Handbuch Datenschutzrecht, Kapitel 9.2, Rn. 123.

Anforderungen sind an eine solche Einwilligungserklärung zu stellen.[90] Die Informationspflicht erstreckt sich auch auf Angaben zu den möglichen Folgen einer Verweigerung der Einwilligung, § 4a Abs. 1 Satz 2 BDSG.[91] Bedeutung erlangt diese Information insbesondere bei Leistungen öffentlicher Stellen: Der Betroffene könnte bei einer Verweigerung der Einwilligung riskieren, bestimmte für ihn möglicherweise besonders wichtige Leistungen nicht zu bekommen.

Die Informationspflicht ist eine Bringschuld der verantwortlichen Stelle. Das Gesetz geht davon aus, dass die Einwilligung wertlos ist, solange der Betroffene nicht über ausreichende, von der verantwortlichen Stelle vermittelte Informationen verfügt.

Herausforderungen

Grundsätzlich sind die Informationen in verständlicher Form zur Verfügung zu stellen. Hierbei ist es geboten, auf die spezifische Nutzergruppe einzugehen. Jede Einwilligung im Zusammenhang mit neuen Technologien erfordert vom Nutzer eine gewisse intellektuelle Kompetenz – so auch bei der Nutzung von AAL-Anwendungen: Die Betroffenen müssen in der Lage sein, die komplexen Vorgänge der elektronischen Verarbeitung ihrer Daten in Kombination mit der AAL-Infrastruktur, also den Hintergrundsystemen in Form des Netzes, der Rechner und Systeme der Dienstleister, zu verstehen. Dann muss der Nutzer bewusst entscheiden können, welche Verarbeitungsoptionen er wünscht und welche nicht. Hierfür ist es nötig zu verstehen, welche indirekten positiven und negativen Konsequenzen eine Verarbeitung hat bzw. haben kann. Derartige Entscheidungen dürften derzeit viele Nutzer überfordern, da die damit verbundenen Interessenlagen sehr komplex sein können und die Nutzer bisher derartige Handlungsoptionen nicht kennen. Ein gewisser Lerneffekt wird sich bei vielen Nutzern mittelfristig einstellen. Dennoch wird die Fähigkeit zur Inanspruchnahme des Rechts auf informationelle Selbstbestimmung von Nutzer zu Nutzer immer stark verschieden sein.

Fehlt dem Betroffenen die nötige Medienkompetenz, so besteht die Gefahr des Fehlgebrauchs des Systems, und das Risiko eines bewussten Missbrauchs durch Dritte und damit verbunden einer Schädigung des Betroffenen erhöht sich, wenn der Betroffene nicht in der Lage ist, missbräuchliche Nutzungen zu erkennen und abzuwehren.[92] Das aktive Informieren, ggf. einschließlich besonderer Schulungen für die Betroffenen, ist nicht nur im Vorfeld der Einführung, d.h. im Zusammenhang mit der Erteilung der Einwilligung, sondern auch im Zusammenhang mit der Wahrung und Ausübung der Betroffenenrechte erforderlich. Künf-

---

90 Roßnagel, Handbuch Datenschutzrecht, Kapitel 9.2, Rn. 123 im Zusammenhang mit Data Mining.

91 Simitis, in: Simitis (Hrsg.), BDSG, 6. Auflage, 2006, § 4a Rn. 73 f.; strittig ist dabei, ob diese Information nur auf Verlangen zu erteilen ist oder zwingend erfolgen muss. Simitis favorisiert entsprechend dem Gesetzeszweck eine Informationspflicht. Dem ist zuzustimmen.

92 Weichert, Medizinische Telematik und Datenschutz, Beitrag zum 111. Deutschen Ärztetag am 22.05.2008 in Ulm, abrufbar unter: https://www.datenschutzzentrum.de/medizin/gesundheitskarte/20080522-weichert-medizinische-telematik.html..

tig wird daher die Funktion eines Lotsen über die in seinem Bereich zum Einsatz kommende AAL-Technik erforderlich sein. Diese Aufgabe könnte im medizinischen Bereich z.B. der Arzt übernehmen, wenn er ausreichend (technisch) geschult ist.

AAL-Anwendungen sind auf einen längerfristigen Einsatz ausgerichtet. Die zu Beginn erteilte Einwilligung in die Datenverarbeitung kann aus mehreren Gründen ihre Wirksamkeit einbüßen. Zum einen ist denkbar, dass die AAL-Anwendung regelmäßig weiterentwickelt wird und so die Datenverarbeitungsvorgänge modifiziert werden. Werden zum Beispiel Verhaltensprofile aufgezeichnet, so unterliegen diese naturgemäß einer gewissen Veränderbarkeit. Der Betroffene kann in diesen Fällen u.U. die Datenverarbeitungsvorgänge nicht mehr ausreichend nachvollziehen. Zum anderen ist zu fragen, ob der Betroffene nach einem gewissen Zeitablauf das Wissen über die Datenverarbeitungsvorgänge verloren hat. Zuletzt ist bei einem Abbau der kognitiven Fähigkeiten (Demenz) fraglich, ob die erforderliche Einsichtsfähigkeit weiterhin besteht.

Offene Fragen

Offen ist, wie die Nutzer von AAL-Anwendungen und -Dienstleistungen ausreichend insbesondere technisch so befähigt werden können, dass sie ihr Recht auf informationelle Selbstbestimmung auch tatsächlich wahrnehmen können. Es ist daneben zu klären, inwieweit Treuhänder oder Paten die Nutzer unterstützen können und wie sich die Einschaltung von unterstützenden Personen auf die jeweiligen Verantwortlichkeiten auswirkt.

3.3.2.2.5 Bestimmtheit der Einwilligung

Grundsatz

Die o.g. Informationspflicht bzw. die erforderliche Informiertheit des Betroffenen bei Abgabe seiner Erklärung steht in einem engen Zusammenhang mit dem Erfordernis der Bestimmtheit der Einwilligungserklärung. Die Einwilligung muss in allen Punkten (wer übermittelt wann was an wen zu welchem Zweck) so bestimmt sein, dass für den Betroffenen eindeutig erkennbar ist, was mit seinen Daten geschieht. Nur wer das überblickt, ist hinreichend informiert, um wirksam einwilligen zu können.[93] Aus der Einwilligungserklärung muss sich klar erkennen lassen, unter welchen Bedingungen sich der Betroffene mit der Verarbeitung welcher Daten einverstanden erklärt hat. Weder Blankoeinwilligungen noch pauschal gehaltene Erklärungen, die dem Betroffenen die Möglichkeit nehmen, die Tragweite ihres Einverständnisses zu überblicken, sind deshalb mit § 4a BDSG vereinbar. Auch mutmaßliche Einwilligungen, stillschweigende oder konkludente Erklärungen genügen nicht den Anforderungen. Dass solche Einwilligungen bei der Durchbrechung der ärztlichen Schweigepflicht jedenfalls

[93] § 4a Abs. 1 Satz 2 BDSG; BGH NJW 1992, 2348, 2350.

zwischen vor- und nachbehandelnden Ärzten ausreichen, ist hier unerheblich, da beide Rechtsgebiete, das Recht der ärztlichen Schweigepflicht und das Datenschutzrecht, nebeneinander Anwendung finden.[94] Wie spezifiziert die Einwilligung sein muss, lässt sich nur vor dem Hintergrund der konkreten Verarbeitungssituation beurteilen. In jedem Fall muss die Erklärung Informationen über die zu verarbeitenden Daten sowie die gebilligten Verarbeitungsziele und Verarbeitungsphasen enthalten. Soweit eine Übermittlung in Betracht kommt, muss sich zusätzlich aus der Einwilligung ergeben, wem konkret die Daten zugänglich gemacht werden dürfen.[95]

Die Bestimmtheit der Erklärung im Zusammenspiel mit der erforderlichen Information durch die Daten verarbeitende Stelle ist eine Grundvoraussetzung für eine echte Einflussnahme der Betroffenen, die durch die Einwilligung gewährleistet werden soll. Nur wenn die Betroffenen die Datenverarbeitungsvorgänge tatsächlich kennen, können sie auch effektiv auf diese Einfluss nehmen. Dazu gehört auch, dass eine Einsichtnahme der Betroffenen in ihre vom System verarbeiteten Daten möglich ist.

Herausforderungen

Das Konzept AAL ist vielfach darauf ausgerichtet, erhobene Daten zu verbinden bzw. zu vernetzen, um sie auszuwerten und daraus Konsequenzen ziehen zu können (d.h. insbesondere um bestimmte Hilfsmaßnahmen einzuleiten). Dies bedeutet eine hohe Komplexität der Verfahren und eine Verarbeitung von einer Vielzahl von Daten. AAL-Anwendungen beabsichtigen eine unaufdringliche, von dem Nutzer möglichst unbemerkte Hilfestellung. Die Betroffenen sollen im Alltag möglichst unauffällig unterstützt werden. Dies führt zu einer weitgehend unbemerkten Erhebung, Auswertung und Weiterleitung von Daten.

Angesichts der neuen, im Regelfall im Hintergrund arbeitenden sehr komplexen Techniken stößt das Instrument der Einwilligung an seine Grenzen, und eine Sicherstellung, dass schon zum Erhebungszeitpunkt alle Datenverarbeitungsvorgänge einschließlich der Übermittlungen und Zugriffe bekannt sind und dem oben dargestellten Bestimmtheitsgrad gerecht werden kann, ist teilweise in der Praxis sicherlich unmöglich. Aus diesem Grund ist zu klären, inwieweit bei der Einwilligungsregelung des BDSG Anpassungen notwendig sind, die gleichzeitig praxisgerecht sind und nicht dem Sinn der Einwilligung zuwiderlaufen. Wie spezifiziert die Einwilligung sein muss, lässt sich auch bei AAL-Anwendungen nur vor dem Hintergrund der konkreten Verarbeitungssituation beurteilen.[96]

---

[94] Dazu auch Abschnitt 3.4.2.2.1.

[95] Simitis, in: Simitis, (Hrsg.), BDSG, 6. Auflage, 2006, § 4a Rn. 80.

[96] Schurig, Datenschutzrechtliche Aspekte bei telemedizinischen Anwendungen, in: Rechtliche Aspekte der Telemedizin, 2006, S. 39.

Daneben sind zusätzlich zu den allgemeinen Wirksamkeitsvoraussetzungen einer datenschutzrechtlichen Einwilligung weitere Zulässigkeitsbedingungen aufzustellen, um den Betroffenen vor Zwangslagen und unbedachten Erklärungen zu schützen. Hier ist zum Beispiel an eine Abstufung des Einwilligungsumfangs und des Einwilligungszwecks, an eine entsprechend angepasste Information und Aufklärung der Betroffenen und ggf. an eine Standardisierung der Einwilligung zu denken.

Offene Fragen

Es ist die offene Frage zu untersuchen, inwieweit die Einwilligungsregelung des BDSG einer Anpassung bedarf, die einerseits keine Hürden aufbaut, die die Praxis überfordern, andererseits jedoch dem Betroffenen ausreichend Schutz gewährt. Ziel muss es sein, die unbemerkte, unsichtbare, im Hintergrund laufende Datenerhebung und -auswertung für den Betroffenen dennoch erkennbar zu machen, um seine Steuerungsmöglichkeiten nicht einzuschränken. In diesem Zusammenhang ist auch zu klären, inwieweit das Instrument der Delegation (siehe Kapitel 7) hilfreich sein kann und wo es an seine Grenzen stößt.

3.3.2.2.6 Besonderheiten im öffentlichen Bereich

Zu berücksichtigen ist, dass im öffentlichen Bereich für eine Einwilligung dort kein Raum ist, wo eine spezielle gesetzliche Vorschrift eine konkrete Datenverarbeitung regelt und die Voraussetzungen für die Datenverarbeitung im Einzelfall nicht gegeben sind.[97] Zu prüfen ist daher, ob der Gesetzgeber explizit geregelt hat, für welche Aufgaben die ausführende Stelle welche personenbezogenen Daten erheben darf – und damit implizit auch, welche Daten zur Erfüllung der Aufgaben nicht erforderlich sind.[98] Versuchen öffentliche Stellen durch das Abfordern von Einwilligungen der Betroffenen die gesetzliche Regelung zu umgehen, so stellt dies einen Rechtsmissbrauch dar, der die Unwirksamkeit der Einwilligung zur Folge hat.[99]

---

97 BSG, Urteil vom 10.12.2008, B 6 KA 37/07, Rn. 18.

98 BSG, Urteil vom 10.12.2008, B 6 KA 37/07, Rn. 19.

99 21. Tätigkeitsbericht des Bundesbeauftragten für den Datenschutz und die Informationsfreiheit (BfDI) 2005-2006, S. 131; Stellungnahme des BfDI abrufbar unter: http://www.bfdi.bund.de/cln_029/nn_531474/DE/Themen/GesundheitUndSoziales/KrankenPflegeversicherung/Artikel/Krankenhausentlassungsberichte.html__nnn=true: „Auf Grund der spezialgesetzlichen Regelungen im SGB V besteht für die Anwendung des § 100 SGB X – soweit es die Übermittlung von Krankenhausentlassungsberichten angeht – kein Raum; dies gilt auch für die zweite Alternative in § 100 Abs. 1 Satz 1 SGB X, nach der eine Übermittlung durch den Arzt dann zulässig ist, wenn der Betroffene im Einzelfall eingewilligt hat. Die Einholung einer Einwilligungserklärung des Versicherten zur Übermittlung der vorgenannten Unterlagen an die Krankenkasse wäre eine Umgehung der gesetzlichen Regelung zur Prüfung der medizinischen Sachverhalte durch den Medizinischen Dienst der Krankenversicherung (MDK). Aus diesem Grunde halte ich die Forderungen der Krankenkassen an Krankenhäuser und Ärzte, bei Vorliegen einer Einwilligungserklärung des Versicherten die vorgenannten Unterlagen an die Krankenkassen zu übermitteln, für rechtlich nicht zulässig."

Gleichermaßen ist eine Einwilligung, die den gesetzlichen Aufgabenbereich erweitert, unwirksam.[100] Krankenkassen und Pflegeversicherungen dürfen daher personenbezogene Daten nur im Rahmen ihrer gesetzlichen Befugnisse erheben. Darüber hinaus dürfen sie weder direkt auf freiwilliger Basis noch indirekt bei den Ärzten über entsprechende Schweigepflichtentbindungserklärungen zusätzliche Daten erheben.[101] Eine Einwilligung in eine über die gesetzlichen Befugnisse hinausgehende Datenverarbeitung ist nach dem Willen des Gesetzgebers unzulässig.

3.3.2.2.7 Besonderheiten in der wissenschaftlichen Forschung

Nach § 4a Abs. 2 BDSG kann im Rahmen wissenschaftlicher Forschung auf die Schriftlichkeit der Einwilligung verzichtet werden. Voraussetzung ist, dass es sich um eine wissenschaftliche Tätigkeit handelt, die nicht notwendigerweise an eine Forschungseinrichtung angebunden sein muss, und dass durch das Verlangen der schriftlichen Einwilligung der konkrete Forschungszweck beeinträchtigt würde. Es ist in einem solchen Fall weiterhin notwendig, dass der Hinweis auf den vorgesehenen Zweck der Erhebung, Verarbeitung oder Nutzung sowie, soweit nach den Umständen des Einzelfalls erforderlich oder auf Verlangen, auf die Folgen der Verweigerung der Einwilligung erfolgt und schriftlich festzuhalten ist. Ebenso müssen die Gründe, aus denen sich die erhebliche Beeinträchtigung des bestimmten Forschungszwecks ergibt, schriftlich dokumentiert werden.

3.3.3 Grundsatz der Zweckbindung

Grundsatz

Personenbezogene Daten dürfen nur für den Zweck verwendet werden, für den sie erhoben worden sind.[102] Dieser Grundsatz sichert für den Betroffenen die Transparenz der Erhebung, Verarbeitung und Nutzung seiner personenbezogenen Daten.[103] Eine über den Erhebungszweck hinausgehende Nutzung oder Verarbeitung der personenbezogenen Daten des Betroffenen ist ohne seine Einwilligung oder eine weitere Erlaubnisnorm nicht zulässig. Bereits bei der Erhebung personenbezogener Daten sind die Zwecke, für die die Daten verarbeitet oder genutzt werden sollen, konkret festzulegen (vgl. § 28 Abs. 1 Satz 2 BDSG). Für jede

---

[100] Simitis, in: Simitis (Hrsg.), BDSG, 6. Auflage, 2006, § 4a, 79 Rn. 15.

[101] Vgl. 21. Tätigkeitsbericht des Bundesbeauftragten für den Datenschutz und die Informationsfreiheit 2005-2006, S. 131.

[102] §§ 28, 29 BDSG, § 12 Abs. 2 TMG.

[103] Vgl. BVerfGE 65, 1, 46: Das Bundesverfassungsgericht hat in dieser Entscheidung „eine Gesellschaftsordnung und eine diese ermöglichende Rechtsordnung (als) … mit dem Recht auf informationelle Selbstbestimmung … nicht vereinbar“ bezeichnet, „in der Bürger nicht mehr wissen können, wer was wann und bei welcher Gelegenheit über sie weiß“. Ein ausreichendes Wissenkönnen soll nicht zuletzt dadurch erreicht werden, dass der Gesetzgeber jeweils den Verwendungszweck bereichsspezifisch und präzise bestimmt.

Zweckänderung ist daher erneut eine Einwilligung des Betroffenen oder eine Rechtsgrundlage erforderlich. Dies gilt auch für die geschäftsmäßige Datenverarbeitung (vgl. § 29 Abs. 1 Satz 2 BDSG).

Ausnahmsweise kommt eine Verwendung für andere Zwecke gem. § 28 Abs. 2 und 3 BDSG in Betracht zur Wahrung berechtigter Interessen der verantwortlichen Stelle, wenn die Daten allgemein zugänglich sind oder veröffentlicht werden dürften, zu wissenschaftlichen Zwecken oder für Zwecke der Werbung sowie der Markt- oder Meinungsforschung bei listenmäßiger Übermittlung. Erforderlich ist nach Maßgabe des Gesetzes stets eine Abwägung zwischen den entgegenstehenden schutzwürdigen Interessen des Betroffenen und dem Interesse an der Zweckänderung.

Herausforderungen

Zum einen stellen sich entsprechende Herausforderungen wie bei der Bestimmtheit der Einwilligungserklärung (siehe Abschnitt 3.3.2.2.5), wenn eine ausreichend präzise Zweckbeschreibung in der Praxis an ihre Grenzen stößt. Zum anderen betrifft die Gewährleistung einer Zweckbindung die Gestaltung von AAL-Systemen, -Anwendungen und -Dienstleistungen, denn es werden in vielen Fällen langjährige Profile über das Verhalten der Betroffenen entstehen, die – zweckändernd bzw. über den konkreten ursprünglichen Zweck hinausgehend – für neue Angebote der AAL-Systemhersteller oder -Dienstleistungsanbieter herangezogen werden könnten. Die Herausforderung besteht daher in einer Gestaltung der Technik und Organisation, so dass die Zweckbindung tatsächlich eingehalten wird (siehe die Ausführungen zu einer Nichtverkettbarkeit in Abschnitt 4.2.3.6).

Offene Fragen

Abgesehen von der offenen Frage, wie ausreichend präzise Zweckbeschreibungen für Einwilligungserklärungen geeignet dargestellt werden können, ist zu untersuchen, unter welchen Umständen Zweckänderungen in Bezug auf die oft sensiblen AAL-Daten überhaupt zugelassen sein können. Daneben besteht eine offene Frage in den konkreten Anforderungen, die bereits an den Entwurf und die Implementierung von AAL-Systemen sowie an die Gestaltung von AAL-Anwendungen und -Dienstleistungen zu stellen sind, um eine Zweckbindung tatsächlich bestmöglich umzusetzen. Die Klärung dieser Frage ist umso wichtiger, als heutige Realisierungen technischer Systeme in der Regel auf Maximierung der zweckübergreifenden Nutzungsmöglichkeiten ausgerichtet sind, anstatt eine Beschränkung auf eng zugeschnittene Zwecke zu implementieren.

3.3.4 Grundsatz der Erforderlichkeit

Grundsatz

Ein weiterer fundamentaler Grundsatz des Datenschutzrechts ist der Grundsatz der Erforderlichkeit der Datenverarbeitung, der in einem engen Zusammenhang mit der Zweckbindung steht. Er bedeutet, dass nur diejenigen Daten erhoben, verarbeitet und genutzt werden dürfen, die für den jeweilig festgelegten Zweck erforderlich sind. Eine über den Zweck hinausgehende Erhebung personenbezogener Daten ist nicht zulässig. Im Ergebnis bedeutet dies, dass für jeden Vorgang erneut überprüft werden muss, welche Daten für diesen Vorgang überhaupt notwendig sind und ob eventuell auf einen Personenbezug verzichtet werden kann und die Daten dementsprechend anonymisiert oder pseudonymisiert werden können.[104]

Weiter beinhaltet dieser Grundsatz, dass die jeweils einschlägigen Löschungsfristen eingehalten werden. Nicht mehr benötigte Daten sind zu löschen. Damit korrespondiert ein Anspruch des Betroffenen auf Löschung solcher Daten. Die Löschung ist Dritten, denen die Daten übermittelt worden sind, mitzuteilen, sofern sich dies nicht als unmöglich erweist oder kein unverhältnismäßiger Aufwand damit verbunden ist. Keiner Frist zur Löschung unterliegt im Übrigen die Aufbewahrung von Daten, die keinen Personenbezug aufweisen, z.B. indem sie anonymisiert worden sind.

Herausforderungen

Der Grundsatz der Erforderlichkeit ist bei jedem Datenverarbeitungsvorgang im Rahmen einer AAL-Anwendung zu beachten. Für den Hersteller bedeutet dies zum Beispiel, dass dieser in jeder Phase die Erforderlichkeit von Daten und deren etwaigem Personenbezug zu prüfen und die technischen Vorkehrungen zu schaffen hat, so dass Daten nur in dem erforderlichen Umfang erhoben, verarbeitet und genutzt werden. Eine ständige und anhaltend mögliche Verfügbarkeit aller erhobenen Daten ist in den seltensten Fällen erforderlich. Daraus folgt insbesondere, dass personenbezogene Daten, die für Vorgänge nicht erforderlich sind, zu löschen sind und nicht auf Vorrat gehalten (siehe auch Abschnitt 3.3.11) werden dürfen.

Offene Fragen

Es ist zu prüfen, durch welche Maßnahmen dem Grundsatz der Erforderlichkeit Nachhaltigkeit verliehen werden kann. In Betracht kommen hier insbesondere technische Möglichkeiten

[104] Bei der Erfüllung von gesetzlichen Aufgaben durch öffentliche Stellen bedeutet dies, dass nur die personenbezogenen Informationen verarbeitet werden dürfen, ohne die die Aufgabe nicht, nicht vollständig oder nicht in rechtmäßiger Weise erfüllt werden kann. Dass die Datenverarbeitung zur Erfüllung der Aufgabe geeignet und zweckmäßig ist, ist nicht ausreichend, vgl. Dammann, in: Simitis (Hrsg.), BDSG, 6. Auflage, 2006, § 14 Rn. 15.

der Pseudonymisierung und Anonymisierung von personenbezogenen Daten in AAL-Anwendungen, die untersucht werden sollten. Darüber hinaus muss analysiert werden, welche Möglichkeiten sich durch die kryptographischen Verfahren der anonymen Credentials[105] eröffnen, die es erlauben, die jeweils erforderlichen Daten stark einzuschränken. Insbesondere ermöglichen solche Credentials, dass die Nutzung einer Anwendung auf die Berechtigten limitiert wird, ohne dass die Nutzer ihre personenbezogenen Daten vorzeigen müssen oder die Nutzungsvorgänge verkettbar sind.

3.3.5 Grundsatz der Datenvermeidung und Datensparsamkeit

Grundsatz

Konkretisiert wird das Erforderlichkeitsprinzip durch den Grundsatz der Datenvermeidung und -sparsamkeit. Ein entsprechender Grundsatz ist explizit sowohl im BDSG als auch im SGB aufgenommen.[106] Hiernach haben sich Gestaltung und Auswahl von Datenverarbeitungssystemen an dem Ziel auszurichten, keine (Datenvermeidung) oder so wenig personenbezogene Daten wie möglich (Datensparsamkeit) zu erheben, zu verarbeiten oder zu nutzen. Dabei ist insbesondere von den Möglichkeiten der Anonymisierung und Pseudonymisierung Gebrauch zu machen.

Hierbei handelt es sich – im Gegensatz zum Grundsatz der Erforderlichkeit, der eine zwingende rechtliche Anforderung darstellt – um eine Gestaltungsanforderung an IT-Systeme. Nach dem Willen des Gesetzgebers soll die Regelung dazu führen, dass durch den gezielten Einsatz datenschutzfördernder Technik die Gefahren für das informationelle Selbstbestimmungsrecht der Betroffenen reduziert werden.[107] Es handelt sich um einen Grundsatz, der Ausdruck des sog. Systemdatenschutzes ist, mit dem die Unterstützung des Datenschutzes durch Technik umgesetzt wird. Der Systemdatenschutz dient dazu, den möglichen Einschränkungen der Privat- und Intimsphäre durch dynamische Technikentwicklung, allgegenwärtige elektronische Datenverarbeitung, für den Einzelnen unübersichtliche Strukturen, un-

---

[105] Camenisch / Lysyanskaya, Efficient Non-transferable Anonymous Multi-show Credential System with Optional Anonymity Revocation, in: Advances in Cryptology – Eurocrypt 2001, S. 93-118.

[106] § 3a BDSG – Datenvermeidung und Datensparsamkeit: „Die Erhebung, Verarbeitung und Nutzung personenbezogener Daten und die Auswahl und Gestaltung von Datenverarbeitungssystemen sind an dem Ziel auszurichten, so wenig personenbezogene Daten wie möglich zu erheben, zu verarbeiten oder zu nutzen. Insbesondere sind personenbezogene Daten zu anonymisieren oder zu pseudonymisieren, soweit dies nach dem Verwendungszweck möglich ist und keinen im Verhältnis zu dem angestrebten Schutzzweck unverhältnismäßigen Aufwand erfordert."; § 78b SGB X – Datenvermeidung und Datensparsamkeit: „Gestaltung und Auswahl von Datenverarbeitungssystemen haben sich an dem Ziel auszurichten, keine oder so wenig Sozialdaten wie möglich zu erheben, zu verarbeiten oder zu nutzen. Insbesondere ist von den Möglichkeiten der Anonymisierung und Pseudonymisierung Gebrauch zu machen, soweit dies möglich ist und der Aufwand in einem angemessenen Verhältnis zu dem angestrebten Schutzzweck steht."

[107] BT-Drs. 14/4329, S. 30.

bemerkte Datenerhebungen und undurchschaubare Verarbeitungsformen zu begegnen.[108] Die Anforderungen des Konzepts des Systemdatenschutzes zielen auf eine technische und organisatorische Gestaltung des gesamten Systems der Datenverarbeitung. Im Ergebnis sind diese so zu gestalten, dass auch „technikbedingt" keine für die Zweckerreichung nicht erforderlichen personenbezogenen Daten erhoben, verarbeitet und genutzt werden. Beispielsweise ist jeweils zu prüfen, ob technisch bedingt entstehende temporäre Dateien, die personenbezogene Daten enthalten, erforderlich sind und umgehend gelöscht werden. Außerdem kommt der Vermeidung von eindeutigen Kennungen, die durch eine Verkettung eine übergreifende Profilbildung von einzelnen Personen ermöglichen, eine besondere Bedeutung zu.

Das Ziel der Datenvermeidung kann auch durch Abstufungen auf der Ebene der Verarbeitungsschritte, insbesondere des Erhebens, Speicherns, Veränderns, Übermittelns oder Nutzens erreicht werden. Als Beispiel lässt sich der Fall anführen, personenbezogene Daten zu erheben und zu speichern, aber ohne Personenbezug an Dritte zu übermitteln.[109] Ein Beispiel für die weitere in der Vorschrift genannte Alternative der Datensparsamkeit wäre der Fall, dass personenbezogene Daten lediglich kurzzeitig oder vorübergehend erhoben und gespeichert, aber unmittelbar nach ihrer Nutzung wieder gelöscht werden.[110]

Herausforderungen

Bei der Realisierung von AAL-Anwendungen ist der Grundsatz der Datenvermeidung und Datensparsamkeit von großer Bedeutung. Angesichts der insbesondere mit der Aufzeichnung von Verhaltensprofilen verbundenen Risiken für das Recht auf informationelle Selbstbestimmung muss bereits bei der Entwicklung solcher Anwendungen darauf geachtet werden, möglichst datensparsame Verfahren vorzusehen bzw. das Augenmerk darauf zu richten, zur Erreichung des vorgesehenen Zwecks so wenig wie überhaupt möglich personenbezogene Daten zu erheben und zu verarbeiten.

Offene Fragen

Es ist zu untersuchen, inwieweit der Grundsatz der Datenvermeidung und Datensparsamkeit bereits bei Entwicklung von AAL-Anwendungen Gewicht verliehen werden kann. Bislang haben diese rechtlichen Anforderungen an die Technikgestaltung kaum einen merkbaren Effekt gehabt. Dies bedeutet, dass auf dem Markt kaum Produkte zur Verfügung stehen, die sich an dem Grundsatz der Datenvermeidung und Datensparsamkeit ausrichten. Viele Hersteller, gerade im internationalen Bereich, werden diese Anforderung gar nicht kennen und

---

[108] Roßnagel / Pfitzmann / Garstka, Modernisierung des Datenschutzrechts, Gutachten im Auftrag des Bundesministeriums des Innern, 2001, S. 39.

[109] Bizer, in: Simitis (Hrsg.), BDSG, 6. Auflage, 2006, § 3a Rn. 57.

[110] Bizer, in: Simitis (Hrsg.), BDSG, 6. Auflage, 2006, § 3a Rn. 64.

auch keine Anreize sehen, ihre Produkte umzugestalten, da sie weder eine signifikante Nachfrage der Anwender spüren noch Aufsichtsbehörden bislang in diesem Punkt Druck haben ausüben können. Noch ist offen, wie ein austariertes System aus Anreizen und Sanktionen auf mindestens europäischer Ebene aussehen könnte und wie es umsetzbar wäre.

Weiterhin besteht ein Forschungsbedarf in Bezug auf Technik, die sich am Grundsatz der Datenvermeidung und Datensparsamkeit orientiert. Dies betrifft beispielsweise den kombinierten Einsatz von Komponenten, die jeweils für sich unproblematisch sind oder sogar den Grundsatz der Datensparsamkeit umsetzen: In der Kombination dieser Komponenten können sich Verkettungsmöglichkeiten ergeben, die aus Datenschutzsicht überaus problematisch sein können.

Schließlich sei hier erneut auf die noch zu prüfenden Möglichkeiten der „anonymen Credentials“ verwiesen, wie bereits in Abschnitt 3.3.4 erläutert.

3.3.6 Grundsatz der Transparenz

Grundsatz

Eine wirksames Recht auf informationelle Selbstbestimmung setzt voraus, dass eine betroffene Person in der Lage ist, sich zu informieren, „wer was wann und bei welcher Gelegenheit über sie weiß“.[111] Für den Betroffenen müssen die Erhebung, Verarbeitung einschließlich der Übermittlung seiner personenbezogenen Daten und die Nutzung transparent sein. Nur eine derartige Transparenz erlaubt es dem Betroffenen, die Kenntnisse seines Gegenüber einzuschätzen, hierüber Auskunft zu verlangen und bei unvollständigen, fehlerhaften, unrechtmäßig erhobenen oder widersprüchlichen Daten Ansprüche auf Berichtigung, Löschung oder Sperrung geltend zu machen. Diese Transparenz soll mittels zahlreicher Instrumente, die im BDSG und den bereichsspezifischen Vorschriften zu finden sind, erreicht werden, d.h. insbesondere mittels Unterrichtungspflichten, Benachrichtigungspflichten sowie Anzeige- und Informationspflichten über Ziele und Datenverarbeitungsvorgänge bis hin zu Auskunftsrechten der betroffenen Personen:[112]

- Zunächst hat die verantwortliche Stelle, wenn sie beim Betroffenen Daten erhebt, diesen gemäß § 4 Abs. 3 BDSG über die Identität der verantwortlichen Stelle, die Zweckbestimmung der Datenverarbeitung und ggf. über die Kategorien von Empfängern zu unterrichten.
- Personenbezogene Daten müssen außerdem im Regelfall direkt bei der betroffenen Person erhoben werden (Grundsatz der Direkterhebung). Werden die personenbezoge-

[111] BVerfGE 65, 1 ff.

[112] Zu den weiteren Betroffenenrechten siehe Abschnitt 3.3.9.

nen Daten nicht direkt beim Nutzer erhoben, so ist dieser nachträglich darüber zu benachrichtigen, welche Daten zu welchem Zweck erhoben, verarbeitet und genutzt werden.[113]

- Weiter muss im Fall eines Datenlecks und der unzulässigen Kenntnisnahme von sensiblen Daten durch Dritte gemäß § 42a BDSG eine Benachrichtigung, die sog. Breach Notification, an die zuständige Aufsichtsbehörde sowie an die Betroffenen erfolgen.
- Zudem hat der Betroffene nach § 34 Abs. 1 BDSG Anspruch auf Auskunft über die zu seiner Person gespeicherten Daten, die Herkunft dieser Daten, den Empfänger oder die Kategorien von Empfängern, an die Daten weitergegeben werden, und den Zweck der Speicherung.
- Im Fall von Scoring, d.h. dem Errechnen eines Wahrscheinlichkeitswerts für ein bestimmtes zukünftiges Verhalten eines Betroffenen (siehe § 28b BDSG), sind ihm auf Verlangen weitere Informationen zu geben, insbesondere über das Zustandekommen des Werts, § 34 Abs. 2 BDSG.

Weitere Verpflichtungen zur Auskunft an den Betroffenen sind beispielsweise § 34 BDSG zu entnehmen. Darüber hinaus kann die zuständige Aufsichtsbehörde Informationen über die verarbeiteten personenbezogenen Daten und eingesetzten Verfahren verlangen.

Herausforderungen

Ziel von AAL-Anwendungen ist es, möglichst ohne Zutun des Betroffenen und damit möglichst unbemerkt und im Hintergrund tätig zu werden und zu wirken. Diese Form der Datenerhebung stellt aber das Gegenteil dessen dar, was die Vorschriften über Transparenz bezwecken. Wenn AAL-Anwendungen umfassend und allgegenwärtig zum Einsatz kommen, diese allgegenwärtige Datenverarbeitung zudem im Hintergrund stattfindet und unmerklich den Menschen bei vielen Alltagshandlungen unterstützt, stößt das bisherige Prinzip der Transparenz an seine Grenzen. Die Wahrnehmungsfähigkeit der Betroffenen droht überfordert zu werden.[114]

Nicht praktikabel und unzumutbar ist sicherlich eine permanente Anzeige aller Datenverarbeitungsvorgänge bei alltäglichen Erhebungen und Verarbeitungen. Eine undifferenzierte Umsetzung von Transparenzregelungen wäre daher nicht sachgerecht und für eine Verbreitung und Durchsetzung der Technik sogar kontraproduktiv. Verzichtet man jedoch gänzlich

[113] § 33 BDSG: So ist die verantwortliche Stelle nach § 33 Abs. 1 BDSG verpflichtet, den Betroffenen bei erstmaliger Speicherung bzw. bei erstmaliger Übermittlung ohne seine Kenntnis diesen über die Art der Daten, der Zweckbestimmung der Erhebung, Verarbeitung oder Nutzung und der Identität der verantwortlichen Stelle zu benachrichtigen. Damit soll gewährleistet werden, dass die Betroffenen ihre Datenschutzrechte geltend machen können.

[114] Roßnagel, Datenschutz in einem informatisierten Alltag, Gutachten im Auftrag der Friedrich-Ebert-Stiftung, 2007, S. 133, abrufbar unter: http://library.fes.de/pdf-files/stabsabteilung/04548.pdf.

auf derartige Informationen, werden die Betroffenen gar nicht mehr wissen können, welche Handlungen beobachtet und registriert und welche Datensammlungen zusammengeführt werden.[115]

Durch die komplexen und vielfältigen Zwecke der Datenverarbeitung in einer Welt, in der smarte Gegenstände miteinander kommunizieren, werden der Transparenz auch in weiterer Hinsicht objektive Grenzen gesetzt.[116] Ein Auskunftsverlangen setzt nämlich voraus, dass der Betroffene die für die Datenverarbeitung verantwortliche Stelle ausfindig machen kann, da nur diese zur Auskunftserteilung verpflichtet ist. Wenn eine Datenbeschaffung bei unterschiedlichen Stellen stattfindet, die anschließende komplexe Auswertung mit mehrstufigen Veränderungen und Übermittlungen wiederum an anderen Stellen erfolgt und nicht vollständig oder gar nicht protokolliert wird, wird die Durchsetzung des Auskunftsanspruchs massiv gefährdet. Diese Probleme gelten insbesondere auch für den Einsatz von AAL-Anwendungen im medizinischen und pflegerischen Bereich. Dort erhebt zwar im Regelfall der Arzt die Daten. Neben diesem sind jedoch häufig weitere verantwortliche Stellen mit verteilten Rollen beteiligt, beispielsweise konsultierte Ärzte, Krankenhäuser, Kompetenzzentren, die die Daten aufbereiten, Krankenkassen usw. Der Betroffene läuft Gefahr, den Überblick zu verlieren, bei welchen Stellen er seinen Auskunftsanspruch geltend machen kann.[117]

Offene Fragen

Es ist eine offene Frage, wie für die Nutzer Transparenz in Bezug auf die Verarbeitung ihrer personenbezogenen Daten geschaffen werden kann. Insoweit ist zu prüfen, inwieweit die Beteiligten selbst einen umfassenden Einblick in die Erhebung, Verarbeitung und Nutzung ihrer eigenen Daten erhalten können.

Daneben ist zu untersuchen, wie eine einfache, verständliche und zusammengefasste Form der Informationen für alle zu erreichen ist, sowohl vor Implementierung von AAL-Anwendungen als auch in begleitender Form bei langfristigem Einsatz. Verständlich formulierte Datenschutz-Policies (verbindliche Leitlinien) könnten hier ein wirksames Mittel sein. Zu prüfen wäre, wie sich die relevanten Informationen zielgruppengerecht und abgestuft – je nach Interesse könnte man weitere Informationen ein- oder ausblenden – darstellen ließen.

Grundvoraussetzung für eine Transparenz gegenüber dem Nutzer ist eine Transparenz der Datenverarbeitung bei der verantwortlichen Stelle. Dies ist leider nicht in allen Fällen gege-

---

115 Roßnagel, Datenschutz in einem informatisierten Alltag, Gutachten im Auftrag der Friedrich-Ebert-Stiftung, 2007, S. 133; Unabhängiges Landeszentrum für Datenschutz / Humboldt-Universität Berlin, TAUCIS – Technikfolgenabschätzung Ubiquitäres Computing und Informationelle Selbstbestimmung, Studie im Auftrag des Bundesministeriums für Bildung und Forschung, S. 208, abrufbar unter https://www.datenschutzzentrum.de/taucis/.

116 CR 2004, S. 629.

117 Weichert, in: DuD 2006, S. 695.

ben. Eine offene Frage besteht darin, wie sichergestellt werden kann, dass die Hersteller und Betreiber der AAL-Systeme alle relevanten Informationen – möglichst standardisiert – zur Verfügung stellen, damit sowohl die verantwortliche Stelle als auch die zuständige Datenschutzaufsichtsbehörde beurteilen können, ob die rechtlichen Anforderungen korrekt umgesetzt sind.

3.3.7 Grundsatz der klaren Verantwortlichkeit

Grundsatz

Die datenschutzrechtlichen Pflichten richten sich jeweils an die für die Datenverarbeitung verantwortliche Stelle.[118] Eine der Kernfragen des Datenschutzrechts ist daher, wer datenschutzrechtlich verantwortlich ist – insbesondere in einem verteilten bzw. vernetzten System der Datenverarbeitung. Eine der zentralen Aufgaben vor Etablierung eines AAL-Systems ist daher eine eindeutige Klärung der datenschutzrechtlichen Verantwortlichkeit, die nicht auf den Betroffenen abgewälzt werden kann und darf.

Grundsätzlich kann auch der Betroffene selbst der datenschutzrechtlich Verantwortliche für bestimmte Verfahren sein, wenn er Zugriff auf die Datenverarbeitungsvorgänge hat, diese steuern kann und personenbezogene Daten Dritter (z.B. Besucher) von ihm verarbeitet werden.

Verantwortliche Stelle gemäß § 3 Abs. 7 BDSG ist jede Person oder Stelle, die personenbezogene Daten für sich selbst erhebt, verarbeitet oder nutzt oder dies durch andere im Auftrag vornehmen lässt. Verantwortlich ist danach die Stelle, die die tatsächliche Verfügungsmacht über die Daten hat oder an einen Dienstleister, den Auftragsdatenverarbeiter, delegiert hat.[119]

Damit ist Verantwortung nicht auf den eigenen tatsächlichen Herrschaftsbereich beschränkt, sondern erstreckt sich auch auf die Auftragsdatenverarbeitung (s.u.). Bei einer solchen Auftragsverarbeitung bleibt der Auftraggeber gem. § 11 BDSG für die Einhaltung der Vorschriften über den Datenschutz verantwortlich. Dies bedeutet, dass durch die Beauftragung und Einschaltung Dritter sich der Auftraggeber nicht seiner datenschutzrechtlicher Verantwortlichkeit entziehen kann. In Folgenden werden die Verantwortlichkeiten bei einer Auftragsda-

---

[118] Dammann, in: Simitis (Hrsg.), BDSG, 6. Auflage, 2006, § 3 Rn. 224.

[119] Für die Feststellung, ob es sich in bestimmten Konstellationen um eine Datenverarbeitung im Auftrag im datenschutzrechtlichen Sinne handelt, kann auf das Arbeitspapier WP 169 der Art. 29-Datenschutzgruppe, „Stellungnahme 1/2010 zu den Begriffen ‚für die Verarbeitung Verantwortlicher' und ‚Auftragsverarbeiter'" vom Februar 2010 zurückgegriffen werden (abrufbar unter: http://ec.europa.eu/justice_home/fsj/privacy/docs/wpdocs/2010/wp169_de.pdf). Das deutsche Datenschutzrecht wird in wesentlichen Teilen durch die Richtlinie 95/46/EG vorgegeben; dies gilt auch für die Vorschriften zur Auftragsdatenverarbeitung (vgl. Art. 17 der Richtlinie). Diese Hinweise sind daher für eine europarechtskonforme Auslegung auch des deutschen Datenschutzrechts zu berücksichtigen.

tenverarbeitung, bei automatisierten Abrufverfahren sowie bei Verbunddateien und vernetzten Systemen beschrieben. Schließlich werden Herausforderungen und offene Fragen in Bezug auf die datenschutzrechtliche Verantwortlichkeit abgeleitet.

Verantwortlichkeiten bei einer Auftragsdatenverarbeitung

AAL-Verfahren und komplexer werdende IT-Infrastruktur bringen es mit sich, dass in zunehmendem Maße Dienstleister beauftragt und personenbezogene Daten, darunter auch Gesundheitsdaten, durch externe Dritte verarbeitet werden (Stichwort: Outsourcing). Beispielsweise können externe Dritte mit Schreibarbeiten, Fernwartung oder Archivierung von Daten beauftragt sein. Die Datenweitergabe zu solchen Zwecken an einen externen Dritten stellt keine Datenübermittlung im datenschutzrechtlichen Sinn dar, sondern eine Auftragsdatenverarbeitung, bei der die Daten verarbeitende Stelle datenschutzrechtlich verantwortlich bleibt. Die Voraussetzungen einer wirksamen Auftragsdatenverarbeitung sind in § 11 BDSG niedergelegt. Zunächst muss der Auftragnehmer – und ggf. auch die Unterauftragnehmer – sorgfältig ausgesucht werden. Weiter unterliegt dieser den Weisungen des Auftraggebers. Dieser muss sich selbst vergewissert haben, ob sein Auftragnehmer die erforderlichen datenschutzrechtlichen Sicherheitsmaßnahmen getroffen hat. Zudem ist immer eine Fixierung des Auftragsdatenverarbeitungsverhältnisses durch einen schriftlichen Vertrag notwendig, in dem Folgendes präzise festzulegen ist:

- der Gegenstand und die Dauer des Auftrags,
- der Umfang, die Art und der Zweck der vorgesehenen Erhebung, Verarbeitung oder Nutzung von Daten, die Art der Daten und der Kreis der Betroffenen,
- die nach § 9 BDSG zu treffenden technischen und organisatorischen Maßnahmen,
- die Berichtigung, Löschung und Sperrung von Daten,
- die nach § 11 Abs. 4 BDSG[120] bestehenden Pflichten des Auftragnehmers, insbesondere die von ihm vorzunehmenden Kontrollen,
- die etwaige Berechtigung zur Begründung von Unterauftragsverhältnissen,
- die Kontrollrechte des Auftraggebers und die entsprechenden Duldungs- und Mitwirkungspflichten des Auftragnehmers,
- mitzuteilende Verstöße des Auftragnehmers oder der bei ihm beschäftigten Personen gegen Vorschriften zum Schutz personenbezogener Daten oder gegen die im Auftrag getroffenen Festlegungen,

[120] Gemäß § 11 Abs. 4 BDSG ist der Auftragnehmer zur Gewährleistung der Datensicherungsmaßnahmen nach § 9 BDSG sowie – bei Vorliegen der gesetzlichen Voraussetzungen – zur Bestellung eines Datenschutzbeauftragten verpflichtet. Das Datengeheimnis (§ 5 BDSG) gilt auch für seine Mitarbeiter. Unbefugte Verarbeitungen stellen auch für ihn ggf. strafbare Handlungen nach § 44 BDSG dar. Ferner unterliegt auch er der Datenschutzaufsicht.

- der Umfang der Weisungsbefugnisse, die sich der Auftraggeber gegenüber dem Auftragnehmer vorbehält,
- die Rückgabe überlassener Datenträger und die Löschung beim Auftragnehmer gespeicherter Daten nach Beendigung des Auftrags.

Nach § 11 Abs. 2 Satz 4 und 5 BDSG muss sich der Auftraggeber regelmäßig von der Einhaltung der beim Auftragnehmer getroffenen technischen und organisatorischen Maßnahmen überzeugen, was zu dokumentieren ist.

Werden vertragliche Aufgaben von einer rechtlichen Einheit auf eine andere übertragen und ist insoweit auch die Verarbeitung personenbezogener Daten betroffen, so stellt sich stets die Frage, ob eine Auftragsdatenverarbeitung oder eine sog. Funktionsübertragung vorliegt. Dabei ist von einer Auftragsdatenverarbeitung auszugehen, wenn die Verarbeitung personenbezogener Daten das wesentliche Element der Aufgabenübertragung darstellt oder der Auftragnehmer lediglich eine Hilfs- und Unterstützungsfunktion innehat. In Abgrenzung hierzu liegt eine Funktionsübertragung vor, wenn auch die der Datenverarbeitung zugrundeliegenden Aufgaben ganz oder teilweise übertragen werden. Ist dies der Fall, so wird die Stelle, an die die Aufgaben übertragen worden sind, zum Verantwortlichen im Sinne des BDSG.[121]

Verantwortlichkeiten bei automatisierten Abrufverfahren

Automatisierte Abrufverfahren ermöglichen für Dritte einen Online-Zugriff auf personenbezogene Daten. Dabei erfolgt eine automatisierte Datenübermittlung an einen Dritten, der durch Abruf den Übermittlungsvorgang selbst auslösen kann.[122] Nach § 10 BDSG ist die Einrichtung eines solchen automatisierten Verfahrens, das die Übermittlung personenbezogener Daten durch Abruf ermöglicht, zulässig, soweit dieses Verfahren unter Berücksichtigung der schutzwürdigen Interessen der Betroffenen und der Aufgaben oder Geschäftszwecke der beteiligten Stellen angemessen ist. Die Vorschriften über die Zulässigkeit des einzelnen Abrufs bleiben unberührt – die Verantwortung für die Zulässigkeit des einzelnen Abrufs trägt der Dritte, an den übermittelt wird, § 10 Abs. 4 BDSG. Die beteiligten Stellen haben zu gewährleisten, dass die Zulässigkeit des Abrufverfahrens kontrolliert werden kann. Hierzu haben sie den Anlass und Zweck des Abrufverfahrens, die Dritten, an die übermittelt wird, die Art der zu übermittelnden Daten und die nach § 9 BDSG erforderlichen technischen und organisatorischen Maßnahmen schriftlich festzulegen.

Im medizinischen Bereich sind automatisierte Abrufverfahren rechtlich unzulässig.

---

[121] Zur Abgrenzung von Auftragsdatenverarbeitung und Funktionsübertragung vgl. z.B. Walz, in: Simitis (Hrsg.), BDSG, 6. Auflage, 2006, § 11 Rn. 17 ff.

[122] Klebe, in: Däubler / Klebe / Wedde / Weichert (Hrsg.), BDSG, 3. Auflage, 2010, § 10 Rn. 1 f.

Verantwortlichkeiten bei Verbunddateien und vernetzten Systemen

Sind bei einer Datei mehrere Stellen speicherberechtigt (sog. Verbunddatei oder vernetzte Systeme), so bleibt jede speichernde Stelle selbst datenschutzrechtlich im Sinne des § 3 Abs. 7 BDSG verantwortlich für die von dieser Stelle eingegebenen Daten.[123] Bei Verbunddateien kann der Betroffenen sich an jede der an der Verbunddatei beteiligten Stellen wenden und seine Datenschutzrechte geltend machen. Diese ist verpflichtet, das Vorbringen des Betroffenen an die Stelle, die die Daten gespeichert hat, weiterzuleiten. Damit wird sichergestellt, dass Betroffene auch bei Verbunddateien und bei vernetzten Systemen ihre Rechte wirksam geltend machen können, ohne komplizierte Nachforschungen anstellen zu müssen, da bei derartigen Datenspeicherungen für sie nicht ohne Weiteres erkennbar ist, wer hinsichtlich der sie betreffenden Daten verantwortliche Stelle ist.[124]

Diese Verantwortlichkeiten müssen den Betroffenen mitgeteilt werden, damit diese dort ihre Rechte geltend machen können. In diesem Zusammenhang sollten die Beteiligten prüfen, ob und inwieweit die Einhaltung dieser Vorschriften mit Hilfe eines automatisierten Datenschutzmanagements sichergestellt werden kann.

Herausforderungen

Die Zunahme der elektronischen Kommunikation und Einbeziehung von einer größeren Zahl an Dienstleistern, wie es im AAL-Bereich typisch ist, stellen erhebliche Herausforderungen an den Grundsatz der klaren Verantwortlichkeit dar.

Offene Fragen

Eine offene Frage besteht darin, welche Instrumente geeignet sind, um bei der Vielzahl der beteiligten Dienstleister in AAL-Anwendungen die effektive Durchsetzung der Betroffenenrechte zu gewährleisten. Möglicherweise könnte dafür eine Erweiterung der bisherigen Informations-, Transparenz- und Auskunftspflichten hilfreich sein.

Zu untersuchen wäre auch, wie es im Zusammenhang mit einer Auftragsdatenverarbeitung dem Auftraggeber erleichtert werden kann, seiner Verantwortung gerecht zu werden.

Daneben könnte z.B. eine Anzeigepflicht an die datenschutzrechtlichen Aufsichtsbehörden sowie eine Stärkung der Stellung des betrieblichen Datenschutzbeauftragten oder die Einsetzung eines einheitlichen Ansprechpartners für die Betroffenen erwogen werden.

---

[123] Mallmann, in: Simitis (Hrsg.), BDSG, 6. Auflage, 2006, § 6 Rn. 28.

[124] Gola / Schomerus, Bundesdatenschutzgesetz, 10. Auflage, 2010, § 6 Rn. 6.

3.3.8 Grundsatz der Kontrolle

Grundsatz

Die Einhaltung der aufgeführten Datenschutzgrundsätze ist durch eine geeignete unabhängige Kontrolle der verantwortlichen Stellen und Dienstleister sicherzustellen. Dies bedeutet, dass die verantwortlichen Stellen und Dienstleister in der Regel einen betrieblichen Datenschutzbeauftragten ernennen müssen.[125] Anbieter und Beteiligte von AAL-Anwendungen müssen sich ebenfalls darüber bewusst sein, dass sie einer Kontrolle durch die jeweils zuständigen Datenschutzbehörden unterliegen. Diese haben neben den Prüfungsrechten auch einen Beratungsauftrag: Daten verarbeitende Stellen können sich an die Aufsichtsbehörden wenden und Beratungen in Anspruch nehmen, vgl. § 38 Abs. 1 Satz 2 BDSG.

Weiter ist eine effektive Möglichkeit des Nutzers zur Eigenkontrolle wesentlich.

Herausforderungen

Je komplexer das AAL-System ist, desto größer ist die Herausforderung, die Möglichkeit einer effektiven Eigenkontrolle für den Nutzer bereitzustellen. Doch auch für die beteiligten Daten verarbeitenden Stellen ist die Beherrschbarkeit ihrer Systeme, wie es für eine Kontrolle notwendig ist, nicht trivial. Nicht immer unterstützen die Systeme in ausreichendem Umfang, dass aussagekräftige interne Kontrollen, z.B. durch den betrieblichen Datenschutzbeauftragten, oder externe Kontrollen, z.B. durch die zuständige Datenschutzaufsichtsbehörde, vorgenommen werden können.

Offene Fragen

Offen ist, wie zum einen geeignete Mittel der Eigenkontrolle für den Nutzer, zum anderen ausreichende Kontrollmöglichkeiten für interne oder externe Kontrollinstanzen gestaltet werden können. In diesem Zusammenhang ist zu klären, ob eine verstärkte Dokumentationspflicht erforderlich ist und inwieweit aussagekräftige „Prüfpunkte“, die sich zu Kontrollzwecken heranziehen ließen, festgelegt, implementiert und möglichst standardisiert werden könnten.

3.3.9 Grundsatz der Gewährleistung der Betroffenenrechte

Grundsatz

Die Rechte der Betroffenen bilden als Verfahrensrechte einen elementaren Bestandteil des Datenschutzrechts. Von grundlegender Bedeutung ist das Recht des Betroffenen auf Aus-

[125] § 4 f. BDSG.

kunft über seine Daten, mit dessen Hilfe es ihm möglich ist, zu überprüfen, ob die verantwortliche Stelle rechtmäßig Daten über ihn verarbeitet. In Kenntnis der zu seiner Person verarbeiteten Daten kann der Betroffene von den weiteren ihm eingeräumten, unabdingbaren Kontroll-, Abwehr- und Gestaltungsrechten wie Berichtigung, Sperrung, Löschung und Widerspruch Gebrauch machen.[126] Sowohl das BDSG als auch die verschiedenen Landesdatenschutzgesetze enthalten jeweils einen eigenen Abschnitt, in dem die Rechte der Betroffenen gesetzlich normiert sind.

Das Auskunftsrecht ist in § 34 BDSG niedergelegt. Danach kann der Betroffene Auskunft verlangen über

- die zu seiner Person gespeicherten Daten, auch soweit sie sich auf die Herkunft dieser Daten beziehen,
- den Empfänger oder die Kategorien von Empfängern, an die Daten weitergegeben werden, und
- den Zweck der Speicherung.

Soweit in AAL-Systemen eine automatisierte Erfassung erfolgt, spielt der Berichtigungsanspruch wohl eine geringere Rolle; relevant sind aber in jedem Fall die Rechte auf Widerspruch, Löschung oder Sperrung nach § 35 BDSG.

Ergänzend zu den § 823 ff. BGB besteht ein Schadenersatzanspruch nach § 7 BDSG, wenn eine verantwortliche Stelle dem Betroffenen durch eine datenschutzrechtlich unzulässige oder unrichtige Erhebung, Verarbeitung oder Nutzung seiner personenbezogenen Daten einen Schaden zufügt.

Bei Verbunddateien und vernetzen Systemen (s.o.) kann der Betroffenen sich gem. § 6 Abs. 2 BDSG an jede an der Verbunddatei beteiligte Stelle wenden und seine Datenschutzrechte wie oben bereits geschildert geltend machen. Auch wenn § 6 Abs. 2 BDSG den Fall nicht ausdrücklich regelt, ist eine entsprechende Weiterleitungs- und Hinweispflicht unter dem Gesichtspunkt von Treu und Glauben auch im Falle der Auftragsdatenverarbeitung zu bejahen, wenn der Betroffene nicht erkennen kann, dass die von ihm vermutete speichernde Stelle nur Auftragnehmer ist.[127]

Herausforderungen

Da das Auskunftsrecht ein wesentlicher Schlüssel zur Wahrnehmung des Rechts auf informationelle Selbstbestimmung ist, ist es dringend geboten, die Auskunftserteilung effektiv zu

[126] Mallmann, in: Simitis (Hrsg.), BDSG, 6. Auflage, 2006, § 19 Rn. 1.

[127] Gola / Schomerus, Bundesdatenschutzgesetz, 10. Auflage, 2010, § 6 Rn. 6.

gewährleisten[128] – auch dann, wenn die Datenverarbeitung stellenübergreifend und komplex ist. Die Komplexität und verteilte Datenverarbeitung stellt sich oftmals als Erschwernis bei der Auskunftserteilung dar. Durch die zunehmende Automation bisher konventionell abgewickelter Geschäftsprozesse und den Versuch, kostenträchtige Medienbrüche zu vermeiden, wächst die Zahl der Verarbeitungsprozesse von personenbezogenen Daten, in die mehr als eine verarbeitende Stelle eingebunden ist.

Als Beispiel sei die medizinische Datenverarbeitung angeführt. Hier kommen oftmals mehrere Verarbeitungszwecke zusammen, so z.B. eine Verarbeitung zu Diagnose-, Behandlungs-, Dokumentations-, Abrechnungs- und Forschungszwecken. Auch sind oft zugleich viele verantwortliche Stellen mit verteilten Rollen beteiligt, z.B. die Daten erhebenden Ärzte, eine Gruppe weiterer behandelnder und konsultierter Ärzte und Krankenhäuser, Daten aufbereitende Kompetenzzentren und die Krankenkassen. Die Arbeitsteilung kann sich wiederum auf jede Art von Datenverarbeitungsschritten beziehen: Erhebung, Übermittlung, Speicherung, Administration, Pseudonymisierung, Auswertung, Nutzung, Rückmeldung.

Bei derartigen Datenflüssen läuft der Betroffene Gefahr, seinen Auskunftsanspruch nicht mehr ausreichend durchsetzen zu können. Er überblickt nicht mehr, welche Stellen über ihn welche Daten verarbeiten. Um einen umfassenden Überblick zu erhalten, müsste er bei sämtlichen Stellen seinen Auskunftsanspruch geltend machen.

Offene Fragen

Zu klären ist, ob eine Erweiterung der Betroffenenrechte sinnvoll ist, z.B. durch weitergehende, konkretisierte Ansprüche auf Information für die Nutzer oder die von ihnen beauftragten Vertrauten, und ob als Grundlage für die Ausübung von Betroffenenrechten eine erweiterte Dokumentationspflicht geboten ist.

Weiterhin ist zu untersuchen, ob AAL-Systeme Schnittstellen zur Verfügung stellen sollten, über die die Betroffenen die Wahrnehmung ihrer Rechte ohne Medienbruch ausüben könnten, z.B. im Rahmen einer Online-Auskunft. Die Rechtewahrnehmung könnte auch über ein Portal vermittelt werden, so dass der Betroffene mit einem Auskunftsersuchen technisch gestützt alle in Frage kommenden Daten verarbeitenden Stellen adressieren könnte. Wichtig ist eine datenschutzgerechte Ausgestaltung solcher technischen Systeme, damit keine zusätzlichen Risiken für den Betroffenen entstehen. Beispielsweise müsste verhindert werden, dass eine unberechtigte Person Zugriff auf die Daten erlangt.

[128] Weichert, in: DuD 2006, S. 694.

3.3.10 Verbot der Profilbildung

Grundsatz

Die Zusammenführung und Verknüpfung personenbezogener Daten zu Profilen stellt eine besondere Gefahr für das Persönlichkeitsrecht dar. Durch Profile können die Verhaltensweisen, Interessen und Gewohnheiten vorhersehbar gemacht werden mit der Gefahr der Manipulation und der Diskriminierung. Derartige Profile gibt es bereits in vielen Bereichen, etwa als Konsumentenprofil, Bewegungsprofil, Nutzerprofil im Internet etc. Der rasante technische Fortschritt in vielen Bereichen lässt große Mengen an personenbezogenen Daten anfallen, oft nur als Nebenprodukt, deren Verknüpfung immer ausgefeiltere und detailliertere Profile möglich macht.

Für das Bundesverfassungsgericht liegt eine Grenze der Datenverarbeitung im Verbot der Erstellung totaler Persönlichkeitsbilder. Das Gericht hat zur Profilbildung durch staatliche Stellen ausgeführt, dass es nicht mit der Menschenwürde vereinbar sei, „wenn der Staat das Recht für sich in Anspruch nehmen könnte, den Menschen zwangsweise in seiner ganzen Persönlichkeit zu registrieren und zu katalogisieren“.[129] Insbesondere bei der Integration automatisierter Informationssysteme entsteht die Gefahr, dass personenbezogene Daten „mit anderen Datensammlungen zu einem teilweisen oder weitgehend vollständigen Persönlichkeitsprofil zusammengefügt werden, ohne dass der Betroffene dessen Richtigkeit und Verwendung zureichend kontrollieren kann“.[130]

Auch im privaten Bereich gilt das Verbot der zwangsweisen und heimlichen Erstellung von Persönlichkeitsbildern.[131] Nicht erst das Erstellen von Profilen, sondern auch die systematische Datensammlung zu einem Menschen, z.B. durch systematische Observation, ist untersagt.[132]

Die vom Bundesverfassungsgericht zur Gewährleistung des Grundrechts auf informationelle Selbstbestimmung gezogene absolute Grenze der Datenverarbeitung in Fällen staatlicher Eingriffe schränkt auch eine freiwillige Profilbildung durch Private ein. Aufgrund der dargestellten Risiken kann trotz einer Einwilligung in die Profilbildung durch Private eine Verletzung der Menschenwürde vorliegen, die eine Schutzpflicht des Staates gegenüber dem Betroffenen bewirkt, beispielsweise wenn ein umfangreicher Bestand an Daten eine Profilbildung ermöglicht, die ein selbstbestimmtes Leben des Betroffenen stark einschränkt. Dies kommt beispielsweise bei der Überwachung des Aufenthaltsortes von Kindern und Demenzkranken durch Dritte oder der Aufzeichnung von Bewegungsmustern und Verhaltensweisen

[129] BVerfG NJW 1969, 1707.

[130] BVerfGE 27, 6.

[131] BGH NJW 1988, 3078.

[132] Vgl. BVerwG NJW 1986, 2332.

in Betracht. Die Kommunikations- und Handlungsfreiheit innerhalb der Gesellschaft ist als Grundbedingung eines freiheitlich demokratischen Gemeinwesens grundrechtlich geschützt.

Herausforderungen

AAL-Anwendungen sind von ihrem Konzept und ihrer Technik her geeignet, umfassende Profile zu erstellen. Dies gilt beispielsweise dann, wenn es sich um Systeme handelt, bei denen sowohl Verhaltensdaten als auch Vitaldaten und Umgebungsdaten des Betroffenen erhoben werden. Wesentlich ist es daher auch vor dem Hintergrund des o.g. Urteils, den Umfang der Profilbildung auf bestimmte Bereiche zu beschränken, Verknüpfungen auszuschließen, Löschroutinen und Transparenzanforderungen einzuhalten – mithin zu gewährleisten, dass keine umfassenden und intransparenten Persönlichkeitsprofile entstehen.

Da als Rechtsgrundlage im Wesentlichen ausschließlich eine Einwilligung in Betracht kommt, muss der Betroffene umfassende Informationen erhalten über Umfang und Herkunft der für das Profil verwendeten Daten, über den Zweck und die Verwendung des konkreten Profils sowie über die Gefährdungen von Profilbildungen. Die Freiwilligkeit und Widerruflichkeit der Einwilligung einschließlich sofortiger Löschung des Profils auch bei etwaigen Empfängern des Profils muss gewährleistet sein.

Nur durch eine strikte Reglementierung der Profilbildung kann in diesem besonders sensiblen Bereich die informationelle Selbstbestimmung gewährleistet werden.[133]

Offene Fragen

Es ist die offene Frage zu untersuchen, wie Regelungen, die der Bildung von Persönlichkeitsprofilen in AAL-Systemen möglichst enge Grenzen setzen, ausgestaltet und durchgesetzt werden können und sollten.

3.3.11 Verbot der Sammlung auf Vorrat

Unzulässig ist die Sammlung von personenbezogenen Daten „auf Vorrat zu unbestimmten oder noch nicht bestimmbaren Zwecken“.[134] Alle Stellen müssen sich auf das Minimum an Daten beschränken, das zur Erfüllung der jeweiligen Aufgabe notwendig ist (siehe auch Abschnitt 3.3.4 zum Grundsatz der Erforderlichkeit und Abschnitt 3.3.5 zum Grundsatz der Datenvermeidung und Datensparsamkeit). Mit dem Verbot der Sammlung auf Vorrat soll verhindert werden, dass Daten „einfach drauflos“, „ins Blaue hinein“ oder „für alle Fälle“ gespeichert werden, ohne dass ein aktueller oder zukünftiger Bedarfsfall klar umschrieben wäre.

[133] Konferenz der Datenschutzbeauftragten des Bundes und der Länder, Ein modernes Datenschutzrecht für das 21. Jahrhundert, Eckpunkte, vorgelegt am 18.03.2010., S. 12.

[134] BVerfGE 65, 46 = NJW 1984, 422.

Das Verbot der Vorratsdatenverarbeitung ist eine Konkretisierung des Übermaßverbots bzw. des Erforderlichkeitsgrundsatzes.

3.3.12 Verbot der automatisierten Einzelentscheidung

§ 6a Abs. 1 BDSG verbietet im Grundsatz automatisierte Einzelentscheidungen, die sich ausschließlich auf die automatisierte Verarbeitung personenbezogener Daten zur Bewertung einzelner Persönlichkeitsmerkmale stützen.[135] Diese Vorschrift soll verhindern, dass Menschen für sie nachteiligen, intransparenten Entscheidungssystemen unterworfen werden, ohne dass sie hierbei ihre Belange hinreichend einbringen können.[136] Dabei kann das generelle Verbot in bestimmten Fällen wieder aufgehoben werden, insbesondere dann, wenn die Wahrung der berechtigten Interessen des Betroffenen durch geeignete Maßnahmen gewährleistet ist.[137] Sind AAL-Anwendungen auf das automatisierte Auslösen von Prozessen gerichtet, die zu einer automatisierten Entscheidung unter Bewertung von einzelnen Persönlichkeitsmerkmalen führen, so ist § 6a BDSG anwendbar.

3.4 Besonderes Datenschutzrecht

Neben den allgemeinen Anforderungen aus den verfassungsrechtlichen Grundlagen und dem Bundesdatenschutzgesetz sind für AAL-Systeme, -Anwendungen und -Dienstleistungen die datenschutzrechtlichen spezialgesetzlichen Regelungen in verschiedenen Bereichen relevant. Die wichtigsten Normen und die sich daraus ergebenen Anforderungen werden in diesem Abschnitt erläutert. Dies betrifft die Bereiche Multimediadatenschutz (siehe Abschnitt 3.4.1), Medizindatenschutz (siehe Abschnitt 3.4.2), Sozialdatenschutz (siehe Abschnitt 3.4.3) sowie Datenschutz bei weiteren natürlichen Personen neben dem Betroffenen (siehe Abschnitt 3.4.4).

3.4.1 Multimediadatenschutz

Da AAL-Anwendungen auf der Nutzung von Telekommunikation und Telemedien beruhen, ist das Multimediadatenschutzrecht einschlägig. Dies wird in Abschnitt 3.4.1.1 verdeutlicht. Während Abschnitt 3.4.1.2 erläutert die relevanten Regelungen im Telekommunikationsgesetz, konzentriert sich Abschnitt 3.4.1.3 auf die telemedienrechtlichen Anforderungen. Anschließend werden Spezialfälle wie die Einbindung von Diensten, die Standortdaten auswerten (siehe Abschnitt 3.4.1.4) oder soziale Netzwerke integrieren (siehe Abschnitt 3.4.1.5) behandelt.

---

[135] Mit dieser Regelung wurde Art. 15 der Datenschutzrichtlinie 95/46/EG umgesetzt.

[136] Weichert, in: Däubler / Klebe / Wedde / Weichert (Hrsg.), BDSG, 3. Auflage, 2010, § 6a Rn. 1.

[137] § 6a Abs. 2 Nr. BDSG.

3.4.1.1 Relevanz für AAL-Anwendungen

Soll eine Dienstleistung aus der Entfernung und über elektronische Übertragungswege wie das Internet angeboten werden, so ist die Einschaltung von Tele- oder Mediendiensten[138] sowie von Telekommunikationsdiensten erforderlich. Dabei sind Telekommunikationsdienste „in der Regel gegen Entgelt erbrachte Dienste, die ganz oder überwiegend in der Übertragung von Signalen über Telekommunikationsnetze bestehen".[139] Während Telekommunikationsdienste damit auf einer unteren Schicht der Kommunikation für die Übertragung der Daten sorgen, satteln Tele- und Mediendienste gleichsam auf dieser Schicht auf und bieten basierend auf den Telekommunikationsdiensten Informationsinhalte bzw. besondere elektronische Zusatzfunktionen an.

AAL-Anwendungen werden typischerweise „aus der Entfernung" mit Hilfe von Web-Services implementiert. In diesem Kontext geben das Telekommunikationsgesetz (TKG) und das Telemediengesetz (TMG) spezialgesetzliche Regelungen vor. Welches dieser Gesetze jeweils Anwendung findet, beurteilt sich nach dem Drei-Schichten-Modell.[140] Hierbei wird zwischen einer Kommunikationsebene, einer Interaktionsebene und einer Inhaltsebene unterschieden:

- Die Kommunikationsebene stellt die Kommunikationsinfrastruktur dar, die erforderlich ist, damit zwei Parteien Informationen über das Internet oder ein elektronisches Medium versenden können. Sie betrifft den reinen Datentransport. Zur Kommunikationsebene gehören Dienste wie ISDN, DSL, E-Mail und Telefon. Besondere gesetzliche Regelung hat der Datenschutz auf dieser Ebene durch das TKG erfahren.
- In Abgrenzung hierzu geht es auf der Interaktionsebene um eine technisch-standardisierte Kommunikation zwischen Nutzer und Diensteanbieter, wie sie etwa beim Abrufen eines Webseitenangebots stattfindet.[141] Die Interaktionsebene stellt damit eine geeigne-

[138] Im Telemediengesetz auch kurz „Telemedien" genannt. In dieser Vorstudie wird synonym der Begriff „Telemediendienst(e)" verwendet.

[139] § 3 Nr. 24 TKG.

[140] Unabhängiges Landeszentrum für Datenschutz / Institut für Informatik der Universität Koblenz-Landau / Institut für Wirtschafts- und Verwaltungsinformatik der Universität Koblenz-Landau, SOAinVO – Chancen und Risiken von Service-orientierten Architekturen in Virtuellen Organisationen, 2007, S. 15.

[141] Unabhängiges Landeszentrum für Datenschutz / Institut für Informatik der Universität Koblenz-Landau / Institut für Wirtschafts- und Verwaltungsinformatik der Universität Koblenz-Landau, SOAinVO – Chancen und Risiken von Service-orientierten Architekturen in Virtuellen Organisationen, 2007, S. 16.

te interaktive Oberfläche bereit.[142] In solchen Fällen ist auf die Datenverarbeitung das TMG anwendbar.[143]

- In der obersten Schicht, der Inhaltsebene, treten zwei Akteure miteinander in Beziehung, zwischen denen sich Kommunikationsvorgänge mit individuellem Inhalt abspielen. Als Beispiel für eine solche individuelle Kommunikation ist die Datenverarbeitung zu nennen, die sich aus dem Ausfüllen eines Web-Formulars eines Dienstleistungsanbieters ergibt. In diesem Bereich sind die bereichsspezifischen Regelungen von TKG und TMG nicht anwendbar, sondern die für die jeweilige Daten verarbeitende Stelle geltenden Vorschriften. Im Fall einer nicht-öffentlichen Stelle sind daher die Vorschriften des BDSG anwendbar.

AAL-Anwendungen bedienen sich der Telekommunikation, um ihren Service auszuführen. Die einzelnen Beteiligten sind durch Telekommunikationsanlagen (§ 3 Nr. 23 TKG) in Form von Kabel- oder Funkverbindungen vernetzt, mittels derer Signale ausgesendet, übermittelt und empfangen werden. Im Ergebnis fallen die Bereitstellung einer AAL-Anwendung in Form eines Telemediendienstes unter die datenschutzrechtlichen Bestimmungen des TMG, die Übertragungen der personenbezogenen Daten durch Telekommunikationsanbieter (Nachrichten, z.B. per E-Mail) unter die Regelungen des TKG und die anderen Verwendungen bzw. Nutzungen personenbezogener Daten in der Regel unter die Bestimmungen des BDSG.[144] Im Folgenden werden aufgrund der o.g. Relevanz die wesentlichen datenschutzrechtlichen Vorschriften des TKG und des TMG kurz dargestellt.

3.4.1.2 Telekommunikationsgesetz

Die §§ 91 ff. TKG enthalten besondere datenschutzrechtliche Vorschriften für Teilnehmer und Nutzer von Telekommunikationsdiensten bei der Erhebung, Verarbeitung und Nutzung von Daten durch Unternehmen und Personen, die geschäftsmäßig Telekommunikationsdienste erbringen oder an deren Erbringung mitwirken. Ein besonderer Schutz personenbezogener Daten ist erforderlich, da durch die zunehmende Digitalisierung der Telekommunikationsnetze sich besondere Gefahren für die Vertraulichkeit der Kommunikation sowie für den

---

142 Schleipfer, Das 3-Schichten-Modell des Multimediadatenschutzrechts, in: DuD 2004, S. 272, 729.

143 Telemedien sind gemäß § 1 Abs. 1 TMG alle elektronischen Informations- und Kommunikationsdienste, die nicht die Tatbestandsmerkmale eines Telekommunikationsdienstes nach § 3 Nr. 24 TKG oder des Rundfunks nach § 2 Rundfunkstaatsvertrag erfüllen. Der Begriff der Telemedien ist zwar weder im TMG noch im TKG legal definiert. Aus § 1 Abs. 1 TMG ergibt sich jedoch, dass davon alle elektronischen Informations- und Kommunikationsdienste erfasst werden sollen, „soweit sie nicht Telekommunikationsdienste nach § 3 Nr. 24 Telekommunikationsgesetz, die ganz in der Übertragung von Signalen über Telekommunikationsnetze bestehen, telekommunikationsgestützte Dienste nach § 3 Nr. 25 des Telekommunikationsgesetzes oder Rundfunk sind“. Im Teledienstegesetz (TDG) als Vorgänger des TMG waren von § 2 Abs. 1 TDG nur „Teledienste“ erfasst, „denen eine Übermittlung mittels Telekommunikation zugrunde liegt“.

144 Schleipfer, in: DuD 2004, S. 727 (732); Rost, Welches Gesetz gilt eigentlich?, 2005, https://www.datenschutzzentrum.de/systemdatenschutz/meldung/sm91.htm/.

Schutz der Privatsphäre vor allem dadurch ergeben, dass eine automatische Speicherung und Verarbeitung personenbezogener Daten über Teilnehmer und Nutzer möglich ist. Durch Auswertung dieser Daten können Nutzerprofile erstellt und Gewohnheiten abgeleitet werden.

Telekommunikationsdiensteanbieter haben ihre Teilnehmer bei Vertragsabschluss über Art, Umfang, Ort und Zweck der Erhebung und Verwendung personenbezogener Daten so zu unterrichten, dass die Teilnehmer in allgemein verständlicher Form Kenntnis von den grundlegenden Verarbeitungstatbeständen der Daten erhalten, § 93 Abs. 1 Satz 1 TKG. Dabei sind die Teilnehmer auch auf die zulässigen Wahl- und Gestaltungsmöglichkeiten hinzuweisen.

Der Telekommunikationsdiensteanbieter darf Bestandsdaten erheben und verwenden, soweit dieses für die Begründung, inhaltliche Ausgestaltung, Änderung oder Beendigung eines Vertragsverhältnisses über Telekommunikationsdienste erforderlich ist, § 95 Abs. 1 TKG. Er darf diese mit Einwilligung der Teilnehmer zur Beratung der Teilnehmer, zur Versendung von Informationen nach § 98 Abs. 1 Satz 3 TKG, zur Werbung für eigene Angebote, zur Marktforschung und zur Unterrichtung über einen individuellen Gesprächswunsch eines anderen Nutzers verwenden, soweit dies für diese Zwecke erforderlich ist und der Teilnehmer eingewilligt hat, § 95 Abs. 2 TKG. Endet das Vertragsverhältnis, sind die Bestandsdaten vom Diensteanbieter mit Ablauf des auf die Beendigung folgenden Kalenderjahres zu löschen, § 95 Abs. 3 TKG.

Die Erbringung von Telekommunikationsdiensten darf nicht von einer Einwilligung des Teilnehmers in eine Verwendung seiner Daten für andere Zwecke abhängig gemacht werden, wenn dem Teilnehmer ein anderer Zugang zu diesen Telekommunikationsdiensten ohne die Einwilligung nicht oder nur in nicht zumutbarer Weise möglich ist. Eine unter solchen Umständen erteilte Einwilligung ist unwirksam, § 95 Abs. 5 TKG.

Stellt der Diensteanbieter fest, dass bei ihm gespeicherte Bestandsdaten oder Verkehrsdaten unrechtmäßig übermittelt worden oder auf sonstige Weise Dritten unrechtmäßig zur Kenntnis gelangt sind, und drohen schwerwiegende Beeinträchtigungen für die Rechte oder schutzwürdigen Interessen des betroffenen Nutzers, gilt § 42a des Bundesdatenschutzgesetzes entsprechend, § 93 Abs. 3 TKG, d.h., es besteht eine Informationspflicht bei unrechtmäßiger Kenntniserlangung von Daten (sog. Breach Notification).

Der Diensteanbieter darf nur die gesetzlich festgelegten Verkehrsdaten erheben, soweit dies für die genannten Zwecke erforderlich ist, § 96 Abs. 1 TKG. Diese sind nach Beendigung der Verbindung zu löschen.[145]

Bei der Einholung der Einwilligung ist dem Teilnehmer mitzuteilen, welche Datenarten für die gesetzlich festgelegten Zwecke verarbeitet und wie lange sie gespeichert werden sollen. Außerdem ist der Teilnehmer darauf hinzuweisen, dass er die Einwilligung jederzeit widerrufen kann, § 96 Abs. 4 TKG.

Telekommunikationsdiensteanbieter dürfen die in § 96 Abs. 1 TKG aufgeführten Verkehrsdaten sowie die weiteren abschließend aufgeführten Daten verwenden, soweit die Daten zur Ermittlung des Entgelts und zur Abrechnung mit ihren Teilnehmern benötigt werden. Diese Daten dürfen bis zu sechs Monate nach Versendung der Rechnung gespeichert werden.

Standortdaten, die in Bezug auf die Nutzer von öffentlichen Telekommunikationsnetzen oder Telekommunikationsdiensten für die Öffentlichkeit verwendet werden, dürfen nur zur Bereitstellung von Diensten mit Zusatznutzen in erforderlichem Maß und innerhalb des dafür erforderlichen Zeitraums verarbeitet werden, wenn sie anonymisiert wurden oder wenn der Teilnehmer seine Einwilligung erteilt hat. Werden die Standortdaten für einen Dienst mit Zusatznutzen verarbeitet, der die Übermittlung von Standortdaten eines Mobilfunkendgeräts an einen anderen Teilnehmer oder Dritte, die nicht Anbieter des Dienstes mit Zusatznutzen sind, zum Gegenstand hat, muss der Teilnehmer abweichend von § 94 TKG seine Einwilligung ausdrücklich, gesondert und schriftlich erteilen, § 98 Abs. 1 TKG.

3.4.1.3 Telemediengesetz

Datenschutzrechtlich relevant für entsprechende AAL-Anwendungen sind die §§ 11 ff. TMG. Insbesondere hat der Anbieter Folgendes zu beachten:

Der Telemedien-Diensteanbieter darf personenbezogene Daten eines Nutzers nur erheben und verwenden, soweit sie für die Begründung, inhaltliche Ausgestaltung oder Änderung eines Vertragsverhältnisses zwischen dem Telemedien-Diensteanbieter und dem Nutzer über die Nutzung von Telemedien erforderlich sind (Bestandsdaten), § 14 Abs. 1 TMG.

Der Telemedien-Diensteanbieter darf personenbezogene Daten eines Nutzers nur erheben und verwenden, soweit dies erforderlich ist, um die Inanspruchnahme von Telemedien zu

[145] Mit dem Urteil des Bundesverfassungsgerichts (BVerfG) vom 02.03.2010 (1 BvR 256/08) ist die Vorratsdatenspeicherung in Deutschland vorerst gestoppt. Das Gericht sprach aus, dass eine sechsmonatige Vorratsdatenspeicherung an sich nicht zwingend verfassungswidrig sei, die Art der Umsetzung mit den zu weit reichenden Zugriffsbefugnissen hingegen schon. Das Gericht stellte fest, dass es sich um einen „besonders schweren Eingriff mit einer Streubreite, wie sie die Rechtsordnung bisher nicht kennt“, handelt. Um eine verfassungsmäßige Umsetzung zu schaffen, müsse es daher „hinreichend anspruchsvolle und normenklare Regelungen hinsichtlich der Datensicherheit, der Datenverwendung, der Transparenz und des Rechtsschutzes“ geben. Zudem dürfe die Speicherung nicht direkt beim Staat erfolgen. Für die unmittelbare Nutzung fordert das Gericht z.B. einen Richtervorbehalt.

ermöglichen und abzurechnen (Nutzungsdaten), § 15 Abs. 1 TMG. Diese Nutzungsdaten darf er über das Ende des Nutzungsvorgangs hinaus verwenden, soweit sie für Zwecke der Abrechnung mit dem Nutzer erforderlich sind (Abrechnungsdaten).

Der Telemedien-Diensteanbieter darf an andere Diensteanbieter oder Dritte Abrechnungsdaten übermitteln, soweit dies zur Ermittlung des Entgelts und zur Abrechnung mit dem Nutzer erforderlich ist. Zum Zwecke der Marktforschung anderer Diensteanbieter dürfen anonymisierte Nutzungsdaten übermittelt werden.

Die Abrechnung über die Inanspruchnahme von Telemedien darf Anbieter, Zeitpunkt, Dauer, Art, Inhalt und Häufigkeit bestimmter von einem Nutzer in Anspruch genommener Telemedien nicht erkennen lassen, es sei denn, der Nutzer verlangt einen Einzelnachweis.

Der Anbieter hat den in §§ 5 und 6 TMG spezifizierten Informationspflichten nachzukommen: Für den Nutzer muss erkennbar sein, wer für die Verarbeitung seiner personenbezogenen Daten verantwortlich ist. Auch hier gilt, dass die Nutzer ihre Auskunftsrechte bezüglich der über sie gespeicherten Daten und ihre sonstigen datenschutzrechtlichen Ansprüche (Widerspruch, Sperrung etc.) nur dann in Anspruch nehmen bzw. durchsetzen können, wenn sie den entsprechenden Diensteanbieter identifizieren können.

Der Nutzer ist zu Beginn des Nutzungsvorgangs umfassend über die Verarbeitung seiner Bestandsdaten und Nutzungsdaten zu unterrichten. Dazu gehören auch Hinweise auf Widerspruchrechte oder auf das Recht zum Widerruf erteilter Einwilligungen. Der Inhalt der Unterrichtung muss für den Nutzer jederzeit abrufbar sein, § 13 Abs. 1-3 TMG.

Stellt der Diensteanbieter fest, dass bei ihm gespeicherte Bestands- oder Nutzungsdaten unrechtmäßig übermittelt worden oder auf sonstige Weise Dritten unrechtmäßig zur Kenntnis gelangt sind, und drohen schwerwiegende Beeinträchtigungen für die Rechte oder schutzwürdigen Interessen des betroffenen Nutzers, gilt § 42a des Bundesdatenschutzgesetzes entsprechend, § 15a TMG, d.h., es besteht eine Informationspflicht bei unrechtmäßiger Kenntniserlangung von Daten.

Der Diensteanbieter hat die Nutzung von Telemedien und ihre Bezahlung anonym oder unter Pseudonym zu ermöglichen, soweit dies technisch möglich und zumutbar ist. Der Nutzer ist über diese Möglichkeit zu informieren, § 13 Abs. 6 TMG.

Der Diensteanbieter hat dem Nutzer nach Maßgabe von § 34 BDSG auf Verlangen Auskunft über die zu seiner Person oder zu seinem Pseudonym gespeicherten Daten zu erteilen. Die Auskunft kann auf Verlangen des Nutzers auch elektronisch erteilt werden, § 13 Abs. 7 TMG.

3.4.1.4 AAL-Anwendungen und Location Based Services

Neben Internet-basierten Diensten können auch Lokalisierungsdienste auf Mobilfunk- und Satellitennavigationsbasis in der AAL-Praxis eine Rolle spielen. Als Mehrwertdienst ist z.B. angedacht, die Nutzer über nahegelegene Einkaufsmöglichkeiten und Sehenswürdigkeiten zu informieren oder aber einen Fahrdienst anzubieten, bei dem die Standortdaten des Nut-

zers herangezogen werden. Das Angebot personalisierter Location Based Services (LBS) setzt das Wissen des Diensteanbieters über die gewünschten Informationen des Nutzers und die Kenntnis von ortsbezogenen Informationen des Nutzers voraus. Denn nur wenn der Diensteanbieter den aktuellen Aufenthaltsort des Nutzers ausreichend genau kennt, kann er diesem Informationen zu den gewünschten Standorten wie beispielsweise nahegelegenen Einkaufsmöglichkeiten, Restaurants, Sehenswürdigkeiten oder Wegstrecken erteilen. Gleiches gilt, wenn der Standort des Nutzers zur Erbringung von Diensten an Dritte weitergegeben werden soll, beispielsweise um ein Taxi oder einen Rettungswagen an dessen Standort zu lotsen. Um sinnvolle Dienste für den Nutzer erbringen zu können, sind zudem Kenntnisse über individuelle Präferenzen des Nutzers erforderlich. Statt einer undifferenzierten Rückmeldung sämtlicher Restaurants oder Geschäfte könnten sich nutzbringende Antworten auf solche beschränken, die den persönlichen Vorlieben, Qualitätsanforderungen und Preisvorstellungen am ehesten gerecht werden.

Das Angebot eines LBS-Dienstes umfasst, wenn er auf Mobilfunk beruht, im Regelfall die drei bereits oben genannten Beteiligten: den LBS-Anbieter, den Telekommunikationsdiensteanbieter und den Nutzer. Um den oben beschriebenen Risiken vorzubeugen, dürfen die Standortdaten von öffentlichen Telekommunikationsdiensteanbietern nach § 98 Abs. 1 TKG an Anbieter von Location Based Services nur weiter gegeben werden, wenn sie anonymisiert sind oder der Teilnehmer seine Einwilligung erteilt hat. Die Teilnehmer müssen nach § 98 Abs. 2 TKG die Möglichkeit haben, die Verarbeitung von Standortdaten für jede Verbindung zum Netz oder für jede Übertragung einer Nachricht auf einfache Weise und unentgeltlich zeitweise zu untersagen.[146]

Für den Anbieter von Location Based Services gelten die Vorschriften des TMG, d.h., die Daten über den Standort oder die spezifische Situation des Nutzers sind Nutzungsdaten und damit zu löschen, wenn die jeweilige Dienstleistung erbracht ist. Bewegungsprofile sind für das Erbringen der Dienstleistung in der Regel nicht erforderlich. Daten etwa über Interessen und Präferenzen dürfen dagegen über eine einzelne Dienstleistung hinaus so lange gespeichert werden, wie sie zutreffen und der entsprechende Vertrag mit dem Nutzer besteht. Sie sind Bestandsdaten, die verarbeitet werden dürfen, soweit dies für die inhaltliche Ausgestaltung des Vertragsverhältnisses erforderlich ist. Kein Datum darf für andere Zwecke genutzt oder weitergegeben werden. Entsprechend der Sensitivität der Daten ist die Zweckbindung eng und strikt zu verstehen. [147]

Erfolgt die Lokalisierung auf Satellitennavigationsbasis, besteht ein Zweipersonenverhältnis. Datenschutzrechtlich relevant ist hier, ob der Träger eines GPS-Empfängers nur mit seinem Wissen geortet werden kann oder aber die Feststellung des Aufenthaltsortes der Person

[146] Roßnagel, in: NZV 2006, S. 285.

[147] Roßnagel, in: NZV 2006, S. 285.

unter Umständen auch ohne Willen und Kenntnis des Betroffenen möglich ist.[148] Notwendig sind auch hier immer die Einwilligung des Betroffenen sowie entsprechende Informationen über den Zweck der Datenverarbeitung und die Weitergabe der Daten. Dem Nutzer muss die Untersagung der Lokalisierung einfach und jederzeit möglich sein. Eine Herausforderung besteht darin, inwieweit sich die Anforderungen an die Einwilligung des Nutzers bei standortbasierten Mehrwertdiensten erfüllen lassen, da sich das mobile Endgerät nur bedingt dazu eignet, um umfassende Erklärungen und Unterrichtungen zu übermitteln.[149]

Im Ergebnis sind keine spezifischen Fragen für AAL-Anwendungen zu klären, sondern allgemeine datenschutzrechtliche Fragen im Zusammenhang mit standortbasierten Diensten.

3.4.1.5 AAL-Anwendungen und soziale Netzwerke

Einen besonderen Dienst im Online-Bereich stellen die sozialen Netzwerke dar, d.h. Kommunikationsplattformen, die es dem Einzelnen ermöglichen, sich Communities von gleich gesinnten Nutzern anzuschließen oder solche zu schaffen. Zur Ermittlung der hier jeweils einschlägigen Rechtsgrundlagen lässt sich wie bei anderen Online-Diensten ebenfalls das oben dargestellte Drei-Schichten-Modell heranziehen. Soziale Netzwerke zeichnen sich dadurch aus, dass die Nutzer aufgefordert werden, ihr persönliches Profil einzustellen und ihr eigenes Material (z.B. Bilder, Videos oder Tagebucheinträge) zu veröffentlichen, und dass die Nutzung der sozialen Netzwerke über Kontaktlisten und Adressbücher erfolgt.[150] Die meisten verbreiteten sozialen Netzwerke zeichnen sich durch eine zentralisierte Datenverarbeitung bei dem jeweiligen Betreiber aus, der auf umfangreiche Datensammlungen zu bereitgestellten Informationen und Bekanntschaften der einzelnen Nutzer Zugriff hat. Ein Großteil heutiger sozialer Netzwerke wird über Werbung finanziert. Es werden daher in einem besonderen Umfang Profildaten und Kommunikationsdaten der Nutzer verarbeitet und ausgewertet, um die Nutzer möglichst zielgerichtet mit Werbung versorgen zu können.

Einige AAL-Anwendungen sind mit sozialen Netzwerken verknüpft, um den Nutzern auch auf diese Art eine Teilhabe am gesellschaftlichen Leben zu ermöglichen. Dies kann dazu führen, dass die in den sozialen Netzwerken vorhandenen personenbezogenen Daten und z.B. die durch Sensoren erhobenen Daten zusammengeführt werden. So können sensible personenbezogene Daten, wie Gesundheitsdaten, in das soziale Netzwerk integriert und womöglich allgemein zugänglich gemacht werden.

---

[148] Vgl. die Forderungen des Bundesbeauftragten für den Datenschutz und die Informationsfreiheit, abrufbar unter: http://www.bfdi.bund.de/cln_136/DE/Oeffentlichkeitsarbeit/Pressemitteilungen/2009/PM_09_09_CeBIT2009_AchtungOrtung.html.

[149] Hellmich, in: MMR 2002, S. 152, 156.

[150] Vgl. Art. 29-Datenschutzgruppe, Stellungnahme 5/2009 zur Nutzung sozialer Online-Netzwerke, WP 163, S. 5.

Werden soziale Netzwerke in AAL-Anwendungen eingebunden, ist es äußerst wichtig, dass diese die allgemeinen datenschutzrechtlichen Bestimmungen einhalten sowie auf die Besonderheiten ihrer Nutzer und ihre Technikkompetenz eingehen. Zusätzlich zu den bereits beschriebenen allgemeinen datenschutzrechtlichen Anforderungen und Problemen stellen sich für diesen Bereich entsprechend spezifische Fragen, die nachfolgend aufgegriffen werden.

Informations- und Unterrichtungspflicht: Anbieter sozialer Netzwerke müssen ihre Nutzer umfassend gemäß den gesetzlichen Vorschriften über die Verarbeitung ihrer personenbezogenen Daten und ihre Wahl- und Gestaltungsmöglichkeiten unterrichten. Dies umfasst eine Darstellung von Risiken für die Privatsphäre, die mit der Veröffentlichung von Daten in Nutzerprofilen verbunden sind. Darüber hinaus haben die Anbieter ihre Nutzer aufzuklären, wie diese mit personenbezogenen Daten Dritter zu verfahren haben. Hier stellen sich hinsichtlich der Einwilligung dieselben Fragen, wie in Abschnitt 3.3.2.2 erörtert, insbesondere danach, wie das Verständnis der Nutzer für die personenbezogene Verarbeitung und damit die notwendige Informiertheit herzustellen und wie die tatsächliche Freiwilligkeit der Erklärung der Betroffenen zu wahren ist. Von besonderer Bedeutung ist auch hier das Koppelungsverbot, d.h., dass die Teilnahme am sozialen Netzwerk grundsätzlich nicht von der Einwilligung in die Verarbeitung oder Nutzung von Daten abhängig gemacht werden darf.

Standardeinstellungen: Bei der datenschutzgerechten Gestaltung von sozialen Netzwerken kommt den Standardeinstellungen – z.B. für die Verfügbarkeit von Profildaten für Dritte – eine zentrale Bedeutung zu. Anbieter sollten, um den verschiedenen technischen Kompetenzen ihrer (AAL-)Nutzer gerecht zu werden, Standardkonfigurationen für ihre Dienste voreinstellen, durch die die Privatsphäre der Nutzer möglichst umfassend geschützt wird. Außerdem sollten die Anbieter zum Schutz der Privatsphäre ihrer Nutzer Fehleinstellungen möglichst systemseitig verhindern und dadurch einem Missbrauch durch Dritte vorbeugen. Der Nutzer sollte die Möglichkeit erhalten, sein Profil auf einfache Weise selbst zu löschen.

3.4.2 Medizindatenschutz

Viele AAL-Anwendungen werden im medizinischen und pflegerischen Bereich eingesetzt, wobei umfangreiche Gesundheitsdaten von medizinischem Personal erhoben werden. Gesundheitsdaten sind besonders sensible Daten im Sinne von § 3 Abs. 9 BDSG, so dass besondere Vorschriften einschlägig sind. Zum einen enthält das BDSG[151] besondere Schutzvorschriften bzw. Erlaubnisnormen (siehe Abschnitt 3.4.2.1). Zum anderen findet das medi-

[151] Arztpraxen sind nicht-öffentliche Stellen im Sinne des § 4 Abs. 2 BDSG, so dass die §§ 27 ff. BDSG sowie die Sondernorm des § 39 BDSG Anwendung finden. Auf Krankenhäuser in privater Trägerschaft ist gleichermaßen das BDSG anzuwenden. Krankenhäuser mit öffentlich-rechtlicher Trägerschaft auf Landesebene unterliegen dem jeweiligen Landesdatenschutzrecht. Für Einrichtungen der öffentlich-rechtlichen Religionsgesellschaften gelten eigene kirchliche Datenschutzbestimmungen. In der folgenden Darstellung werden die Regelungen des BDSG für den privaten Bereich zugrunde gelegt.

zinische Standesrecht einschließlich der Regelungen zur ärztlichen Schweigepflicht, den besonderen Dokumentationspflichten und dem Fernbehandlungsverbot Anwendung (siehe Abschnitt 3.4.2.2).

3.4.2.1 Allgemeines Datenschutzrecht

§ 3 Abs. 9 BDSG unterwirft Gesundheitsdaten einem besonderen Regime, so dass die für sie geltenden besonderen Vorschriften und Schutzbestimmungen Anwendung finden. Eine Erlaubnisnorm für Gesundheitsdaten stellt § 28 Abs. 7 BDSG dar. Nach dieser Vorschrift ist das Erheben von personenbezogenen Gesundheitsdaten zulässig, wenn dies zum Zweck der Gesundheitsvorsorge, der medizinische Diagnostik, der Gesundheitsversorgung oder Behandlung oder für die Verwaltung von Gesundheitsdiensten erforderlich ist und die Verarbeitung der Daten durch ärztliches Personal oder durch sonstige Personen erfolgt, die einer entsprechenden Geheimhaltungspflicht unterliegen. Hinsichtlich der Beteiligung Dritter ergeben sich danach erhöhte Anforderungen für diejenigen, die nicht einer gesetzlichen Verpflichtung zur Verschwiegenheit unterliegen. Sie müssen in die im Datenschutzrecht und im Berufsrecht geltenden Vorgaben für Dokumentation und Schweigepflicht eingebunden werden.

AAL-Anwendungen kommen im Regelfall im Behandlungszusammenhang zum Einsatz. Es gilt daher gemäß dem o.g. § 28 Abs. 7 BDSG, dass die für die Erfüllung der Verpflichtung aus dem Behandlungsverhältnis notwendigen Daten auch ohne Einwilligung des Patienten erhoben und verarbeitet werden dürfen, wenn die Datenverarbeitung erforderlich ist. Überschreitet die Datenverarbeitung die Grenzen des Erforderlichen oder das Maß des Üblichen, gemessen an den Erwartungen des Patienten, ist eine gesonderte Einwilligung des Patienten erforderlich. AAL-Dienstleistungen, die sich im Regelfall noch nicht standardmäßig etabliert haben, bedürfen daher im Regelfall einer gesonderten schriftlichen Einwilligung des Patienten entsprechend den Anforderungen gem. § 4a BDSG.[152] Dabei ist die spezifische Anforderung des § 4a Abs. 3 BDSG zu beachten, d.h., die Einwilligung muss sich über die sonstigen Anforderungen hinaus ausdrücklich auf die Gesundheitsdaten beziehen.

Vor der Einführung automatisierter Verfahren, in denen medizinische Daten verarbeitet werden, ist eine Vorabkontrolle durchzuführen. Eine Vorabkontrolle ist eine Prüfung, ob die Datenverarbeitung mit den gesetzlichen Regelungen in Einklang steht und ob die erforderlichen technischen und organisatorischen Maßnahmen umgesetzt werden. Diese Prüfung erfolgt durch den betrieblichen bzw. behördlichen Datenschutzbeauftragten oder, wenn ein solcher nicht bestellt ist, durch die zuständige Datenschutzaufsichtsbehörde, § 4d Abs. 5, 6 BDSG.

[152] Vgl. Dierks, Rechtsfragen der Telemedizin – eine Übersicht, in: Rechtliche Aspekte der Telemedizin, 2006, S. 13.

3.4.2.2 Ärztliches Berufsrecht

Neben dem Datenschutzrecht ist bei der Verarbeitung von Patientendaten ärztliches Berufsrecht anzuwenden. Dies umfasst insbesondere Regelungen zur ärztlichen Schweigepflicht (siehe Abschnitt 3.4.2.2.1), zu ärztlichen Dokumentationspflichten (siehe Abschnitt 3.4.2.2.2) sowie zum Fernbehandlungsverbot (siehe Abschnitt 3.4.2.2.3).

3.4.2.2.1 Ärztliche Schweigepflicht

Grundsatz

Ärzte unterliegen der ärztlichen Schweigepflicht; sie haben also das sog. Patientengeheimnis zu wahren. Die Schweigepflicht ist im Strafgesetzbuch (StGB) verankert; die Regelung wird in den ärztlichen Berufsordnungen der (Landes-)Ärztekammern wiederholt. Soweit es um die Weitergabe von Daten aus einer medizinischen Behandlung durch Ärzte oder Krankenhäuser an Dritte geht, sind neben den Vorschriften der Datenschutzgesetze auch die Vorgaben zu beachten, die sich aus dem Recht der ärztlichen Schweigepflicht ergeben.[153] Dies folgt aus § 1 Abs. 3 Satz 2 BDSG, wonach die Verpflichtung zur Wahrung von Berufsgeheimnissen von den Regelungen des BDSG unberührt bleibt. Zudem verweist das materielle Datenschutzrecht in § 28 Abs. 7 BDSG unmittelbar auf das Recht der ärztlichen Schweigepflicht.

Nach § 203 StGB werden unter anderem die Angehörigen der Heilberufe mit Freiheitsstrafe bis zu einem Jahr oder mit Geldstrafe bestraft, wenn sie unbefugt ein fremdes Geheimnis offenbaren. Als fremdes Geheimnis gilt alles, was der Berufsgeheimnisträger im Rahmen seiner Berufsausübung von seinen Patienten erfährt. Schon die Tatsache eines Arztbesuches fällt unter das Berufsgeheimnis und damit unter den strafrechtlichen Schutz des § 203 StGB. Unter das Arztgeheimnis fallen daneben medizinische Informationen über den Patienten, z.B. die Diagnose, die Therapievorschläge und die Befunde. Neben der Strafnorm des § 203 StGB ist das Arztgeheimnis durch das Zeugnis- und Gutachtenverweigerungsrecht (§§ 53 Abs. 1 Nr. 3, 53a, 76 Strafprozessordnung (StPO)), das Beschlagnahmeverbot (§ 97 StPO) sowie das eingeschränkte Durchsuchungsrecht gem. § 103 Abs. 1 StPO geschützt. Diese Vorschriften dienen gleichermaßen dem Schutz des Vertrauensverhältnisses zwischen Arzt und Patient und des Rechts auf informationelle Selbstbestimmung.[154] Der Sinn der ärztlichen Schweigepflicht besteht darin, dass sich die Patienten vertrauensvoll an einen Arzt wenden oder in ein Krankenhaus zum Zweck einer Untersuchung begeben können, ohne fürchten zu müssen, dass die zum Teil besonders sensiblen Informationen, die sie bei der Behandlung offenlegen, zu ihrem Schaden oder Nachteil genutzt werden. Vertrauen auf der

[153] Vgl. z.B. Gundermann, Datenschutz und ärztliche Schweigepflicht, in: Trill (Hrsg.), Praxisbuch eHealth, 2009, S. 175.

[154] Hanika, in: Rieger / Dahm / Steinhilper (Hrsg.), Heidelberger Kommentar Arztrecht – Krankenhausrecht – Medizinrecht, Stand Nov. 2008, Stichwort Datenschutz, Nr. 1340, Rn. 22.

Seite des Patienten setzt daher notwendigerweise Verschwiegenheit auf der Seite des Arztes voraus.[155] Diese Verschwiegenheit ist damit Basis für eine auf Heilung ausgerichtete Patient-Arzt-Beziehung.[156]

Eine verbotene Verletzung der Schweigepflicht liegt jedoch nur dann vor, wenn die fragliche Information an einen Empfänger weitergegeben wird, der nicht zu dem Kreis der „zum Wissen berufenen Personen" gehört. Dies sind die Personen, die zum sog. Behandlungsteam gehören. Das Behandlungsteam umfasst in einer Arztpraxis das ärztliche Hilfepersonal und im Krankenhaus zusätzlich die zur Station gehörenden Ärzte und das medizinische Hilfspersonal. Die ärztliche Schweigepflicht gilt danach grundsätzlich auch zwischen Ärzten, die nicht demselben Behandlungsteam angehören.[157] Dies gilt z.B. für die (anderen) Ärzte einer Praxisgemeinschaft sowie den Konsiliararzt und externe Ärzte.[158]

Durchbrechung der ärztlichen Schweigepflicht

Ärzte sind von der Schweigepflicht entbunden, d.h. zur Offenbarung befugt, wenn sich dies aus dem Behandlungsvertrag ergibt, gesetzliche Aussage- oder Anzeigepflichten bestehen oder sie vom Patienten von der Schweigepflicht entbunden worden sind. Gesetzliche Befugnisse zur Offenbarung können sich insbesondere aus den Krebsregistergesetzen, dem Infektionsschutzgesetz und dem SGB V ergeben.

Eine stillschweigende Einwilligung des Patienten wird dann als ausreichend angesehen, wenn es im Rahmen einer Mit-, Weiter- oder Nachbehandlung zu einem für die Behandlung notwendigen Informationsaustausch zwischen den beteiligten Ärzten kommt.[159] Diese stillschweigende Einwilligung setzt voraus, dass der Patient Kenntnis von der Informationsweitergabe hat. Denn nur in diesem Fall kann sein Schweigen als Zustimmung zur Datenweitergabe gedeutet werden. Aus diesem Grund gilt hier das oben bereits Ausgeführte: Eine Durchbrechung der Schweigepflicht im Rahmen von bzw. mittels AAL-Anwendungen bedarf der ausdrücklichen Einwilligung der Betroffenen, da der Einsatz solcher Systeme noch nicht zum medizinischen Standard gehört und vom Patienten nicht erwartet wird.

Ausnahmsweise kann auch eine mutmaßliche Einwilligung ausreichend sein, wenn eine ausdrückliche Einwilligung des Patienten nicht, nicht rechtzeitig oder nicht ohne Gefährdung

---

155 Siehe auch: BVerfGE 32, 379 f. = NJW 1972, 1123.

156 Weichert, Vertraulichkeitsschutz durch IT-Sicherheit bei der elektronischen Gesundheitskarte, Vortrag abrufbar unter: https://www.datenschutzzentrum.de/vortraege/050510_weichert_bsi.htm.

157 Schurig, Datenschutz und Telemedizin, in: Rechtliche Aspekte der Telemedizin, 2006, S. 38.

158 Ausführlich dazu Gundermann, Datenschutz und ärztliche Schweigepflicht, in: Trill (Hrsg.), Praxishandbuch eHealth, 2009, S. 168 ff.

159 Dazu bestimmte § 9 Abs. 4 der Musterberufsordnung Ärzte: Wenn mehrere Ärztinnen und Ärzte gleichzeitig oder nacheinander dieselbe Patientin oder denselben Patienten untersuchen oder behandeln, so sind sie untereinander von der Schweigepflicht insoweit befreit, als das Einverständnis der Patientin oder des Patienten vorliegt oder anzunehmen ist.

seiner Interessen eingeholt werden kann, bei objektiver Beurteilung jedoch davon ausgegangen werden muss, dass er im Falle seiner Befragung mit der Geheimnisoffenbarung einverstanden wäre (z.B. bei Bewusstlosigkeit des Patienten).[160]

Die Einschaltung privater Verrechnungsstellen sowie externer Dienstleister bedarf nach gefestigter Rechtsprechung immer der ausdrücklichen Einwilligung.[161]

Im Ergebnis wird bei AAL-Anwendungen regelmäßig eine ausdrückliche Schweigepflichtentbindung des Patienten erforderlich sein. Hier müssen wiederum die bereits dargestellten Anforderungen an eine Einwilligung nach § 4a BDSG erfüllt werden. Spezialgesetzliche Regelungen zur Einwilligung sind dabei in § 73 Abs. 1b SGB V sowie in §§ 140a ff. (integrierte Versorgung) SGB V enthalten:

§ 73 Abs. 1b SGB V: gesetzliche Ermächtigung des Hausarztes

„Ein Hausarzt darf mit schriftlicher Einwilligung des Versicherten, die widerrufen werden kann, bei Leistungserbringern, die einen seiner Patienten behandeln, die diesen Versicherten betreffenden Behandlungsdaten und Befunde zum Zwecke der Dokumentation und der weiteren Behandlung erheben. Die einen Versicherten behandelnden Leistungserbringer sind verpflichtet, den Versicherten nach dem von ihm gewählten Hausarzt zu fragen und diesem mit schriftlicher Einwilligung des Versicherten, die widerrufen werden kann, die gesetzlich festgelegten Daten zum Zwecke der bei diesem durchzuführenden Dokumentation und der weiteren Behandlung zu übermitteln; die behandelnden Leistungserbringer sind berechtigt, mit schriftlicher Einwilligung des Versicherten, die widerrufen werden kann, die für die Behandlung erforderlichen Behandlungsdaten und Befunde bei dem Hausarzt und anderen Leistungserbringern zu erheben und für die Zwecke der von ihnen zu erbringenden Leistungen zu verarbeiten und zu nutzen. Der Hausarzt darf die ihm nach den Sätzen 1 und 2 übermittelten Daten nur zu dem Zweck verarbeiten und nutzen, zu dem sie ihm übermittelt worden sind; er ist berechtigt und verpflichtet, die für die Behandlung erforderlichen Daten und Befunde an die den Versicherten auch behandelnden Leistungserbringer mit dessen schriftlicher Einwilligung, die widerrufen werden kann, zu übermitteln. [...]“

§§ 140a ff. SGB V: Teilnahme an einer integrierten Versorgung

Eine Datenverarbeitung wird ebenfalls in den §§ 140a ff. SGB V im Rahmen der sog. integrierten Versorgung geregelt. Sinn dieser Vorschriften ist die bessere Vernetzung der einzelnen gesundheitlichen Versorgungsbereiche. Die an der integrierten Versorgung Beteiligten sorgen dafür, dass eine ausreichende Dokumentation sichergestellt ist, die allen Beteiligten im jeweils erforderlichen Umfang zugänglich gemacht werden

[160] Vgl. dazu Ulsenheimer, in: Laufs/Kern (Hrsg.), Handbuch des Arztrechts, 4. Auflage, 2010, § 67 Rn. 10.

[161] Dazu auch im Folgenden unter dem Stichwort „Einschaltung externer Dienstleister“.

muss (§ 240b Abs. 3 SGB V). Nimmt der Versicherte an einer Form der integrierten Versorgung teil, darf der behandelnde Leistungserbringer aus dieser gemeinsamen Dokumentation die den Versicherten betreffenden Gesundheitsdaten abrufen unter der Voraussetzung, dass dieser ihm gegenüber seine Einwilligung erteilt hat und der Empfänger § 203 StGB unterliegt.

Beide Versorgungssysteme, das System über den Hausarzt und die integrierte Versorgung, bieten sich für die Telemedizin – und damit auch für AAL-Anwendungen – geradezu an, da sie eine Zusammenarbeit zwischen verschiedenen Leistungserbringern im Gesundheitswesen in Hinblick auf den Informationsaustausch regeln. Aus datenschutzrechtlicher Sicht wird durch sie jedoch keine unmittelbare Erlaubnisnorm für die Datenerhebung und -verarbeitung eingeführt. Vielmehr hängt eine (tele-)medizinische Zusammenarbeit weiterhin von der Einwilligung des Patienten ab. Diese muss im Falle des § 73 Abs. 1b SGB V schriftlich erteilt werden. Folglich ist die Telemedizin auch nach diesen Normen nur mit der Einwilligung des Patienten zulässig.

Einbindung in ein Praxisnetz

AAL-Verfahren ermöglichen unter Umständen den Abruf von Patientendaten über ein Datennetz. Patientendaten können nach Erteilung einer Einwilligung des Patienten im Einzelfall für einen Zugriff durch den Berechtigten freigegeben werden. Ein Zum-Abruf-Bereitstellen gem. § 10 BDSG von Patientendaten durch einen Arzt über ein Datennetz ist nach der aktuellen Gesetzeslage nicht zulässig,[162] weil der Arzt vor einer Übermittlung von Patientendaten an Dritte verpflichtet ist, zu prüfen, ob eine Befugnis zur Offenbarung der Daten an den Empfänger vorliegt. Vor jeder Abfrage ist die Freischaltung durch den „Datenherrn", d.h. den behandelnden Arzt, erforderlich. In der Bereitstellung zum Abruf von Patientendaten liegt bereits eine unbefugte Offenbarung. Hielte ein Arzt Patientendaten für einen Abruf durch Dritte bereit und käme es zu einem Abruf, der nicht durch eine Einwilligung oder gesetzliche Grundlage gedeckt wäre, hätte er sich nach § 203 StGB strafbar gemacht.[163]

Krankheitsdaten in einem zentralen Datenbestand zum Abruf durch andere Ärzte bereitzuhalten, bedarf daher zunächst einer grundsätzlichen Einwilligung des Betroffenen und zusätzlich der jeweiligen Freigabe des Patienten in Bezug auf die Übermittlung von Daten in jedem Einzelfall.[164] Im Ergebnis sind danach nur solche automatisierte Übermittlungsverfah-

[162] Schurig, Datenschutz und Telemedizin, in: Rechtliche Aspekte der Telemedizin, 2006, S. 38.

[163] Konferenz der Datenschutzbeauftragten des Bundes und der Länder, Datenschutz und Telemedizin – Anforderungen an Medizinnetze, Oktober 2002.

[164] Schurig, Datenschutz und Telemedizin, in: Rechtliche Aspekte der Telemedizin, 2006, S. 38.

ren zulässig, bei denen neben der ärztlichen Freischaltung auch eine technische Autorisierung durch den Patienten vorgesehen ist.[165]

Einschaltung externer Dienstleister

Für den Einsatz von AAL-Anwendungen im medizinischen und pflegerischen Bereich ist die Einschaltung externer Dritter von besonderer Bedeutung. Im Regelfall werden die durch die AAL-Anwendung erhobenen Daten in die Praxissoftware der Arztpraxis oder Klinik aufgenommen und gespeichert. Die Software wird typischerweise von einer Servicefirma gewartet. Eine solche Wartung birgt immer das Risiko, dass auf Patientendaten zugegriffen werden kann, so dass hier technische und organisatorische Maßnahmen zum Schutz dieser personenbezogenen Daten erforderlich sind.

Ein Zugang zu personenbezogenen Patientendaten durch externe Dritte ist geeignet, eine strafbewehrte Durchbrechung der ärztlichen Schweigepflicht zu verwirklichen (§ 203 StGB). Ein Arzt darf daher grundsätzlich keine externen Dritte ohne Einwilligung des Betroffenen einschalten. Bei der Beauftragung eines externen Dritten (Auftragsdatenverarbeitung) kann bei geeigneter Gestaltung der Systeme durch Verschlüsselung der medizinischen Daten sichergestellt werden, dass es dem Auftragnehmer nicht möglich ist, personenbezogene medizinische Daten im Klartext zur Kenntnis zu nehmen.[166]

Kann ein Zugriff nicht verhindert werden, so bedarf es einer ausdrücklichen Einwilligungserklärung des Betroffenen. Eine stillschweigende Einwilligungserklärung kommt nicht in Betracht, da für den Betroffenen regelmäßig nicht erkennbar ist, welche Stelle in welchem Umfang und mit welchen konkreten Aufgaben in die Verarbeitung einbezogen wird. Im Hinblick auf die gebotene Rechtssicherheit sollten die Patienten ersucht werden, die Einwilligungserklärung schriftlich abzugeben. Eine Einwilligung wäre jedoch dann verzichtbar, wenn in einer spezialgesetzlichen Regelung eines Landes (insb. eines Landeskrankenhausgesetzes, wenn dort das Telemonitoring eingeführt wird) eine Rechtsgrundlage zur Durchbrechung der Schweigepflicht bei der Einschaltung externer Stellen enthalten ist.[167]

Aber auch wenn eine Rechtsgrundlage für eine Datenweitergabe zur Auftragsdatenverarbeitung vorliegt, müssen die erforderlichen technischen und organisatorischen Maßnahmen zur Datensicherheit getroffen werden. Dies bedeutet insbesondere, dass der Kreis derjenigen Personen, die personenbezogene Patientendaten zur Kenntnis erhalten, so weit wie möglich

---

[165] Weichert, Datenschutzrechtliche Anforderungen an zertifizierte IT-Produkte für den Bereich Telemedizin, Vortrag bei der Sommerakademie 2003, abrufbar unter: https://www.datenschutzzentrum.de/sommerakademie/2003/sak03wei.htm#4.

[166] Beispielsweise liegt bei Konzepten zur digitalen externen Archivierung, bei denen eine Verschlüsselung aller Informationen vorgesehen ist, keine Durchbrechung der ärztlichen Schweigepflicht vor.

[167] Gundermann, Datenschutz und ärztliche Schweigepflicht, in: Trill (Hrsg.), Praxishandbuch eHealth, 2009, S. 172, der weiter ausführt, dass im Hinblick auf die wachsende Bedeutung der Telemedizin entsprechende gesetzliche Änderungen erwogen werden könnten.

begrenzt werden bzw. unter Umständen sogar eine Kenntnisnahme der personenbezogenen Daten vollständig ausgeschlossen werden muss.

Keine Aufzeichnung der Verbindungsdaten

Nicht vereinbar mit der ärztlichen Schweigepflicht ist eine Aufzeichnung von Verbindungsdaten bei jeder Art von elektronischer Kommunikation mit dem Arzt. Aus den Verbindungsdaten dürfen sich keine Rückschlüsse auf die Identität des Patienten ergeben, da bereits die Tatsache der Kontaktaufnahme mit dem Arzt seiner Schweigepflicht unterfällt.[168] Nur die Berufsgeheimnisträger selbst sind (außer dem Patienten für seinen eigenen Bereich) berechtigt, solche Daten zu speichern. Es darf also keine automatische Speicherung von E-Mail-Adressen der Patienten in Systemen geben, auf die von anderen Personen als den Ärzten und sonstigen Schweigepflichtigen zugegriffen werden kann. Lässt sich eine solche Speicherung nicht vermeiden, muss eine ausdrückliche Einwilligung bzw. Entbindung von der Schweigepflicht vorliegen.

Herausforderungen und offene Fragen

Im AAL-Bereich kommt die ärztliche Schweigepflicht gem. § 203 StGB aufgrund der Komplexität der Systeme besonders zum Tragen. AAL-Anwendungen und moderne IT-Infrastruktur erleichtern zunächst durch ihre elektronische Vorhaltung den Zugang zu medizinischen Daten, was entsprechende Vorkehrungen zum Schutz vor Zugriffen unbefugter Dritter erfordert. Zugleich bedeutet die Weitergabe der personenbezogenen Patientendaten an einen externen Dritten wie einen AAL-Anbieter oder einen Dienstleister grundsätzlich eine Durchbrechung der ärztlichen Schweigepflicht, so dass der Arzt für diese Datenweitergabe eine rechtliche Befugnis i.S.v. § 203 StGB benötigt, mithin die Einwilligung der Patienten oder eine gesetzliche Ermächtigung. Einige Landeskrankenhausgesetze sehen z.B. die Möglichkeit einer Auftragsdatenverarbeitung für die Krankenhäuser vor und enthalten damit eine gesetzliche Offenbarungsbefugnis. Es stellt sich daher die Frage, ob die Einführung von weiteren Offenbarungsvorschriften, wie z.B. in einigen Landeskrankenhausgesetzen bereits vorgenommen, erforderlich ist.

Daneben ist zu prüfen, ob durch die zunehmende Einschaltung Dritter, wie sie gerade im AAL-Bereich und durch die Einrichtung von entsprechenden Infrastrukturen zu erwarten ist, noch ein ausreichendes Schutzniveau bezüglich des Vertrauensverhältnisses zwischen Patient und Arzt vorhanden ist oder ob es diesbezüglichen Anpassungsbedarf gibt.

Ein Outsourcing von sensiblen Daten wie im AAL-Bereich steht zugleich vor der praktischen Herausforderung, dass der Auftraggeber, der einen Auftragnehmer beauftragt, Verantwortli-

[168] Gundermann, Datenschutz und ärztliche Schweigepflicht, in: Trill (Hrsg.), Praxishandbuch eHealth, 2009, S. 167.

cher bleibt und sich damit Einflussmöglichkeiten auf die Datenverarbeitung vorbehalten muss. Dies wird in der Praxis umso schwieriger, je komplexer das System ist, das durch den Auftragnehmer zum Einsatz kommt. Eine offene Frage besteht darin, auf welche Weise in solchen Fällen eine Beherrschbarkeit gewährleistet werden kann und ob ausgleichende Maßnahmen, z.B. durch Einführung von Anzeigepflichten, zu treffen sind.

Außerdem wird von Ärzten und medizinischem Personal ein nicht unerhebliches Verständnis der technischen Abläufe erwartet, um Risiken durch entsprechende Maßnahmen geeignet begegnen zu können und die Betroffenen aufzuklären. Es ist zu untersuchen, inwieweit die medizinische Aus- und Fortbildung diese Themen aufnehmen kann und ein Nachweis über ein solches Wissen bei Verwendung von AAL-Systemen verpflichtend werden soll.

3.4.2.2.2 Ärztliche Dokumentationspflichten

Nach der Berufsordnung ist der Arzt verpflichtet, die im Rahmen des Behandlungszusammenhangs erforderlichen Aufzeichnungen über die in Ausübung seines Berufs gemachten Feststellungen und getroffenen Maßnahmen anzufertigen. Es handelt sich um eine vertragliche Nebenpflicht aus dem Behandlungsvertrag. Ist die Dokumentation lückenhaft, kann dies im Haftungsprozess eine Umkehr der Beweislast zugunsten des Patienten nach sich ziehen. Digitalisierte Dokumente können in Bezug auf den Nachweis der Urheberschaft und Echtheit Mängel aufweisen.[169]

Bei ärztlichen Unterlagen gilt, dass diese aus Dokumentationsgründen in jedem Fall zehn Jahre lang aufbewahrt werden müssen, § 10 Abs. 3 Berufsmusterordnung der Ärzte (BMO-Ä). Nach § 32 Abs. 2 Strahlenschutzverordnung und § 28 Abs. 4 Nr. 1 Röntgenverordnung (RöV) sind Aufzeichnungen über die Behandlung mit radioaktiven Stoffen sowie über Röntgenbehandlungen dreißig Jahre nach der letzten Behandlung aufzubewahren. Aus Behandlungsgründen, etwa bei chronischen Krankheiten oder Transplantationen kann sich eine Aufbewahrungsdauer von über dreißig Jahren ergeben.

Erfolgt innerhalb des medizinischen Bereichs eine Speicherung nach verschiedenen Zwecken, so besteht u.U. eine frühere Löschpflicht. So unterliegen z.B. sämtliche Abrechnungsdaten nicht der medizinischen Dokumentationspflicht. Diese Daten werden nicht mehr benötigt, wenn sie für finanzrechtliche Zwecke (Abrechnung nach SGB V, Dokumentationspflichten nach Handelsgesetzbuch bzw. Steuerrecht) nicht mehr aufbewahrt werden müssen.

AAL-Anwendungen sind so zu gestalten, dass sie die Ärzte in ihren Dokumentationspflichten unterstützen. Dies beinhaltet auch, dass für unterschiedliche Daten die verschiedenen Löschfristen berücksichtigt und die Löschungen automatisiert umgesetzt werden können.

[169] Gundermann, Datenschutz und ärztliche Schweigepflicht, in: Trill (Hrsg.), Praxishandbuch eHealth, 2009, S. 173.

Daten mit unterschiedlichen Löschfristen sind getrennt voneinander zu speichern, so dass Daten mit früherem Löschdatum tatsächlich rückstandsfrei entfernt werden können.

3.4.2.2.3 Fernbehandlungsverbot

Grundsatz

Nach § 7 Abs. 3 BMO-Ä dürfen Ärzte „individuelle ärztliche Behandlung, insbesondere auch Beratung, weder ausschließlich brieflich noch in Zeitungen oder Zeitschriften noch ausschließlich über Kommunikationsmedien oder Computerkommunikationsnetze“ durchführen. Schutzgedanke ist, dass eine Behandlung ohne eine persönliche Patient-Arzt-Beziehung nicht zulässig ist. Entscheidend ist, dass die Behandlung nicht ausschließlich durch die o.g. (unpersönlichen) Kommunikationswege erfolgt.

Telematische Anwendungen sind daher immer dann zulässig, wenn im Rahmen eines therapeutischen Gesamtkonzepts sichergestellt wird, dass dem Patienten ausreichende Möglichkeiten einer persönlichen Patient-Arzt-Beziehung verbleiben, auch wenn diese nicht mit dem Fernbehandler selbst bestehen.[170] Daher ist die Tätigkeit eines Arztes in einem Telemonitoring-Center keine „ausschließliche“ Fernbehandlung des Patienten, wenn der Patient in den für den Einzelfall erforderlichen Abständen weiterhin im persönlichen Kontakt mit dem Primärbehandler steht. Ausgeschlossen ist danach nur eine ausschließliche telefonische bzw. über das Internet erfolgende Beratung durch einen Arzt, der seinen Patienten zuvor noch nie leibhaftig gesehen hat.[171]

Nach § 9 Heilmittelwerbegesetz (HWG) besteht ein Werbeverbot für Fernbehandlungen.

Herausforderungen und offene Fragen

Bei AAL-Anwendungen kann es sich in bestimmten Fällen durchaus um eine ausschließliche Fernbehandlung des Patienten handeln. Daher ist zu prüfen, ob und ggf. unter welchen Voraussetzungen das Verbot ausschließlicher Fernbehandlung aufgehoben werden kann. Zu diesem Zweck sollte herausgearbeitet werden, in welchen Fällen z.B. eine Fernbehandlung unbedenklich und ungefährlich für den Patienten ist und wo kein besonderes Vertrauensverhältnis zwischen Patient und Arzt erforderlich ist. Entsprechend ist zu prüfen, ob und inwiefern das Werbeverbot nach § 9 HWG aufgehoben oder gelockert werden sollte.

---

[170] Dierks, Rechtsfragen der Telemedizin, in: Rechtliche Aspekte der Telemedizin, S. 14.

[171] Gundermann, Datenschutz und ärztliche Schweigepflicht, in: Trill (Hrsg.), Praxishandbuch eHealth, 2009, S. 165, wobei selbst eine reine telefonische Beratung zum Teil von Callcentern der Krankenkassen durchgeführt und danach von diesen als rechtlich zulässig angesehen werden.

3.4.3 Sozialdatenschutz

Der Sozialdatenschutz erlangt im Zusammenhang mit AAL-Anwendungen immer dann Bedeutung, wenn diese im medizinischen und pflegerischen Bereich eingesetzt werden und die mit der Anwendung erhobenen und verarbeiteten personenbezogenen Daten an die Sozialversicherungen weitergeleitet werden. Für AAL-Anwendungen in diesem Bereich bedeutet dies, dass sie so konzipiert und konfiguriert sein müssen, dass die Aufzeichnungen und Datenübermittlungen an die Sozialversicherungen den gesetzlichen Anforderungen des Sozialdatenschutzes genügen.

Eine andere Frage ist, ob der Einsatz bzw. die Kosten von AAL-Anwendungen von den Sozialversicherungen überhaupt übernommen werden. Dieser Frage wird in Kapitel 6 zu Sozialversicherungsrecht nachgegangen.

Im Folgenden werden die für AAL-Anwendungen besonders relevanten Regelungen zu Sozialdatenschutz skizziert. Dies beginnt mit einer Definition von Sozialdaten (siehe Abschnitt 3.4.3.1) und einer Beschreibung des Sozialgeheimnisses (siehe Abschnitt 3.4.3.2). Weiterhin werden Sonderregelungen des SGB angerissen, die sich auf die integrierte Versorgung sowie Auftragsdatenverarbeitung beziehen (siehe Abschnitt 3.4.3.3). Schließlich wird die Datenerhebungs- und Speicherbefugnis der Kranken- und Pflegekassen vorgestellt (siehe Abschnitt 3.4.3.4).

3.4.3.1 Sozialdaten

Sozialdaten sind nach der Legaldefinition in § 67 Abs. 1 Satz 2 SGB X „Einzelangaben über persönliche oder sachliche Verhältnisse einer bestimmten oder bestimmbaren natürlichen Person (Betroffener), die von einer in § 35 des Ersten Buches genannten Stelle im Hinblick auf ihre Aufgaben nach diesem Gesetzbuch erhoben, verarbeitet oder genutzt werden“. Um den Möglichkeiten der modernen Datenverarbeitung Rechnung zu tragen, ist der Begriff weit zu verstehen.[172] Zu den Sozialdaten gehören daher alle Angaben, die eine Person bestimmen oder bestimmbar machen, die einen Sachverhalt beschreiben, der sich auf den Betroffenen bezieht, wie insbesondere Datum und Ort der Geburt, Namen, Anschrift, Beruf, Beschäftigung und Arbeitgeber, selbstständige Tätigkeit, Versicherungsverhältnisse, Sozialversicherungsnummer, Einkommens- und Vermögensverhältnisse, behandelnde Ärzte und andere Leistungserbringer, Zeiten der Arbeitsunfähigkeit, Krankheiten und Behinderungen usw. Sozialdaten können sich dabei nicht nur auf Versicherte, sondern auf alle natürlichen Personen (Betroffene) beziehen, über die die o.g. Stellen Informationen verarbeiten. Nicht zu den Sozialdaten gehören aggregierte Sammelangaben über Personengruppen, mit denen sich kein Bezug zu einzelnen Betroffenen herstellen lässt, insbesondere statistische Daten. Per-

[172] Kranig, in: Hauck / Noftz (Hrsg.), Sozialgesetzbuch V, Gesetzliche Krankenversicherung, Loseblatt-Kommentar, Stand 2006, § 284 Rn. 6.

sonenbezogene Daten lassen sich anonymisieren (§ 67 Abs. 8 SGB X) oder pseudonymisieren (§ 76 Abs. 8a SGB X).

3.4.3.2 Sozialgeheimnis

Das Sozialgeheimnis ist in § 35 SGB I geregelt und wird in den §§ 67 ff. SGB X präzisiert. Gemäß § 35 Abs. 1 Satz 1 SGB I hat jeder einen Anspruch darauf, dass die ihn betreffenden Sozialdaten von den (oben genannten) Leistungsträgern nicht unbefugt erhoben, verarbeitet oder genutzt werden. Die Wahrung des Sozialgeheimnisses umfasst die Verpflichtung, auch innerhalb des Leistungsträgers sicherzustellen, dass die Sozialdaten nur Befugten zugänglich sind oder nur an diese weitergegeben werden (§ 35 Abs. 1 Satz 2 SGB I).

3.4.3.3 Sonderregelungen im SGB für den AAL-Bereich

Neben diesem allgemeinen Grundsatz ist im AAL-Bereich vor allem eine Sonderregelung von Bedeutung, auf die bereits im Rahmen des Medizindatenschutzes eingegangen worden ist: die integrierte Versorgung nach §§ 140a ff. SGB V, da diese sich für den Einsatz von AAL-Technik und -Systemen besonders anbietet (siehe Abschnitt 3.4.2.2.1).

Des Weiteren gelten besondere Bestimmungen bezüglich der Auftragsdatenverarbeitung. Die Einschaltung von AAL-Dienstleistern im medizinischen und pflegerischen Bereich ist auch durch die Krankenkassen bzw. Pflegekassen denkbar. Bei dieser Einschaltung muss aus datenschutzrechtlicher Sicht die für die Krankenkassen und Pflegekassen geltende Sonderregelung der Auftragsdatenverarbeitung in § 80 SGB X beachtet werden, die ähnlich wie § 11 BDSG Vorgaben zur Art und Weise der Auftragsdatenverarbeitung macht. Bei Verträgen mit nicht-öffentlichen Stellen gelten darüber hinaus besondere Anforderungen. Nach § 80 Abs. 5 SGB X ist die Erhebung, Verarbeitung oder Nutzung von Sozialdaten im Auftrag durch nicht-öffentliche Stellen nur zulässig, wenn beim Auftraggeber sonst Störungen im Betriebsablauf auftreten können (Nr. 1) oder die übertragenen Arbeiten beim Auftragnehmer erheblich kostengünstiger besorgt werden können und der Auftrag nicht die Speicherung des gesamten Datenbestands des Auftraggebers umfasst. Der überwiegende Teil der Speicherung des gesamten Datenbestands muss beim Auftraggeber oder beim Auftragnehmer, der eine öffentliche Stelle ist und die Daten zur weiteren Datenverarbeitung im Auftrag an nicht-öffentliche Auftragnehmer weitergibt, verbleiben (Nr. 2). Hier stellen sich im Ergebnis dieselben Fragen zur Auftragsdatenverarbeitung wie bereits oben geschildert beim Outsourcing von Daten durch Ärzte (siehe Abschnitt 3.4.2.2.1).

3.4.3.4 Datenerhebungs- und Speicherbefugnis der Kranken- und Pflegekassen

Die Kranken- und Pflegekassen dürfen Daten nur erheben und speichern, wenn sie hierfür eine Befugnis haben. Diese Erhebungsbefugnis finden ihre Grenzen an den für die gesetzliche Krankenversicherung (GKV) und die gesetzliche Pflegeversicherung (GPV) abschließend im SGB geregelten Übermittlungsbefugnissen der Leistungserbringer und Dritter.

Materielle Rechtsgrundlage für die Datenerhebung und -speicherung der gesetzlichen Krankenkassen ist § 284 Abs. 1 Satz 1 SGB V. Entsprechendes gilt für die Pflegekassen nach § 94 SGB XI.

Die Krankenkassen dürfen außerdem mit Erlaubnis der Aufsichtsbehörde die Datenbestände leistungserbringer- oder fallbeziehbar für zeitlich befristete und im Umfang begrenzte Forschungsvorhaben, insbesondere zur Gewinnung epidemiologischer Erkenntnisse, von Erkenntnissen über Zusammenhänge zwischen Erkrankungen und Arbeitsbedingungen oder von Erkenntnissen über örtliche Krankheitsschwerpunkte selbst auswerten und über die sich aus § 304 SGB V ergebenden Fristen hinaus aufbewahren.[173] Pflegekassen haben gem. § 98 SGB XI entsprechende Befugnisse.[174]

Eine Übermittlung von Daten an die Krankenkassen und Pflegekassen kommt daher nur in Betracht, wenn AAL-Anwendungen und -Dienstleitungen durch Aufnahmen in deren Leistungskatalog aufgenommen sind.[175] Dann darf unter den genannten Voraussetzungen auch eine Auswertung zu Forschungszwecken erfolgen. Besonderheiten sind hier jedoch nicht festzustellen.

3.4.4 Datenschutz von weiteren Betroffenen: Besuchern, Stellvertretern, Mitarbeitern

Neben dem Nutzer einer AAL-Anwendung kommen weitere Beteiligte in Frage, die als natürliche Person ebenfalls ein Recht auf informationelle Selbstbestimmung haben. Dies sind insbesondere die folgenden drei Gruppen:

- Besucher im (häuslichen) AAL-Umfeld des Nutzers,
- Stellvertreter: vom Nutzer beauftragte Personen seines Vertrauens, die in seinem Auftrag bestimmte Handlungen ausführen sollen,
- Mitarbeiter von beteiligten Dienstleistern.

Generell gilt, dass die Persönlichkeitsrechte der natürlichen Personen nebeneinander Bestand haben.

Bei **Besuchern** des Nutzers mit einer im Haushalt installierten AAL-Anwendung ist die Konstellation relevant, dass diese möglicherweise ebenfalls von den AAL-Sensoren erfasst und ihr Verhalten beobachtet und ausgewertet werden kann. In diesem Fall sind deren Persönlichkeitsrechte im Ergebnis gleichermaßen zu wahren. Das bedeutet vor allen Dingen, dass die Besucher durch die Sensorik bzw. die Technik erst gar nicht erfasst werden bzw. dass

[173] § 287 Abs. 1 SGB V.

[174] Udsching, SGB XI, Soziale Pflegeversicherung, Kommentar, 3. Auflage, 2010, § 98 Rn. 2.

[175] Dazu siehe Kapitel 6.

bei einer Erfassung eine Einwilligung vorliegen oder aber ein Aussetzen der Anwendung ermöglicht werden muss.

Bei gesetzlichen Vertretern des Nutzers oder ihm vertrauten Personen, die von ihm beauftragt wurden, für ihn als **Stellvertreter** tätig zu werden, können bei ihren Handlungen ebenfalls in ihrer Privatsphäre berührt sein.[176] Dies gilt in besonderem Maße, wenn der Nutzer deren Handlungen, die im Auftrag und Interesse des Nutzers erfolgen, selbst genau kontrollieren will oder dafür eine Kontrollinstanz einschaltet. Hier ist darauf hinzuwirken, dass eine faire Balance zwischen den berechtigten Interessen des Nutzers und denen seiner Vertreter gefunden wird (siehe Kapitel 7 zu Delegation in AAL-Systemen).

Werden im Rahmen von AAL-Anwendungen unterstützende Dienstleister eingebunden, so werden durch den Einsatz der Anwendung im Regelfall auch personenbezogene Daten der **Mitarbeiter** erhoben, die von dieser dritten Seite in die Prozesse der Anwendung eingebunden sind. Dann sind nicht nur die personenbezogenen Daten der Betroffenen zu schützen, sondern auch diejenigen der Mitarbeiter der Dienstleister. Der Einsatz von AAL-Technik schafft die Möglichkeit, Daten über jeden einzelnen Beschäftigten in einem weitgehenden Ausmaß zu erhalten und auszuwerten. Bei Unterstützungsleistungen z.B. mittels Monitoring-Einrichtungen kann durch das System erfasst werden, welche Arbeiten wann, mit welchem Aufwand und von wem erledigt worden sind. Für den Beschäftigten ist in vielen Fällen nicht wahrnehmbar, welche Informationen über ihn erhoben und gespeichert werden. Aufgrund seiner Abhängigkeiten im Arbeitsverhältnis kann er sich der Erhebung der Information nur schwer oder gar nicht entziehen.

Damit bergen solche technischen Einrichtungen zur Datenerhebung die Gefahr eines Eingriffs in das Persönlichkeitsrecht des Beschäftigten, so dass der Beschäftigtendatenschutz ebenfalls eine Rolle spielt. Die Verarbeitung von Beschäftigtendaten unterliegt einem besonderen Regime: Zwischen Arbeitgeber und Beschäftigten besteht ein intensives Beziehungsgeflecht, das eine umfangreiche gegenseitige Information voraussetzt. Da Beschäftigte dienstlich weisungsgebunden sind und sich in einer ökonomisch bedingten Abhängigkeit befinden,[177] zugleich aber im Rahmen des Arbeitsverhältnisses Anspruch auf Achtung ihres Persönlichkeits- und Selbstbestimmungsrechts haben, besteht ein besonderer und differenzierter Schutzbedarf.

Die Überwachung von Beschäftigten durch Arbeitgeber ist daher bereichsspezifisch zu regeln. Hier ist geboten, ein verfassungskonformes Gesetz zu schaffen, das einen gerechten Ausgleich zwischen dem Persönlichkeitsschutz von Beschäftigten einerseits und den berechtigten Kontrollbedürfnissen der Arbeitgeber andererseits vorsieht. Im Jahr 2010 hat die Bun-

[176] Hansen / Raguse / Storf / Zwingelberg, 2010, S. 27 ff.

[177] BVerfG JZ 1994, S. 410.

desregierung den Entwurf für ein Beschäftigtendatenschutzgesetz als Teil des Bundesdatenschutzgesetzes auf den Weg gebracht.[178]

3.5 Ergebnisse und offene Fragen

Obwohl das juristische Gebiet des Datenschutzes in der Literatur gut untersucht und kommentiert ist, zeigen sich Probleme in der Anwendung der datenschutzrechtlichen Regelungen auf neue Technologien. Dies zeigt sich besonders stark bei Ambient Assisted Living, das auf alle Lebensbereiche seiner Nutzer umfasst, sich durch eine Vielzahl eingebundener Dienstleister mit entsprechenden Datensammlungen und Datenflüssen auszeichnet und wo sich noch kein Standard herausgebildet hat, der als datenschutzgerecht gelten kann.

Offen ist insbesondere, wie Nutzer in einer verständlichen Form über die Datenverarbeitung informiert werden, wie sie auf dieser Basis Einwilligungen geben können, welche Kontroll- und Einflussmöglichkeiten sie haben und wie sich vermeiden lässt, dass sie dem AAL-System und seinen Betreibern ausgeliefert sind.

Weiterhin ist zu untersuchen, inwieweit das Datenschutzrecht anzupassen ist, um den modernen Anforderungen heutiger (und kommender) Technik wie Sensorik, umfassender Auswertungsmethoden und Entscheidungsunterstützungsverfahren im vernetzten System, ggf. mit Anbindung an soziale Netzwerke oder Standortdienste, zu genügen. Bedenkt man außerdem, dass für die AAL-Systeme Finanzierungsmodelle per Werbung im Gespräch sind und dass es erhebliche Interessen auf Seiten von Krankenkassen oder Versicherungen gibt, um alle für sie wesentlichen Facetten der Betroffenen auszuwerten, wird die Relevanz der Umsetzung der Datenschutzforderungen noch deutlicher.

[178] BR-Drs. 535/10. Vgl. auch die Stellungnahme des ULD zu diesem Gesetzesentwurf, abrufbar unter: https://www.datenschutzzentrum.de/arbeitnehmer/20101012-stellungnahme.html.

4 Anforderungen an die Datensicherheit und den technischen Datenschutz

Dieses Kapitel beschreibt die Anforderungen an die Gestaltung von AAL-Systemen in Bezug auf Datensicherheit und technischen Datenschutz. Basis für diese Ausführungen sind sowohl rechtliche Grundlagen als auch die Arbeiten zur Datensicherheit, die auf nationaler und internationaler Ebene ein bewährtes Instrumentarium bereitstellen und weiter entwickelt werden. Dies betrifft insbesondere die Orientierung an übergeordneten Schutzzielen, die für den jeweiligen Fall in verschiedenen Ausprägungen anzulegen und mit zugehörigen technischen und organisatorischen Maßnahmen zu unterlegen sind. Daraus resultieren juristische Fragen, z.B. für eine mögliche Festlegung, inwieweit bestimmte Schutzziele berücksichtigt werden müssen oder welche Methoden oder Maßnahmen für die Erfüllung der Anforderungen in Frage kommen.

Das Kapitel gliedert sich wie folgt: Abschnitt 4.1 stellt die verschiedenen Perspektiven von Datenschutz und Datensicherheit dar. Die Schutzziele und ihre Methodik werden in Abschnitt 4.2 erläutert. Abschnitt 4.3 erläutert Best Practices und Zertifizierungen für Datensicherheit. Schließlich fasst Abschnitt 4.4 die Ergebnisse in Bezug auf eine Anwendung auf AAL-Systeme zusammen und geht auf offene Fragen ein.

4.1 Unterschiedliche Perspektiven von Datenschutz und Datensicherheit

Die Schutzziele *Verfügbarkeit, Integrität und Vertraulichkeit* sind die konventionellen, seit den 1980er Jahren gut verstandenen, wesentlichen Schutzziele der Datensicherheit.[179] Diese Ziele beziehen sich vor allem auf die Sicherung des Betriebs insbesondere der IT von Organisationen. Im Unterschied dazu nimmt Datenschutz den Betrieb von Organisationen zunächst aus der Perspektive der von diesem Betrieb betroffenen Personen wahr, wobei es zu Konflikten zwischen den Perspektiven des Primats der Datensicherheit oder des Primats des Datenschutzes kommen kann. Eine perfekt gesicherte Kommunikationsinfrastruktur ohne Datenschutz kann dazu führen, dass sich sämtliche Aktivitäten der betroffenen Teilnehmer perfekt miteinander verbinden lassen, weil jeder authentisiert mit Aufenthalt, Tätigkeit und, im Falle von AAL, zumeist auch mit seiner körperlichen Verfassung beobachtet und protokolliert wird. Aus diesem Grund haben sich die auf Datenschutzanforderungen hin zugespitzten speziellen Datenschutz-Schutzziele *Transparenz, Intervenierbarkeit und Nichtverkettbarkeit* herausgebildet, die die konventionellen Schutzziele der Datensicherheit ergänzen.[180] Sowohl Datenschutz als auch Datensicherheit betrachten somit zwangsläufig dieselben sechs Schutzziele, allerdings aus unterschiedlichen Perspektiven. Die Schutzziele müssen im Hin-

[179] Federrath / Pfitzmann, in: DuD 2000, S. 704 ff

[180] Rost / Bock, in DuD 2011, S. 30 ff.

blick auf deren Bedeutung bzw. Wirkung für die betroffenen Personen bzw. für die Organisationen jeweils spezifiziert und profiliert werden. Sowohl Personen als auch Organisationen haben ihre jeweils eigenen Interessen der Risikominimierung in Bezug auf Datenschutz und Datensicherheit.

4.2 Schutzziele und ihre Umsetzung mittels technischer und organisatorischer Maßnahmen

Das Konzept der Arbeit mit Schutzzielen sieht vor, dass Schutzziele Maßnahmen systematisch bündeln, mit denen die Ziele sich erreichen lassen. Eine wesentliche Maßnahme, um das Schutzziel Verfügbarkeit umzusetzen, besteht beispielsweise darin, ein System oder eine Komponente eines Systems redundant auszulegen. Vertraulichkeit von Kommunikationen lässt sich beispielsweise dadurch erreichen, dass Kommunikationsinhalte verschlüsselt übertragen werden. Und das Schutzziel Integrität lässt sich umsetzen, indem über Dateien sogenannte Hashwerte vor einer Aktivität und nach einer Aktivität verglichen werden, um festzustellen, ob eine Datei verändert wurde. Die Schutzziele Transparenz, Intervenierbarkeit und Nichtverkettbarkeit kennen ebenfalls eine ganze Reihe an technischen Hilfsmitteln zu deren Umsetzung. Dies führen wir im Detail nachfolgend aus. Technische Maßnahmen sind dabei immer eingebettet in organisatorische Prozesse und Regeln, um ihre Wirksamkeit entfalten zu können.

Die Berücksichtigung der Schutzziele deckt die zu treffenden technisch-organisatorischen Maßnahmen und normativen gesetzlichen Anforderungen ab. Zwar findet man im BDSG, das in technisch-organisatorischer Hinsicht noch immer dem Zentralrechner-Paradigma der Prä-Internet-Ära verhaftet ist,[181] bislang keine Schutzziele, wohl aber in den jüngeren Landesdatenschutzgesetzen der fünf neuen Bundesländer sowie in denen von Berlin, Hamburg und Nordrhein-Westfalen.[182] In jedem Fall ist für die Erfüllung der technisch-organisatorischen Vorgaben des Datenschutzrechts die Orientierung an dem Schutzziele-Konzept sinnvoll, weil es insbesondere in der Phase einer Planung mit vielen Unwägbarkeiten – und in diesem Status befinden sich noch viele AAL-Projekte – in Bezug auf Datenschutz ungleich effizienter und kompakter umzusetzen ist als die Orientierung am „veralteten“ Anhang zu § 9 BDSG, zumal die Arbeit mit der Schutzziele-Methodik seit vielen Jahren Standard im Bereich der Datensicherheit ist.[183] Hinzu kommt, dass das Schutzziele-Konzept auf das aktuelle Grundsatz-Urteil des Bundesverfassungsgerichts zu reagieren gestattet, das ein Grundrecht

[181] Vgl. Roßnagel / Pfitzmann / Garstka, Modernisierung des Datenschutzrechts, Gutachten für das Bundesministerium des Innern, 2001.

[182] In der Entschließung der 79. Konferenz der Datenschutzbeauftragten des Bundes und der Länder vom März 2010 ist die Bedeutung der Schutzziele für eine anstehende BDSG-Novellierung herausgehoben worden.

[183] Vgl. BSI: „IT-Grundschutz“, https://www.bsi.bund.de/cln_165/ContentBSI/Publikationen/BSI_Standard/it_grundschutzstandards.html.

auf die Gewährleistung von Vertraulichkeit und Integrität eigengenutzter informationstechnischer Systeme geschaffen hat und damit zwei Schutzziele der Datensicherheit aufnimmt.

4.2.1 Schutzziele und Schutzmaßnahmen in AAL-Umgebungen

Aus technisch-organisatorischer Sicht ist zu fragen, wie sich Daten verarbeitende Systeme, zu denen die Computernetze, Computer und Programme sowie die Prozesse und Organisationen zu zählen sind, in AAL-Umgebungen so planen und betreiben lassen, dass deren Betrieb datenschutzgerecht funktionieren kann. AAL-Projekte befinden sich zurzeit überwiegend im Stadium der Planung und der ersten Pilotprojekte. Planer, Konstrukteure und Betreiber von Systemen ebenso wie Aufsichtsbehörden, Mitarbeiter und Angehörige sowie die betroffenen Nutzer von AAL-Systemen erwarten, dass die gewünschten AAL-Funktionalitäten bzw. -Dienstleistungen den materiellen Anforderungen des Rechts auf informationelle Selbstbestimmung genügen.

Zwei wesentliche Elemente des modernen Datenschutzes können den operativen Lösungskorridor dieser neuen und großen Herausforderungen öffnen: zum einen das Konzept der Schutzziele, die für die Konstruktion und den Betrieb von AAL-Infrastrukturen umzusetzen sind (siehe Abschnitt 4.2.1.1), zum anderen das Paradigma der Nutzersteuerbarkeit (siehe Abschnitt 4.2.1.2).

4.2.1.1 Schutzziele

Das Konzept der Schutzziele und Schutzmaßnahmen spielt seit Anfang der 1990er Jahre die wesentliche Rolle im Rahmen der Herstellung von Datensicherheit der Informationstechnik, insbesondere beim Militär oder anderen Erbringern gesellschaftlich kritischer Infrastrukturleistungen.[184] Zu den (elementaren) Schutzzielen des Datenschutzes zählen zum einen die drei „klassischen“ Schutzziele der Datensicherheit *Verfügbarkeit, Integrität und Vertraulichkeit*, die dann im Hinblick auf Datenschutz für natürliche Personen zu spezifizieren sind. Zum anderen kommen die drei spezifischen Schutzziele des Datenschutzes *Transparenz, Intervenierbarkeit und Nichtverkettbarkeit* hinzu.[185] Neben der Definition der Ziele umfasst das Schutzziele-Konzept Kataloge mit technisch-organisatorischen Schutzmaßnahmen zur Umsetzung der ausgewiesenen Ziele. Dabei führt das Durchdeklinieren der elementaren Schutzziele sowie weiterer zusätzlicher Schutzziele für besondere Konstellationen dazu, dass bei den Anforderungen von Datenschutz und Datensicherheit nichts Wesentliches vergessen wird.

[184] Vgl. die Auflistung in Rost / Pfitzmann, in: DuD 2009, S. 353 ff., sowie in Rost / Bock, in: DuD 2011, S. 30 ff.

[185] Vgl. Rost / Pfitzmann, in: DuD 2009, S. 353 ff., sowie Rost / Bock, in: DuD 2011, S. 30 ff.

Das Vorgehen bei der Anwendung von Schutzzielen auf konkrete Anwendungen läuft standardisiert ab: Zunächst wird der Schutzbedarf der verarbeiteten Daten ermittelt und festgelegt, den dann die Systeme, Organisationseinheiten und Prozesse, die diese Daten verarbeiten, „erben". Anschließend ist anhand der in den Katalogen aufgelisteten Maßnahmen zu entscheiden, welche Schutzmaßnahmen auf dem Stand der aktuellen Technik geeignet sind. Welche technischen und organisatorischen Maßnahmen für einen ganz konkreten Anwendungsfall einer AAL-Problemstellung in welcher Ausprägung angemessen auszuwählen sind, ergibt sich aus einer Risikoanalyse, in der der Schutzbedarf der Daten anhand der Schutzziele formuliert ist.

4.2.1.2 Nutzersteuerbarkeit

Nutzersteuerbarkeit bedeutet, dass der Nutzer eine wirksame Kontrolle über Datenerhebungen, Systeme und Datenflüsse ausüben kann. Der Nutzer muss grundsätzlich das System, das ihm helfen soll und das einen direkten Einfluss auf seine Lebensumstände und auf sein Leben hat, selbst steuern können. Kann der Betroffene dies nicht mehr selbst leisten, so soll er zumindest noch bestimmen können, welcher ihm vertraute Mensch entsprechende Steuerungsaktivitäten stellvertretend für ihn auslösen darf oder soll (Stichwort: Delegation[186]). Die Möglichkeiten zur Steuerung durch den Nutzer gehören zu den wichtigsten Maßnahmen, um das Schutzziel der Intervenierbarkeit für den Betroffenen umzusetzen. Ein wirksames Instrument zur Umsetzung von Nutzersteuerbarkeit ist dabei das Identitätenmanagement.[187]

4.2.2 Der „AAL-Würfel Datenschutz": Strukturierung in drei Dimensionen

Nachfolgend wird zunächst versucht, die Komplexität der Adressierung von Datenschutz in AAL-Systemen durch eine Schematisierung in drei Dimensionen überschaubarer zu machen („AAL-Würfel Datenschutz", siehe Abb. 8). Dieser Würfel besteht in einer Dimension aus Kategorien von Daten, die durch AAL-Systeme erzeugt werden, in der zweiten Dimension aus Kategorien beteiligter Akteure und Systeme, die zugleich für bestimmte Aktivitäten und Prozesse stehen, sowie in der dritten Dimension aus den elementaren Datenschutz-Schutzzielen.[188] Diese Unterscheidungen dienen dazu, den Transfer von Daten sowie Daten-

[186] Siehe Kapitel 7.

[187] Hansen, User-controlled identity management: the key to the future of privacy?; in: International Journal of Intellectual Property Management Vol. 2, No. 4, 2008, S. 325-344. Vgl. auch die Projekte FIDIS, PRIME und PrimeLife mit Beteiligung des ULD: https://www.datenschutzzentrum.de/projekte/idmanage/.

[188] Erste Umrisse eines solchen „AAL-Würfels Datenschutz" entstanden, noch ohne Ausdifferenzierung der Schutzziele-Dimension, in der Arbeitsgruppe „AAL-Architektur" anlässlich des AAL-Workshops am 26.07.2010 bei der TMF in Berlin mit den Teilnehmern Herrn Dr. Backmann, Herrn Gök, Herrn Norgall, Herrn Prof. Pommerening und Herrn Reich, denen unser Dank gilt. Die Erweiterung der Schutzziele-Dimension geschieht hier in Eigenverantwortung, um die spezielle Datenschutzperspektive in den Würfel operativ zugänglich zu integrieren.

flüsse und deren Schutzbedarfe für Akteursgruppen darstellbar zu machen. Dieses bildet die Grundlage für die Festlegung der technisch-organisatorischen Maßnahmen. In den dadurch entstehenden vielen Einzelwürfeln dieses „AAL-Gesamtwürfels Datenschutz“ sind dann die zu treffenden konkreten Maßnahmenbündel und Verantwortlichkeiten zu verorten.

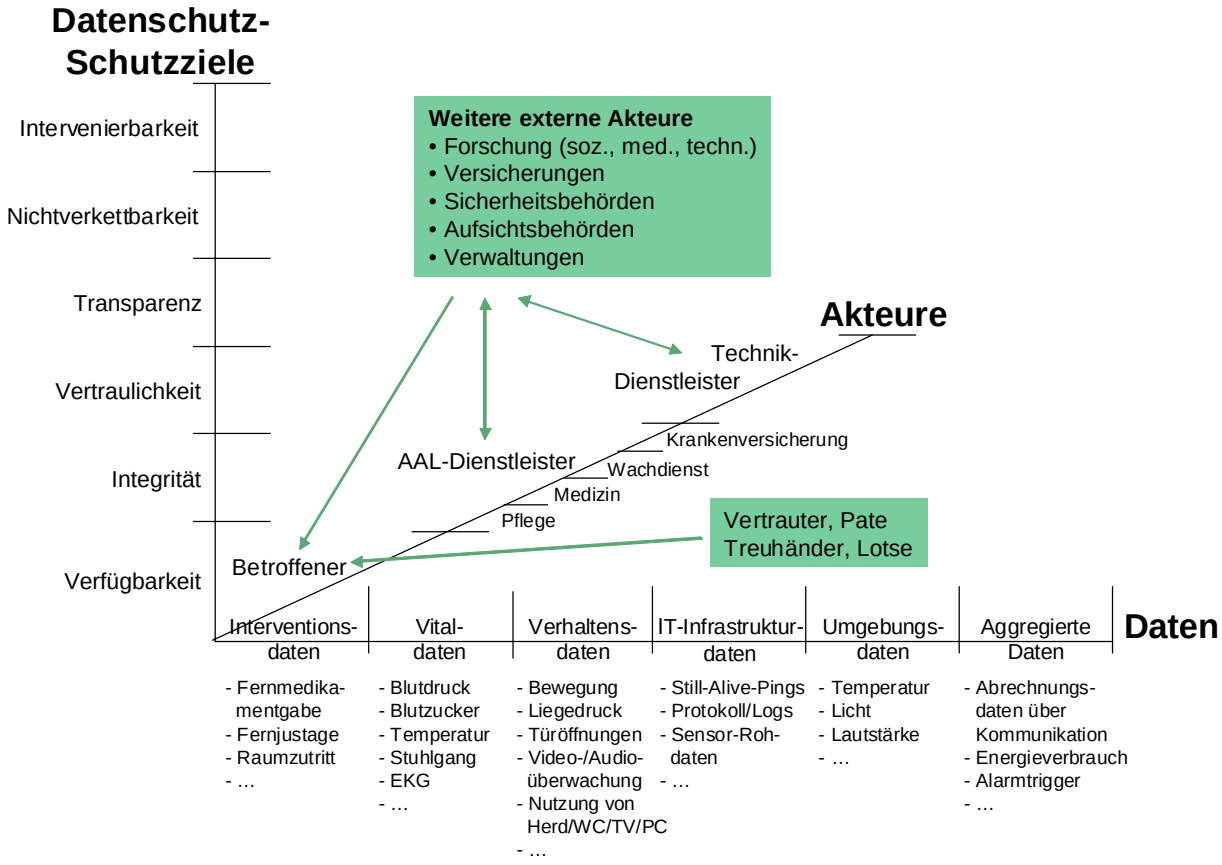


Abb. 8: Der „AAL-Würfel Datenschutz“: Daten, Akteure und Schutzziele in einer 3-dimensionalen Matrix

Im Folgenden werden zunächst die Akteure beschrieben, die jeweils Verantwortung für Teilbereiche im AAL-System haben (siehe Abschnitt 4.2.2.1). Anschließend wird erläutert, wie sich der jeweilige Schutzbedarf feststellen lässt (siehe Abschnitt 4.2.2.2), gefolgt von einer Kategorisierung der Daten, die im AAL-System eine Rolle spielen (siehe Abschnitt 4.2.2.3). Aufbauend auf diesen Ausführungen werden im folgenden Abschnitt 4.2.3 die Schutzziele genauer erörtert und auf AAL-Fragestellungen hin betrachtet.

4.2.2.1 Die Akteure

Aus der Sicht des Datenschutzrechts ist es für die Belange des AAL maßgeblich auszuweisen, welche Instanz zu welchem Zeitpunkt über die Erhebung, Verarbeitung und Auswertung der personenbezogenen Daten entscheidet, d.h. Verantwortlicher ist.[189]

Aus Datenschutzsicht – hier deckt sich dies mit der Datensicherheitssicht – bestehen dann die geringsten Probleme, wenn die AAL-Daten des Betroffenen grundsätzlich in den eigenen vier Wänden bleiben und dieser (oder ein persönlich von ihm eingesetzter Vertrauter) darüber entscheidet, welche Sensorik eingeschaltet ist und wie die Auswertung der Daten erfolgt, und selbst die Aktivitäten auslöst, indem er beispielsweise eine Alarmmeldung abgesetzt. Die Daten verbleiben dann ausschließlich im Zugriff des Betroffenen (oder des von ihm eingesetzten Vertrauten). Das Paradigma ist das des Einsatzes eines Beobachtungssystems zur Steigerung des Komforts im Sinne einer Heimautomation, deren Steuerung und deren Auswirkungen auf den Betroffenen vom Betroffenen selbst bestimmt werden.

Eine weitere typische Konstellation für AAL besteht darin, dass der Betroffene einen professionellen Hilfedienstleister beauftragt. Als typische Dienstleister kommen z.B. ein Wachdienst, ein Pflegedienst, der Hausarzt oder ein beispielsweise mit der Nachsorge befasstes Krankenhaus in Frage. Personen dieser Organisationen haben Zugriff auf entweder die Sensor-Rohdaten, oder sie erhalten bereits das Ergebnis einer Verarbeitung in Form eines ausgelösten (Vor-)Alarms und können daraufhin selbst differenzierte Aktionen auslösen. Diese Aktionen können beispielsweise aus telefonischen Rückrufen oder im Aufschalten einer anlassbezogenen Videoüberwachung beim Betroffenen bestehen. Die Daten, seien es die Rohdaten der Sensorik oder seien es vor Ort beim Betroffenen erstellte Auswertungsdaten, verlassen die vom Betroffenen kontrollierte Umgebung.

Denkbar sind des Weiteren Mischmodelle, wobei Eskalationsstufen eingerichtet sind, z.B. die Vorprüfung eines Alarms, der bei einem Vertrauten des Betroffenen eingeht, dann Ingangsetzen von Hilfemaßnahmen beim Pflegedienst oder einem Krankentransport. Umgekehrt kann auch eine Alarmmeldung bei einem professionellen Hilfedienstleister eintreffen, woraufhin dieser dann einen Vertrauten des Betroffenen darum bittet, Kontakt zum Betroffenen aufzunehmen, nachdem ein erster Anruf gescheitert ist (durch Aufsuchen oder Einschalten einer Videoüberwachung per Internet). Ein anderes Mischmodell sind Selbsthilfegruppen mit Mitgliedern, die beispielsweise über das Internet verbunden video- und mailgestützt „aufeinander aufpassen“.

Als dritte Akteursgruppe kommen reine Beobachter in Betracht, die die grundsätzlich anonymisierten Sensor-Rohdaten, die entweder von diesen selbst erfasst oder typischerweise von Hilfedienstleistern übermittelt werden, zu eigenen Zwecken weiterverarbeiten. Dazu ge-

[189] Zur datenschutzrechtlichen Verantwortlichkeit siehe Abschnitt 3.3.7.

hören z.B. Versicherungen und Forschungseinrichtungen, die diese Daten für ihre Zwecke verwenden möchten.

Es lassen sich für AAL-Infrastrukturen grob vereinfachend insofern fünf Akteursgruppen unterscheiden:[190]

- der Betroffene in seiner Umgebung,
- die assistierenden professionellen, vertraglich gebundenen Hilfedienstleister für den Betroffenen,
- die Dienstleister der Dienstleister (vor allem: IT-Bereich wie Rechenzentren, Fernwartung),
- die an Wissensgewinnung interessierten externen Beobachter (Forschung, Versicherungen, Aufsichts- und Strafverfolgungsbehörden) sowie
- verschiedene Beobachter (Selbsthilfe-Netzwerke, Freunde, Nachbarn, Vertraute, Vertreter).

4.2.2.2 Feststellung des Schutzbedarfs

Im Modell stehen hinter den Daten die technischen Systeme und Verfahren, mit denen die Daten erzeugt, verarbeitet und weitergegeben werden. Ist für Daten eines Akteurs ein durch die Schutzziele bestimmtes Schutzniveau gefordert, wird dieses Schutzniveau der Daten an die dahinterliegende technische Infrastruktur vererbt.

Betrachtet wird nachfolgend nur der Schutzbedarf der medizinisch relevanten Daten, weil diese den Regelfall für AAL-Systeme darstellen dürften und gem. § 3 Abs. 9 BDSG besonders schutzbedürftig sind. Da hier im Grunde eine Systematik und Methodik der Vorgehensweise dargelegt wird, um ein AAL-System datensicher und datenschutzgerecht planen, betreiben und prüfen zu können, lässt sich an dem Beispiel der medizinisch relevanten Beobachtungsdaten erschließen, welche Anforderungen aus Datenschutzsicht auch in den anderen Fällen zu erfüllen sind.

Zwischen den beteiligten Akteuren, d.h. dem Nutzer, den Dienstleistern und den Dienstleistern der Dienstleister sowie weiteren Organisationen fließen Daten. Die Erhebung und Verarbeitung von personenbezogenen Sensordaten geschieht in der Regel auf dedizierten Computern in den Räumen des Betroffenen; die Weitergabe von Daten geschieht in der Regel über Gateway-Rechner. Die Technik für Hilfeleistungen (Telemedizin, Aufschalten von Videoüberwachung nach Alarmierung, Fernschalten von Gerätschaften) oder bzgl. der Technik beim Betroffenen (Fernwartung, Updates, Installation neuer Systeme) oder bei anderen

[190] Damit werden die Beteiligtengruppen aus Abschnitt 2.3 zusammengefasst, die ähnliche Eigenschaften in Bezug auf diese Betrachtung haben.

Organisationen (Weiterleitung eines als gültig bewerteten Alarms an Rettungskräfte) geschieht auf Rechnern bei den Dienstleistern.

Das AAL-Gateway beim Betroffenen ist der geeignete Ort, um das nutzergesteuerte Identitätenmanagement des Betroffenen technisch an zentraler Stelle zu unterstützen. Am Gateway ist zentral zu entscheiden bzw. zu konfigurieren, welcher Dienstleister welche in den Räumen des Betroffenen erhobenen (Sensor-)Daten erhält. Dieses Gateway könnte vergleichbar einer Firewall agieren, über die das gesamte Kommunikationsmanagement, beispielsweise auch mit Forschungsinstituten, nutzergesteuert zugeschnitten abliefe und vom Nutzer überwacht und protokolliert werden könnte. Es muss sichergestellt sein, dass das Gateway ausschließlich im Sinne des Betroffenen betrieben wird, und zwar gerade dann, wenn der Betroffene in einem besonderen Maße auf die Hilfe der Hilfedienstleister angewiesen ist. Daher ist kritisch zu prüfen, ob und wenn ja, unter welchen Umständen, ein Zugriff auf dieses Gateway für andere wie z.B. Hilfedienstleister möglich sein soll.

Sowohl das Gateway als auch die gesamte sonstige Informationstechnik, die von der installierten Sensorik bis zu den möglicherweise komplexen Auswertungstools des Risikomanagements bei Versicherungen reicht, sollten den von den Schutzzielen formulierten Anforderungen genügen. Solange der Personenbezug der Daten bestehen bleibt, also die Sensordaten als Daten dieser Person vorliegen, erbt die Kette nachfolgender IT-Systeme diesen Schutzbedarf der Daten bzw. der Systeme bzw. der Prozesse und Verfahren.

Die Klassifikation des Schutzbedarfs von Daten lässt sich den Ausführungen zum IT-Grundschutz im „BSI-Standard 100-2“, dort: Textziffer 3.2.3, entnehmen: „Bestimmung des angemessenen Sicherheitsniveaus der Geschäftsprozesse“. Diese Ausführungen beziehen sich zwar speziell auf die Schutzziele der Datensicherheit, also Verfügbarkeit, Integrität und Vertraulichkeit, können aber methodisch verallgemeinert werden und sind somit auch auf die Schutzziele Transparenz, Intervenierbarkeit und Nichtverkettbarkeit anwendbar. Es folgt ein Ausschnitt aus Textziffer 3.2.3 des „BSI-Standards 100-2 IT-Grundschutz-Vorgehensweise“[191]:

„Zur besseren Verständlichkeit der Informationssicherheitsziele kann das angestrebte Sicherheitsniveau für einzelne, besonders hervorgehobene Geschäftsprozesse bzw. Bereiche der Institution in Bezug auf die Grundwerte der Informationssicherheit (Vertraulichkeit, Integrität, Verfügbarkeit) dargestellt werden. Dies ist für die spätere Formulierung der detaillierten Sicherheitskonzeption hilfreich.

Nachstehend sind einige beispielhafte Kriterien zur Bestimmung eines angemessenen Sicherheitsniveaus aufgeführt. Anhand derjenigen Aussagen, die am ehesten zutreffen, lässt

[191] BSI-Standard 100-2 IT-Grundschutz-Vorgehensweise, abrufbar unter: https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Publikationen/ITGrundschutzstandards/standard_1002.pdf.

sich das Sicherheitsniveau (normal, hoch oder sehr hoch) bestimmen. In dieser Phase des Sicherheitsprozesses geht es um die Formulierung der ersten richtungweisenden Aussagen, die in den späteren Phasen als Grundlage dienen und nicht um eine detaillierte Schutzbedarfsfeststellung.

Sehr hoch:

- Der Schutz vertraulicher Informationen muss unbedingt gewährleistet sein und in sicherheitskritischen Bereichen strengen Vertraulichkeitsanforderungen genügen.
- Die Informationen müssen im höchsten Maße korrekt sein.
- Die zentralen Aufgaben der Institution sind ohne IT-Einsatz nicht durchführbar. Knappe Reaktionszeiten für kritische Entscheidungen fordern ständige Präsenz der aktuellen Informationen, Ausfallzeiten sind nicht akzeptabel.
- Der Schutz personenbezogener Daten muss unbedingt gewährleistet sein. Anderenfalls kann es zu einer Gefahr für Leib und Leben oder für die persönliche Freiheit des Betroffenen kommen.

Weiterhin gilt: Der Ausfall der IT führt zum totalen Zusammenbruch der Institution oder hat schwerwiegende Folgen für breite gesellschaftliche oder wirtschaftliche Bereiche.

Hoch:

- Der Schutz vertraulicher Informationen muss hohen Anforderungen genügen und in sicherheitskritischen Bereichen stärker ausgeprägt sein.
- Die verarbeiteten Informationen müssen korrekt sein, auftretende Fehler müssen erkennbar und vermeidbar sein.
- In zentralen Bereichen der Institution laufen zeitkritische Vorgänge oder es werden dort Massenaufgaben wahrgenommen, die ohne IT-Einsatz nicht zu erledigen sind. Es können nur kurze Ausfallzeiten toleriert werden.
- Der Schutz personenbezogener Daten muss hohen Anforderungen genügen. Anderenfalls besteht die Gefahr, dass der Betroffene in seiner gesellschaftlichen Stellung oder in seinen wirtschaftlichen Verhältnissen erheblich beeinträchtigt wird.

Weiterhin gilt: Im Schadensfall tritt Handlungsunfähigkeit zentraler Bereiche der Institution ein; Schäden haben erhebliche Beeinträchtigungen der Institution selbst oder betroffener Dritter zur Folge.

Normal:

- Der Schutz von Informationen, die nur für den internen Gebrauch bestimmt sind, muss gewährleistet sein.

- Kleinere Fehler können toleriert werden. Fehler, die die Aufgabenerfüllung erheblich beeinträchtigen, müssen jedoch erkenn- oder vermeidbar sein.
- Längere Ausfallzeiten, die zu Terminüberschreitungen führen, sind nicht zu tolerieren.
- Der Schutz personenbezogener Daten muss gewährleistet sein. Anderenfalls besteht die Gefahr, dass der Betroffene in seiner gesellschaftlichen Stellung oder in seinen wirtschaftlichen Verhältnissen beeinträchtigt wird.

Weiterhin gilt: Schäden haben Beeinträchtigungen der Institution zur Folge.

Für die Formulierung der Informationssicherheitsziele ist die Mitwirkung der Leitungsebene unbedingt notwendig. Für diesen im Sicherheitsprozess grundlegenden Schritt kann auch die Einbeziehung eines externen Informationssicherheitsexperten sinnvoll sein. Zur Bestimmung des angestrebten Sicherheitsniveaus müssen die Ziele der Institution in Bezug auf ihre Sicherheitsanforderungen betrachtet werden, jedoch unter Berücksichtigung der Tatsache, dass in der Regel begrenzte Ressourcen für die Implementierung von Sicherheitsmaßnahmen zur Verfügung stehen. Aus diesem Grund ist es von besonderer Bedeutung, den tatsächlichen Bedarf an Verfügbarkeit, Integrität und Vertraulichkeit zu identifizieren, da ein hohes Sicherheitsniveau in der Regel auch mit hohem Implementierungsaufwand verbunden ist. Es ist außerdem empfehlenswert, die formulierten Anforderungen zu priorisieren, wenn dies zu diesem Zeitpunkt bereits möglich ist. Dies wird bei der Ressourcenplanung in späteren Phasen des Sicherheitsprozesses eine Entscheidungsgrundlage bilden.“

4.2.2.3 Datenarten in AAL-Systemen

Daten, die mit Personenbezug oder Personenbeziehbarkeit im Rahmen von AAL-Umgebungen ganz überwiegend automatisiert (aber vereinzelt auch manuell durch den Betroffenen oder durch den Vor-Ort-Pflegedienst) erhoben, ausgewertet, übertragen und archiviert werden und denen häufig zumindest eine Personenbeziehbarkeit zu attestieren ist, lassen sich wie folgt unterscheiden:

- **Interventionsdaten**, die einen Datenverarbeitungsprozess auslösen, der zwingend in einen Eingriff in die körperliche Unversehrtheit oder die Bewegungsfreiheit darstellt und **damit in ein Grundrecht des Betroffenen eingreift**
  (Schutzbedarf: sehr hoch)
  - Medizinische Daten, die einen unmittelbar Eingriff in den Körper des Betroffenen auslösen
    - Bsp.: Fernmedikation
  - Daten, die unmittelbare pflegerische Aktivitäten auslösen, **also unmittelbar auf den Betroffenen einwirken**
    - Bsp.: senkrechte Einrichtung der Bettposition

  - Daten, die unmittelbar einen Eingriff in die Bewegungsfreiheit des Betroffenen auslösen
    - Bsp.: externes Verschließen von Türen, externe Scharfschaltung von Alarm- bzw. Überwachungsgeräten

- **Vitaldaten**
  (Schutzbedarf in der Regel sehr hoch, insbesondere dann, wenn sie Voraussetzung für Interventionsdaten bilden (Vererbungsprinzip bei Schutzanforderungen))
  - Bsp.: Blutdruck, Körpertemperatur, Puls, Gewicht, …
- **Verhaltens- und Nutzungsdaten**
  (Schutzbedarf: in der Regel sehr hoch)
  - Verhaltens- oder Aktivitätsdaten des Betroffenen
    - Bsp.: Raumnutzung durch den Betroffenen erhoben durch Teppich- oder Schuhsensorik oder GPS-Armbanduhren
  - Nutzungsdaten elektronischer Geräte des Betroffenen
    - Bsp.: Daten über den Internetgebrauch, Telefongebrauch oder Elektrogerätegebrauch
- **IT-Infrastrukturdaten** der technischen Infrastruktur des AAL-Systems
  (Schutzbedarf: überwiegend normal, möglicherweise hoch, sofern auf Verfügbarkeit geprüft wird), im Kern sind dies Daten ohne direkten Personenbezug
  - Verfügbarkeit bzgl.
    - des Systems (der Sensoren, Komponenten bzw. PC, Gateway, Netzanschluss)
    - der Reaktionsbereitschaft der (Systeme der) Dienstleister
  - Integritäts-Checks (Hashwert-Vergleiche)
  - Zertifikate-Handling, etwa für VPN-Verbindungen
  - Protokollierung von Transaktionen (einschließlich der Zugriffe auf Protokollierungsdateien)
  - Monitoren und Verwalten von Fernwartungszugriffen
  - Konfigurationsdaten für die Systeme
  - Testdaten
  - Updates für Software
  - …
- **Umgebungsdaten**, d.h. Daten der Umgebung, in der sich der Betroffene aufhält
  (Schutzbedarf: normal)

- Bsp.: Temperatur, Licht, Lautstärke

- **Zusammengeführte Daten**
  (Schutzbedarf: normal (Abrechnung) bis sehr hoch (Alarmmeldung, medizinische Daten))
  - Bsp.: Zusammengeführte, u.U. medizinische Daten (Verknüpfung von Vital-, Interventions- und Verhaltensdaten), die aufgrund der Datenquelle ihren Personenbezug erhalten bzw. behalten
  - Bsp.: Zusammengeführte, u.U. medizinische Daten (Verknüpfung von Vital-, Interventions- und Verhaltensdaten), die zu einem umfassenden Bild des Personenzustands führen und aufgrund dessen eine Trigger- oder Alarmmeldung auslösen

Generell gilt bei der Ermittlung von Schutzbedarfen der Daten, dass immer die schutzbedürftigsten Daten diese Eigenschaft an die anderen betroffenen Systemteile vererben. Wird also an irgendeinem Punkt des Systems hoher oder sehr hoher Schutzbedarf festgestellt, vererbt sich diese Anforderung auf alle damit befassten oder nachfolgenden Systemteile.

4.2.3 Schutzziele

Der bereits oben skizzierte Schutzziel-Kanon enthält sowohl Datensicherheits- als auch Datenschutzanforderungen und koppelt die entsprechenden normativen Anforderungen an die korrespondierend zu treffenden technisch-organisatorischen Schutzmaßnahmen. Die Funktion des „AAL-Würfels Datenschutz“ (Daten, Akteure, Schutzziele) besteht darin, dass Akteure, die bestimmte Daten verarbeiten, die zur Erreichung von Schutzzielen zu treffenden Schutz-Maßnahmen verorten können. Welche konkrete Schutzmaßnahme zu wählen ist, hängt vom Schutzbedarf der Daten bzw. der Systeme ab. Dies wird nachfolgend erläutert.

Organisationen, die zu ihrer Datenverarbeitung eine IT-Infrastruktur betreiben, setzen Schutzziele anhand von Schutzmaßnahmen, die sich auf dem „aktuellen Stand der Technik“[192] befinden müssen, im Sinne von Best Practices um. Wesentlich ist auch, dass grundsätzlich jede technische und organisatorische Maßnahme fortgesetzt zu kontrollieren ist.[193] Insofern sind unter Schutzmaßnahmen immer *gesteuerte und regulierte Schutzmaßnahmen* zu verstehen, die sich nicht auf ein bloßes Vorhandensein bzw. die Installation einer Technik allein beschränken.

---

[192] Das Landesdatenschutzgesetz Schleswig-Holstein bestimmt in § 5 ausdrücklich, dass die von der Daten verarbeitenden Stelle zu treffenden technischen und organisatorischen Maßnahmen nach dem Stand der Technik (und der Schutzbedürftigkeit der Daten) angemessen sein müssen. Dies gilt auch im Anwendungsbereich des BDSG, obwohl dieser ausdrücklich nur in Bezug auf die Maßnahme „Verschlüsselung“ erwähnt wird.

[193] Aus dem Controlling der Betriebswirtschaft entstammt das Konzept der „Key Performance Indicators“.

Die drei klassischen Schutzziele der Datensicherheit – Verfügbarkeit, Integrität und Vertraulichkeit – fokussieren primär auf Anforderungen, die zur sicheren Aufrechterhaltung eines IT-Betriebs bzw. der Infrastruktur einer Organisation zu erfüllen sind. Die Schutzziele des Datenschutzes – Transparenz, Intervenierbarkeit und Nichtverkettbarkeit – fokussieren primär die Sicht von Betroffenen auf Anforderungen an die Datenverarbeitung einer Organisation. Für eine datenschutzgerechte Technikgestaltung ist nicht nur die Umsetzung der spezifischen Datenschutz-Schutzziele erforderlich, sondern auch die Umsetzung der Schutzziele der Datensicherheit, ausgerichtet auf die Perspektive betroffener Menschen (allgemein: Bürger, Kunden, Patienten, AAL-spezifisch: der Betroffenen, aber auch der Mitarbeiter bei den Hilfeorganisationen), deren Daten weitgehend automatisiert erhoben und verarbeitet werden. Datenschutz kann es ohne Datensicherheit nicht geben: Datenschutz setzt Datensicherheit voraus bzw. betrachtet die Datensicherheit als wesentlich zum Erreichen der Datenschutzziele.[194] Datenschutz weist gegenüber Datensicherheit ein zusätzliches Set an spezifischen Schutzzielen aus, in denen die Interessen der von der Datenverarbeitung Betroffenen in Bezug zur Organisation, deren Dienste sie beanspruchen, adressiert werden. Etwaige Konflikte zwischen Anforderungen der Datensicherheit und des Datenschutzes müssen gelöst werden.

Die Schutzziele, die von den Akteuren zu beachten sind, und der festzulegende Schutzbedarf gelten im Hinblick auf die Verarbeitung der personenbezogenen *Daten*. Die *Systeme*, mit denen diese personenbezogenen Daten erhoben bzw. verarbeitet werden, und die *Prozesse*, mit denen diese Systeme technisch und organisatorisch am Laufen gehalten werden, erben diesen für die Daten ermittelten Schutzbedarf.[195] Insofern ist es aus Datenschutzsicht zu rechtfertigen, eine Schutzzielanalyse für AAL-Systeme auf die technisch erhobenen personenbezogenen bzw. personenbeziehbaren Daten zu konzentrieren und entsprechende Schutzmaßnahmen zu formulieren. Allerdings muss wiederum, um die erzeugten und genutzten Daten transparent zu machen, das gesamte System einschließlich der Komponenten transparent gemacht werden. So muss transparent sein, welche Daten erhoben werden, wie das System diese Daten erzeugt und welche Prozesse dafür sorgen, dass das System verfügbar ist, integer funktioniert, vertrauliche Datenverarbeitung zulässt, es prüfbar ist, es unter Kontrolle ist und keine nicht-zweckgebundenen Daten abfließen oder einfließen. Die Schutzziele müssen u.a. bezogen werden auf

- die einzelnen **Komponenten** und das aus diesen Komponenten zusammengesetzte AAL-Gesamtsystem,
- die **Prozesse**, in die die Funktionen der Systeme und die Daten eingespannt sind,

[194] Meints, in: DuD 2006, S. 13 ff.

[195] Auch Infrastrukturen wie Netze oder Räume sowie die mit der Datenverarbeitung befassten Personen erben den Schutzbedarf der von ihnen verarbeiteten Daten.

- die **Daten**, die fortlaufend vom System erzeugt werden,
- den **Kontext**, z.B.:
  - Anforderungen, die erfüllt sein müssen, damit ein AAL-System in einer Wohnung installiert werden kann oder
  - vertragliche Gegebenheiten (ggf. muss z.B. der Vermieter zustimmen).

Der Vollständigkeit halber sei an dieser Stelle erwähnt, dass weitere Maßnahmen, die die Komponenten und Prozesse auf der Systemebene betreffen,[196] in einer zusätzlichen Ebene für eine vollständige Darstellung vorzunehmen sind. Dies kann wegen der Spezialität der AAL-Komponenten und der Hardware und Software von IT-Systemen an dieser Stelle nicht vorgenommen werden.

Zwischen diesen verschiedenen o.g. Bereichen bestehen Abhängigkeiten. So lassen sich Verfügbarkeit und Integrität einer technischen Komponente eines AAL-Systems bzw. des AAL-Systems insgesamt durch Prozesse auf der Ebene der Organisation des Gesamtsystems anhand von Funktionsdaten der Systeme feststellen. Umgekehrt lässt sich anhand mehrerer verfügbarer und integrer Funktionsdaten technisch automatisiert auf die ausreichend sichere Verfügbarkeit des Gesamtsystems schließen, wobei die Anforderung besteht, dass die zum Controlling des Gesamtsystems vorgesehene Informationstechnik ihrerseits wiederum sicher verfügbar sein muss.

Sofern ein standardisiertes Kommunikationsprotokoll für die verschiedenen Komponenten eines AAL-Systems zur Verfügung stünde oder zumindest für eine Interoperabilität zwischen verschiedenen Systemen gesorgt wäre, indem beispielsweise ein gemeinsamer Datenbus für standardisierte Datenanlieferungen verwendet würde, könnte von der Komplexität der Einzelsysteme abstrahiert werden, um auf Eigenschaften des Gesamtsystems zu schließen und das Controlling vorzunehmen. Ein etabliertes AAL-Protokoll gestattete einen Großteil zumindest des Controllings der Schutzmaßnahmen der einzelnen Komponenten und Prozesse.[197] Man kann aus dieser Sicht auch vermuten: Ohne ein standardisiertes AAL-Protokoll bzw. Interoperabilitäts-Mechanismen für ein AAL-System bzw. einen standardisierten AAL-Bus, mit dem sich zumindest alle Komponenten innerhalb der Umgebung des Betroffenen integrieren ließen und der besser noch auch die AAL-Komponenten auf Seiten des Dienstleisters umfassen sollte, ist ein sicheres Funktionieren nach Maßgabe der Schutzziele praktisch nicht zu garantieren.

---

[196] Dazu zählten beispielsweise Integritäts-Checks von CPUs, RAMs oder Festplatten.

[197] Vgl. Eichelberg, Die Bedeutung von Interoperabilität für AAL (Stand 30.07.2010). Der Vortrag ist abrufbar unter: http://www.ebn.din.de/sixcms_upload/media/2929/4_Eichelberg_Interoperabilitaet_AAL.pdf); Wichert, Configuration and Dynamic Adaptation of AAL Environments to Personal Requirements and Medical Conditions; (Stand: 30.07.2010), abrufbar unter: http://www.aal.fraunhofer.de/publications/Configuration-and-adaptation-of-AAL-Environments.pdf

Um die Datensicherheit von Systemen zu gewährleisten, empfiehlt sich die Einrichtung eines Informationssicherheitsmanagements gemäß der Vorgehensweise nach IT-Grundschutz. Die wesentlichen Schritte, um zu einem gesicherten Betrieb von IT-Systemen zu gelangen, umfassen eine Strukturanalyse, eine Schutzbedarfsfeststellung, eine Modellierung des gesamten (Verbund-)Systems, einen Basissicherheitscheck (eventuell sind auch weitere Sicherheitsmaßnahmen zu treffen) und eine Sicherheitsrevision.[198] Inhaltlich orientiert sich die Herstellung und Überprüfung der Datensicherheitsanforderungen an den Schutzzielen Verfügbarkeit, Integrität und Vertraulichkeit. Zu diesen Schutzzielen wurden die IT-Grundschutz-Kataloge entwickelt, die insbesondere von den folgenden Komponenten geprägt sind:

Bausteine:

- B 1: Übergreifende Aspekte der Informationssicherheit
- B 2: Sicherheit der Infrastruktur
- B 3: Sicherheit der IT-Systeme
- B 4: Sicherheit im Netz
- B 5: Sicherheit in Anwendungen

Gefährdungskataloge:

- G 1: Höhere Gewalt
- G 2: Organisatorische Mängel
- G 3: Menschliche Fehlhandlungen
- G 4: Technisches Versagen
- G 5: Vorsätzliche Handlungen

Maßnahmenkataloge:

- M 1: Infrastruktur
- M 2: Organisation
- M 3: Personal
- M 4: Hard- und Software
- M 5: Kommunikation
- M 6: Notfallvorsorge

[198] Vgl. https://www.bsi.bund.de/cln_156/ContentBSI/grundschutz/kataloge/allgemein/einstieg/01001.html#1_3.

Zur Illustration der Anwendung in der Praxis sei ein Beispiel gegeben: In den Gefährdungskatalogen wird unter G4.1 ein Ausfall der Stromversorgung thematisiert. Dort wird also ein Risiko für das Schutzziel Verfügbarkeit von IT-Systemen formuliert. In den Maßnahmenkatalogen dazu werden unter M1.25 zu treffende Maßnahmen bzgl. Überspannungsschutzes geschildert, während sich unter M1.28, M1.70 Details bzgl. unterbrechungsfreier Stromversorgung finden. In den Katalogen ist die Darstellung der allgemeinen Gefährdungen und der Maßnahmen zum Erfüllen der drei nachfolgend näher beschriebenen Schutzziele Verfügbarkeit, Integrität und Vertraulichkeiten von IT-Systemen enthalten. Diese Kataloge sind nicht auf AAL-Systeme hin ausgelegt. Die Hersteller und Verantwortlichen für den Betrieb von AAL-Systemen sind deshalb aufgefordert, diese Kataloge der Datensicherheit auf ihre Systeme hin zu spezifizieren. Für diese Vorstudie konzentrieren wir uns bezüglich zu treffender Maßnahmen auf die spezifischen Datenschutz-Schutzziele Transparenz, Intervenierbarkeit und Nichtverkettbarkeit, weil die IT-Grundschutz-Kataloge aufgrund ihrer Ausrichtung auf Datensicherheit diese Schutzziele nur unzureichend bedienen. Alle sechs Schutzziele werden im Folgenden in ihrer Bedeutung kurz erläutert, und es werden zugehörige Schutzmaßnahmen exemplarisch aufgezeigt.

4.2.3.1 Verfügbarkeit

4.2.3.1.1 Beschreibung

Als Verfügbarkeit wird die Möglichkeit eines gesicherten Zugriff auf Informationen (oder ein System oder ein Verfahren, das Daten bzw. Informationen erzeugt) innerhalb festgelegter Zeit bezeichnet. Hiernach sollen Informationen (oder ein System oder ein Verfahren) zeitgerecht zur Verfügung stehen und ordnungsgemäß verwendet werden können.[199] Aus normativer Sicht bedeutet dies, dass technisch-organisatorische Maßnahmen zu treffen sind, die geeignet sind zu gewährleisten, dass personenbezogene Verfahren und Daten zeitgerecht zur Verfügung stehen und diese ordnungsgemäß angewendet werden können. Aus Sicht des Betroffenen soll die AAL-Dienstleistung verfügbar sein, was wiederum voraussetzt, dass die AAL-Daten für den Dienstleister verfügbar sind.

4.2.3.1.2 Schutzmaßnahmen

Die einzelnen Gefährdungen und Schutzmaßnahmen zum Erreichen dieses Ziels „Sicherung der Verfügbarkeit“ von IT-Systemen sind den IT-Grundschutz-Katalogen entnehmbar. Die jeweils AAL-System-relevanten Aspekte sind dann für den einzelnen Anwendungsfall herausfiltern.

[199] Vgl. § 9 Abs. 2 Nr. 3 Sächsisches Datenschutzgesetz (SächsDSG), wonach Verfügbarkeit bedeutet, dass „personenbezogene Daten zeitgerecht zur Verfügung stehen und ordnungsgemäß verarbeitet werden können“

Verfügbarkeit bedeutet im Fall von AAL: Je lebenswichtiger eine Funktion für einen Menschen ist, desto unwahrscheinlicher muss der Ausfall der Funktion bzw. des Systems sein. Dieses Schutzziel zu erreichen, werden alle beteiligten Organisationen bereits aus haftungsrechtlichen Gründen anstreben. Das aus Datenschutzsicht besonders Herauszuhebende ist: Die informationelle (und operationelle) Selbstbestimmung wird erst durch das AAL-System ermöglicht und wahrnehmbar. Um die Verfügbarkeit sicherzustellen, muss der Ausfall eines Systems bzw. einer Systemkomponente hinreichend schnell erkannt, analysiert (als Störung, Problem, Veränderungsbedürftigkeit) und, typischerweise durch eine andere Komponente, die als redundante Ausfallsicherheit vorgesehen ist, ersetzt werden. Auf Seiten der Dienstleister kommen zudem organisatorische Vorkehrungen, etwa im Rahmen von Vertretungsregeln, sowie die Fernwartbarkeit von Systemen durch spezialisierte Servicetechniker dazu. Die verschiedenen im Detail zu installierenden Sicherungsmechanismen und Organisationsregeln findet man, wie oben angegeben, in den IT-Grundschutz-Katalogen. Die Anforderungen an die Verfügbarkeit von verschiedenen Sensoren und Aktoren und deren Datenverarbeitung vor Ort sind andere als Anforderungen, die an die Informationstechnik auf Seiten der verschiedenen Infrastruktur- und AAL-Dienstleister oder etwa an einen Rechenzentrumsbetrieb im Auftrag eines AAL-Dienstleisters zu stellen sind.

Betroffene müssen sich auf die Verfügbarkeit der Funktionen des AAL-Systems verlassen können. Es ist im Alltag häufig unmittelbar erkennbar, ob die Verfügbarkeit einer Funktion gegeben ist oder nicht. Im Rahmen von AAL wird für den Betroffenen jedoch oft nicht erkennbar sein, ob die Sensoren, die Datenverarbeitung und die Aktoren, nach Auslösung eines Triggers, funktionieren bzw. funktionieren werden und dass diese Trigger beispielsweise bei einem Dienstleister auch die richtige Hilfeaktion auslösen. Es muss deshalb für die Erkennbarkeit der Verfügbarkeit von Sensorik, Datenverarbeitung und Aktoren sowie letztlich der dadurch tatsächlich in Gang gesetzten Hilfefunktionalität gesorgt werden, ohne den jeweiligen Nutzern zu viel Komplexität zuzumuten. Die Erkennbarkeit der Verfügbarkeit muss auf jeden Fall auf Seiten der Dienstleister gegeben sein, und es ist sicher auch sinnvoll, dass der Betroffene selbst sich Gewissheit über das Funktionieren seines Assistenz-Systems oder dessen Komponenten verschaffen kann.

4.2.3.2 Integrität

4.2.3.2.1 Beschreibung

Integrität verlangt, dass ein System ausschließlich seine zweckbestimmte Funktion, diese aber verlässlich und erwartungsgemäß erfüllt; etwaige Nebenwirkungen müssen ausgeschlossen oder berücksichtigt sein. Personenbezogene Daten müssen während der Verar-

beitung unversehrt, vollständig und aktuell bleiben.[200] Aus normativer Sicht bedeutet dies, dass technisch-organisatorische Maßnahmen zu treffen sind, die geeignet sind zu gewährleisten, dass Daten aus personenbezogenen Verfahren unversehrt, zurechenbar und vollständig bleiben. Aus der Sicht des Betroffenen soll die AAL-Dienstleistung verlässlich, sicher, korrekt, unverfälscht und zutreffend zurechenbar zur Verfügung stehen, was wiederum bedeutet, dass die Daten (und damit die Systeme und Prozesse), die den AAL-Dienstleister erreichen, diese Anforderungen ebenfalls erfüllen müssen.

4.2.3.2.2 Schutzmaßnahmen

Die einzelnen Gefährdungen und Schutzmaßnahmen zum Erreichen dieses Ziels „Sicherung der Integrität“ sind den IT-Grundschutz-Katalogen entnehmbar. Die jeweils AAL-Systemrelevanten Aspekte sind dann für den einzelnen Anwendungsfall herausfiltern.

Integrität thematisiert den Aspekt, dass die erzeugten Daten auf Seiten des Nutzers unverfälscht bei den betreuenden Dienstleistern ankommen und dass diese Daten wiederum bei den Dienstleistern korrekte Aktivitäten auslösen. Sehr wichtig ist der Aspekt, dass keine Fehlalarme ausgelöst werden, möglicherweise sogar vom Nutzer vorsätzlich, weil dann die Aufmerksamkeit der Dienstleister verloren geht, von den unnötigen Kosten ganz zu schweigen.[201] Zur Sicherstellung der Integrität und der Verfügbarkeit etwa von Alarmmeldungen ist die Durchführung von Tests unerlässlich.

Die wesentliche Schutzmaßnahme besteht in der Organisation des Controllings von Systemen und Prozessen. Es muss beständig kontrolliert werden, ob sich der aktuell festgestellte Ist-Zustand innerhalb der vorgegebenen Sollgrenzen befindet und ob die Feststellung des Ist-Zustands korrekt zustande gekommen ist. Technisch setzt man Integritäts-Checks dadurch um, dass man Informationen anhand von Vorher-nachher-Hashwert-Vergleichen auf ihre Unversehrtheit hin testet. Die Integrität ist durch Tests der einzelnen Komponenten durch Tests für einzelne Komponenten (Sensorik, Datenverarbeitung, Reaktionen auf Seiten Beobachter und Bewerter) in dem Gesamtsystem und dann für das Gesamtsystem sicherzustellen, indem beispielsweise Penetrationstests durchgeführt werden, die darauf abzielen, Fehlfunktionalitäten zu erzeugen, um sich vom Grad der Robustheit der Korrekturmaßnahmen zu überzeugen.

---

[200] Vgl. § 9 Abs. 2 Nr. 2 SächsDSG.

[201] Clausen / Dombrowsky, in: Zeitschrift für Soziologie, 1984, S. 293 ff.

4.2.3.3 Vertraulichkeit

4.2.3.3.1 Beschreibung

Vertraulichkeit verlangt, dass nicht zuständige, unbeteiligte Dritte keine Möglichkeit erhalten, von Daten unbefugt Kenntnis zu bekommen oder das System einzusehen und den Betroffenen identifizieren zu können. Dies erfordert es, dass die AAL-Teilsysteme hinreichend von den unterschiedlichen Dienstleistern abgeschottet sein müssen, d.h., jeder Dienstleister darf nur auf die Daten (und Systeme und Programme) Zugriff erhalten, die er zur zweckgemäßen Erfüllung seiner spezifischen Aufgabe benötigt.[202] Aus normativer Sicht bedeutet dies, dass technisch-organisatorische Maßnahmen zu treffen sind, die geeignet sind zu gewährleisten, dass nur befugt auf personenbezogene Verfahren und Daten zugegriffen werden kann.

4.2.3.3.2 Schutzmaßnahmen

Die einzelnen Gefährdungen und Schutzmaßnahmen zum Erreichen des Ziels „Sicherung der Vertraulichkeit“ sind den IT-Grundschutz-Katalogen entnehmbar. Die jeweils AAL-System-relevanten Aspekte sind dann für den einzelnen Anwendungsfall herausfiltern.

Die wesentliche Schutzmaßnahme besteht darin, Daten und Systeme so voneinander zu separieren, dass kein unbefugter Zugriff möglich ist und dort, wo einem möglichen Zugriff zu geringe Hürden entgegenstehen, Daten zu verschlüsseln. Auf organisatorischer Ebene sind Funktions- bzw. Rollentrennungen vorzunehmen. Bei einer zweckgeänderten, aber begründeten Weitergabe von anonymisierten oder pseudonymisierten AAL-Daten, typisch etwa für wissenschaftliche Forschungszwecke, ist für dieses Schutzziel darauf zu achten, dass für die empfangende Stelle keine Rückschlüsse aus den ehemals personenbezogenen Daten auf die Person möglich sind.

Allein die Information über den Umstand, dass in einem Haushalt AAL-Komponenten installiert und genutzt werden, ist bereits schutzwürdig.

4.2.3.4 Transparenz

4.2.3.4.1 Beschreibung

Zur Transparenz gehört, dass für Betroffene und Betreiber von Systemen jederzeit klar sein muss, welche Dienstleistungen erbracht werden, welche Sensoren und Aktoren wo installiert sind und wie tätig werden, welche Daten erhoben werden, wem diese gehören, wohin sie fließen, wie sie verarbeitet und von wem zu welchem Zweck ausgewertet werden und wann sie durch wen in welcher Form gelöscht werden. Insgesamt ist also Transparenz für den ge-

[202] Vgl. auch § 9 Abs. 2 Nr. 1 SächsDSG.

samten Lebenszyklus der Daten von ihrer Entstehung bis ihrer Löschung erforderlich. Transparenz der Datenverarbeitung ist Voraussetzung dafür, dass Betroffene oder deren vertraute Stellvertreter in die Verarbeitung der Daten einwilligen oder dieser widersprechen können. Transparenz müssen die Dienstleister gegenüber den von ihnen Betreuten gewähren in Bezug darauf, welche Daten in welcher Form von ihnen verarbeitet werden und ob Daten an Dritte weitergereicht werden. Insbesondere müssen die Betroffenen wissen, welche Aktionen sie auslösen können, die für sie von Bedeutung sind.[203]

Aus normativer Sicht bedeutet dies, dass, werden personenbezogene Verfahren betrieben, Maßnahmen zu treffen sind, die je nach Art der zu schützenden Daten gewährleisten, dass die Verfahren zur Erhebung, Verarbeitung und Nutzung mit zumutbarem Aufwand nachvollzogen, überprüft und bewertet werden können.

4.2.3.4.2 Schutzmaßnahmen

Das Maßnahmenbündel zur Sicherstellung der Herstellbarkeit von Transparenz betrifft im Wesentlichen die Prüffähigkeit der Prozesse und Daten in Organisationen. Organisationen müssen deshalb verfügen über:

- ein methodisches Projektmanagement, einschließlich stufenweiser Tests und Freigaben;
- eine Dokumentation ihrer IT-Infrastruktur, der Daten und der Datenflüsse, der Schnittstellen nach außen und der genutzten Datenformate, der Sicherheitsmaßnahmen und der Tests und Freigaben ihrer Systeme. Die Dokumentation muss für sachkundige Personen in angemessener Zeit nachvollziehbar sein. Sie ist nach jeder Änderung des Systems fortzuschreiben und mindestens fünf Jahre nach der letzten automatisierten Verarbeitung personenbezogener Daten aufzubewahren. Das bedeutet im Einzelnen zunächst die Dokumentation der eingesetzten Informationstechnik und die daran anschließende Dokumentation der Sicherheitsmaßnahmen, sowohl für das gesamte AAL-System als auch für die einzelnen Komponenten:[204]
    - Die **IT-Dokumentation** sollte mindestens beschreiben:
        - den Einsatzzweck sowie die Maßnahmen zur Datenvermeidung und Datensparsamkeit,
        - die für den Einsatzzweck verwendeten informationstechnischen Geräte einschließlich des Standorts,

[203] Vgl. auch § 9 Abs. 2 Nr. 1 SächsDSG.

[204] Die nachfolgende Auflistung entstammt weitgehend der Datenschutzverordnung des Landes Schleswig-Holstein, Stand: 01.01.2009. Diese Dokumentationsanforderungen sind abgeglichen mit den Anforderungen nach IT-Grundschutz.

- die für den Einsatzzweck verwendeten Programme und die zur Inbetriebnahme getätigten Schritte,
- bei vernetzten informationstechnischen Geräten die physikalischen und logischen Verbindungen zu anderen informationstechnischen Geräten (Netzplan),
- die technischen und organisatorischen Vorgaben für die Datenverarbeitung einschließlich der Darstellung, welche Personen für welche Aspekte der Datenverarbeitung verantwortlich und berechtigt sind,
- die Änderungen an informationstechnischen Geräten, Programmen oder Verfahren einschließlich der Personen, die die Veränderungen vorgenommen haben,
- die vorgesehenen und durchgeführten Datenübermittlungen einschließlich der Empfängerinnen und Empfänger der Daten,
- bei Vorliegen einer Datenverarbeitung im Auftrag die hierfür nötigen schriftlichen Vereinbarungen,
- die Maßnahmen zum Erfüllen von Auskunftsansprüchen von Betroffenen,
- die Maßnahmen für die Berichtigung, die Löschung und die Sperrung personenbezogener Daten.

o Die **Sicherheitsdokumentation** sollte die technischen und organisatorischen Maßnahmen sowie die Analyse möglicher Gefährdungen behandeln in Bezug auf:

- Personal,
- Räume und Gebäude,
- informationstechnische Geräte und Programme und
- die interne und externe Vernetzung der informationstechnischen Geräte.

Werden Daten verschlüsselt oder erfolgt eine elektronische Signierung, so müssen die technischen und organisatorischen Maßnahmen zur Vergabe und zum Entzug von Schlüsseln sowie zur Schlüsselhinterlegung dokumentiert werden.

Grundsätzlich sind sämtliche relevanten, im Vorfeld festzulegenden Aktivitäten, nicht nur die mit einem unmittelbar ersichtlich hohen Risiko für die Betroffenen, zu protokollieren. Die einzelnen Überwachungssysteme sowie das Gesamtsystem sind zu dokumentieren, indem Konzepte, Monitoringsysteme und Protokollierungsdaten beschrieben werden. Aus den Protokollierungsdaten muss jeweils hervorgehen, welche Entität (System, Person, Organisationseinheit) welche Operationen zu welchem Zeitpunkt ausführen soll, gerade ausführt oder ausgeführt hat. Dies gilt insbesondere auch im Zusammenspiel mit externen Systemen. Es ist dabei ferner zu dokumentieren, welche technischen und organisatorischen Maßnahmen hinsichtlich des

Zugriffs, der Auswertung und der Löschung der Protokollierungsdaten getroffen wurden.

Zu dokumentieren ist ferner, welche technischen und organisatorischen Maßnahmen getroffen wurden, um ein Datenschutzmanagementsystem zu ermöglichen.

Liegt eine Verarbeitung personenbezogener Daten im Auftrag vor, so sind die beim Auftragnehmer getroffenen technischen und organisatorischen Maßnahmen, die der Umsetzung der sechs Schutzziele dienen, von der Daten verarbeitenden Stelle zu dokumentieren.

- Dokumentation von Tests und Freigaben

  Die eingesetzten informationstechnischen Geräte und Programme sowie die in der Dokumentation festgelegten Sicherheitsmaßnahmen sind vor der Aufnahme der Verarbeitung personenbezogener Daten zu testen. Die vorgenommenen Tests und die dabei erzielten Ergebnisse sind zu dokumentieren. Festgestellte Mängel sind nach ihrer Bedeutung zu gewichten.

  Die Freigabe einer Komponente oder des gesamten Systems hat schriftlich zu erfolgen. Sie ist nur zulässig, soweit bei den Tests keine wesentlichen Mängel festgestellt wurden. Die Beseitigung geringfügiger Mängel muss in angemessener Zeit vorgenommen werden.

  Test und Freigabe können in einem gestuften Verfahren erfolgen. In jeder Stufe können der Test und die Freigabe auf die geplante Verarbeitung personenbezogener Daten begrenzt werden.

Die Praxis muss den Grundsätzen ordnungsgemäßer Buchführung genügen. Hierbei gilt, dass die Dokumentation eines Verfahrens zum notwendigen Bestandteil eines Verfahrens zählt und keine Option darstellt.

4.2.3.5 Intervenierbarkeit

4.2.3.5.1 Beschreibung

Der Betroffene muss im Grundsatz souverän jederzeitig und überall darüber bestimmen können, was in welchem Maße wann und wie an ihm beobachtbar ist bzw. beobachtet wird und welche Auswirkungen diese Beobachtungen auf ihn haben können. Schon bei der Konstruktion des ihn beobachtenden Systems muss im Sinne einer Intervenierbarkeit vorgesehen werden, dass ein Betroffener die Erhebung und Kontrolle seiner Daten (zumindest vorübergehend) beeinflussen und abschalten kann. Grundsätzlich muss der Betroffene darüber entscheiden, ob das ihn beobachtende System an- oder abgeschaltet ist. Wenn er sich das nicht zutraut, müssen vertrauenswürdige Delegationsmodelle greifen. Die Betreiber der Systeme müssen nachweisen, dass sie ihre Systeme im Griff haben, d.h. jeden Prozess in einem kontrollierten Betrieb fahren, der jederzeit auch abgeschaltet werden kann.

Aus normativer Sicht bedeutet dies für personenbezogene Verfahren: Es sind Maßnahmen zu treffen, die gewährleisten, dass die Verfahren dem Betroffenen die Ausübung der ihm zustehenden Rechte wirksam ermöglichen.

4.2.3.5.2 Schutzmaßnahmen

Das Schutzziel Intervenierbarkeit erfordert einen operativen Zugriff auf Verfahren und Daten und bedeutet im Einzelnen, dass Organisationen verfügen müssen über

- einen SPOC (Single-Point-of-Contact) für Betroffene, zur Adressierung einer Intervention mit Verfolgbarkeitsoption,
- eine Steuerung regulierter Prozesse des Erhebens, Nutzens, Weitergebens und Löschens von personenbezogenen Daten, mit Prüfungstechniken jeweils auf dem aktuellen Stand, und
- geeignet gestaltete Einwilligungsverfahren, insbesondere feingranular statt pauschal sowie beschränkt in Zeit und Umfang auf das erforderliche Maß.

Vorhandene Daten müssen im Grundsatz vom Betroffenen oder auch von einem von ihm beauftragten Stellvertreter einsehbar, korrigierbar, sperrbar und löschbar sein.

Wichtig ist auch die Möglichkeit für einen Betroffenen, das AAL-System oder Teile davon, z.B. Beobachtungskomponenten, für eine gewisse Zeit abstellen zu können, um unbeobachtet zu sein. Der Betroffene muss wissen, welches Risiko er mit dem Abschalten in Kauf nimmt, da dann u.U. eine schnelle Hilfeleistung im Notfall nicht möglich ist.

4.2.3.6 Nichtverkettbarkeit

4.2.3.6.1 Beschreibung

Nichtverkettbarkeit bedeutet die Unmöglichkeit der Verkettung von Daten und Entitäten untereinander und miteinander.[205] Dazu gehört insbesondere das Sicherstellen, dass Daten nur für den Zweck verarbeitet und ausgewertet werden, für den sie erhoben wurden. Dies bedeutet, dass Daten nicht ohne Zweckbestimmung erhoben und entgegen diesem Zweck verarbeitet werden dürfen (z.B. für Werbezwecke oder im Falle von AAL naheliegender: für empirische Sozialforschung oder für medizinische oder versicherungsmathematische Forschung oder Technikforschung seitens der AAL-Komponentenhersteller). Es ist zu bedenken, dass große Datenbestände Begehrlichkeiten wecken können. Aus normativer Sicht bedeutet dies: Werden personenbezogene Verfahren betrieben, sind Maßnahmen zu treffen, dass deren

[205] Rost / Pfitzmann, in: DuD 2009, S. 353 ff.

Daten nicht oder nur mit unverhältnismäßig hohem Aufwand für einen anderen als den ausgewiesenen Zweck erhoben, verarbeitet und genutzt werden können.

4.2.3.6.2 Schutzmaßnahmen

Das Maßnahmenbündel zur Umsetzung dieses Zieles sieht insbesondere für Organisationen vor, dass sie verfügen müssen beispielsweise über

- angemessene Funktions- und Rollentrennungen zwischen und innerhalb von Organisationen mit Verantwortungszuweisungen an kompetente Belegschaftsangehörige, die sich in der technischen Infrastruktur wiederfindet wie beispielsweise als Mandantenfähigkeit von Datenbanken bzw. als „Isolated Service Containers“,
- Konzepte, Implementierungen, Konfigurationen, Regelungen für die Inbetriebnahme und Außerbetriebnahme von Programmen, Tests und Simulationen in den jeweiligen Phasen – nach Best-Practice-Gesichtspunkten,
- Techniken, die lose Kopplungen ermöglichen und eng zugeschnittene Dienste bieten (Metadirectory, Federation-Services, Service-orientierte Architekturen etc.),
- Ein nutzergesteuertes Identitätsmanagement, das über das Vermeiden von zweckübergreifend eingesetzten Kennungen und eine technisch gestützte Pseudonymnutzung eine Steuerung[206] gewünschter Verkettungen und Entkettungen bewirkt und unerwünschte Verkettungsmöglichkeiten vermeidet (hier besonders wirkungsvoll die sogenannten „anonymen Credentials“[207]),
- eine fallbezogene Einrichtung und Separierbarkeit von Subprozessen, damit sich partielle Interventionen durch Betroffene oder andere „Systemstörungen“ nicht über die Grenzen des Systems hinaus auswirken,
- Prozesse zum Löschen von Daten und Prozessen, sobald sie nicht mehr für den jeweiligen Zweck erforderlich sind,
- gehärtete Computersysteme, die möglichst keine Nebenfunktionen bieten, oder der Einsatz virtueller Server.

[206] Beim nutzergesteuerten Identitätsmanagement liegt der Schwerpunkt auf der Nutzersteuerung einer etwaigen Verkettung oder Verkettbarkeit statt auf unbedingter Nichtverkettbarkeit, vgl. Hansen, Linkage Control – Integrating the Essence of Privacy Protection into Identity Management Systems, in: Proceedings of eChallenges 2008, S. 1585-1592.

[207] Camenisch / Lysyanskaya, Efficient Non-transferable Anonymous Multi-show Credential System with Optional Anonymity Revocation, in: Advances in Cryptology – Eurocrypt 2001, S. 93-118.

4.2.3.7 Verhältnis der Schutzziele untereinander

Die Schutzziele lassen sich in eine systematisch kontrollierbare Beziehung zueinander bringen, wenn man zunächst von den Schutzzielen der Datensicherheit ausgeht. In bestimmten Konstellationen ergänzen sich beispielsweise Verfügbarkeit und Vertraulichkeit, in anderen schließen sie einander aus: Eine Information ist dann nicht mehr vertraulich gegenüber einer Entität, sobald sie für diese verfügbar ist, und umgekehrt. Wenn man für das dritte klassische Schutzziel, also Integrität, eine analog strukturierte gegensätzliche Komplementarität sucht, dann ist diese mit dem Schutzziel Intervenierbarkeit ausgedrückt. Hiernach muss ein System es möglich machen, dass unter zu bestimmenden Umständen ein einwandfrei funktionierender Automatismus unterbrochen werden kann, sei es direkt durch den Betroffenen oder auf jeden Fall durch den Betreiber. Dies ist ein techniknah formuliertes Schutzziel, um Betroffenenrechte und Einzelfallgerechtigkeit operativ umzusetzen, gerade in Hinblick auf die Zunahme von automatisierten Einzelfallentscheidungen. Integrität bestimmt die Qualität einer verfügbaren Information oder eines Systems, und sowohl Verfügbarkeit als auch Integrität setzen die Möglichkeit eines Zugriffs bzw. Beobachtbarkeit voraus; sie sind insoweit auf Transparenz als Voraussetzung angewiesen. Es muss auf Daten, Funktionen und Systeme transparent zugegriffen werden können, um deren Verfügbarkeit und Integrität feststellen zu können.

Sucht man dann ebenfalls nach einer gegensätzlichen Komplementarität zum Schutzziel Transparenz, dann findet man das in dem Schutzziel Nichtverkettbarkeit, die in einem gewissen Sinne auch den Aspekt des Opaken, also einer Negation von Transparenz, enthält: Es wird nämlich dem vom Opaken Verdeckten die Bezeichnung bzw. Bezeichenbarkeit entzogen – die Sichtbarkeit erstreckt sich nicht auf den durch Nichtverkettbarkeit abgetrennten Bereich. So erfolgt eine funktionale Separierung von Daten und Systemen mit Ereignisverkettungen, die von einem Zweck bestimmt sind und nicht-zweckkonforme Ereignisverkettungen ausblenden bzw. verunmöglichen. Auf diese Weise hat man ein Instrument, um Gewaltenteilungen und Funktionstrennungen operativ durchzusetzen.

Lässt man darüber hinaus methodisch auch Selbstbezüge von Schutzzielen zu – beispielsweise lassen sich Findbarkeit als verfügbare Verfügbarkeit oder Unbeobachtbarkeit als anonyme Anonymität auffassen –, und unterscheidet Informationsinhalt (Nutzdaten) und Informationsumfeld (Kontextdaten), dann ergibt sich das in Abb. 9 dargestellte Tableau an Schutzzielen.[208]

[208] Rost / Bock, in: DuD 2011, S. 30 ff.

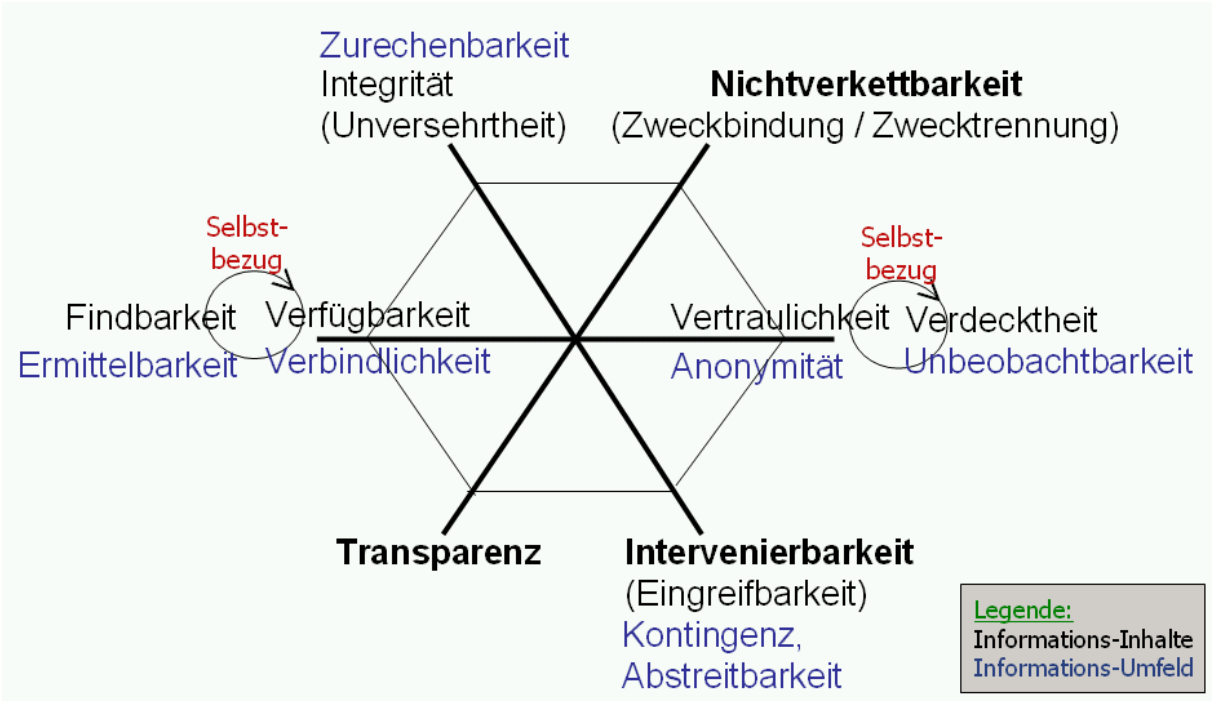


Abb. 9: Die Systematik der Schutzziele

4.2.4 Weitere Schutzziele, die im Rahmen von AAL besonders zu beachten sind

Aus den bislang aufgeführten sechs elementaren Schutzzielen (Vertraulichkeit, Integrität, Verfügbarkeit, Transparenz, Intervenierbarkeit und Nichtverkettbarkeit) lassen sich weitere Schutzziele ableiten, die in besonderen Konstellationen eine herausgehobene Rolle spielen können: Zu diesen weiteren Schutzzielen zählen Verdecktheit, Findbarkeit, Abstreitbarkeit, Kontingenz, Authentizität, Zurechenbarkeit, Verbindlichkeit, Erreichbarkeit, Ermittelbarkeit, Anonymität und Unbeobachtbarkeit.[209]

Auch die weiteren, aus den sechs elementaren Schutzzielen abgeleiteten Schutzziele müssen in Bezug auf AAL-Umgebungen im Grundsatz detailliert betrachtet werden. Beginnen sollte man aber stets mit den oben aufgeführten elementaren Schutzzielen, die bereits eine Art Datenschutz-Grundschutz erzeugt, den es in einem ersten Schritt zu erreichen gilt und der prioritär bleibt.

Im Rahmen von AAL-Umgebungen hat das Schutzziel der Unbeobachtbarkeit große Bedeutung. Es muss Räume und Zeiten geben, in denen durch eine intervenierende Aktivität des Betroffenen (oder des Vertrauten) Unbeobachtbarkeit für den Betroffenen hergestellt werden

[209] Rost / Pfitzmann, in: DuD 2009, S. 353 ff.

kann. Unbeobachtbarkeit ist mehr und anderes als die technisch-organisatorische Bereitstellung von Maßnahmen zur Herstellung von Vertraulichkeit oder Anonymität. Der Wunsch nach Unbeobachtbarkeit kann beispielsweise Aspekte der Sexualität betreffen, aber auch Aspekte politischer oder ökonomischer Handlungen des Betroffenen, die er ganz ausschließlich in seiner Verfügungsgewalt wissen will.

Auf der anderen Seite muss sichergestellt werden, dass die AAL-Dienstleistungen auch tatsächlich nur dem Betroffenen zugutekommen und zugerechnet werden, und nicht von irgendwelchen anderen Menschen nutzbar sind. Alle Beteiligten haben ein Interesse daran, dass nachweisbar korrekt, fair und vertrauenswürdig Leistungen erbracht und abgerufen werden. Zuletzt: Auch der Aspekt der Findbarkeit kann insofern eine Rolle spielen, indem das Thema, welche Hilfestellungen im Rahmen von AAL verfügbar sind, den Nutzern zur Kenntnis gebracht wird.

4.3 Best-Practice-Vorgehensweisen im Bereich Datensicherheit

Die Best-Practice-Vorgehensweise zur Umsetzung von Schutzmaßnahmen lässt sich am Beispiel der Methodik des „IT-Grundschutzes“, ergänzt um Risikoanalyse nach ISO 2700x (x = 1 bis 7), gut darstellen (siehe Abschnitt 4.3.1). Wesentliche Aspekte davon wurden bereits am Anfang dieses Kapitels skizziert. Darüber hinaus sind Standardvorgehen zur ganzheitlichen Planung im Zusammenspiel von Organisation und Technik wie ITIL (Information Technology Infrastructure Library) und COBIT (Control Objectives for Information and Related Technology) verbreitet (siehe Abschnitt 4.3.2).

4.3.1 IT-Grundschutz

4.3.1.1 Allgemeines zur Zertifizierung nach IT-Grundschutz

Unternehmen können ihre IT-Infrastruktur beim Bundesamt für Sicherheit in der Informationstechnik (BSI) zertifizieren lassen und ein IT-Grundschutz-Zertifikat erhalten.[210] Durch ein IT-Grundschutz-Zertifikat wird nachgewiesen, dass im betrachteten Verbund IT-Grundschutz erfolgreich umgesetzt worden ist. Grundlage für die Vergabe eines solchen Zertifikats ist die Durchführung eines Audits durch einen externen, vom BSI anerkannten Auditor. Das Ergebnis des Audits ist der Auditreport, der der Zertifizierungsstelle vorgelegt wird, die über die Vergabe des IT-Grundschutz-Zertifikats entscheidet.

Kriterienwerke des Verfahrens sind die IT-Grundschutz-Kataloge sowie der BSI-Standard 100-2 „IT-Grundschutz-Vorgehensweise“. In den IT-Grundschutz-Katalogen werden Standard-Sicherheitsmaßnahmen für typische Geschäftsprozesse, Anwendungen und IT-

[210] Siehe auch http://www.bsi.bund.de/gshb/zert/.

Systeme empfohlen. IT-Grundschutz verfolgt dabei einen ganzheitlichen Ansatz: Durch die geeignete Kombination von organisatorischen, personellen, infrastrukturellen und technischen Standard-Sicherheitsmaßnahmen wird ein Sicherheitsniveau erreicht, das für den normalen Schutzbedarf angemessen und ausreichend ist, um geschäftsrelevante Informationen zu schützen. Darüber hinaus bilden die Maßnahmen der IT-Grundschutz-Kataloge nicht nur eine Basis für hoch schutzbedürftige IT-Systeme und Anwendungen, sondern liefern an vielen Stellen bereits höherwertige Sicherheit.[211]

Seit 2006 ist die ursprüngliche Zertifizierung nach IT-Grundschutz durch eine anerkannte ISO 27001-Zertifizierung auf der Basis von IT-Grundschutz vollständig abgelöst worden.[212] Bei einer ISO 27001-Zertifizierung auf der Basis von IT-Grundschutz wird neben dem IT-Sicherheitsmanagement auch die konkrete Umsetzung von IT-Sicherheitsmaßnahmen auf der Basis von IT-Grundschutz geprüft. Das Audit wird nach dem Dokument „Zertifizierung nach ISO 27001 auf der Basis von IT-Grundschutz – Prüfschema für ISO 27001-Audits“ durchgeführt.[213]

4.3.1.2 Vorgehensweise

Beim IT-Grundschutz wird zunächst, wie oben bereits erläutert, die Vorgehensweise des Konzepts sowie das Informationssicherheitsmanagement dargestellt. Aufbauend hierauf werden Baustein-, Gefährdungen- und Maßnahmenkataloge beschrieben, die Bestandteile eines effizienten Informationssicherheitsmanagements im Rahmen entsprechender Organisationsstrukturen sind. Zudem stellt IT-Grundschutz Hilfsmittel zur Verfügung, z.B. Checklisten und Formulare, Muster und Beispiele, Dokumentationen und Studien sowie Informationen externer Anwender. Daneben bietet das GSTOOL eine technische Unterstützung zur Modellierung der technischen Infrastruktur (siehe Abschnitt 4.3.1.3).

4.3.1.3 Software GSTOOL

Das GSTOOL nimmt eine wichtige unterstützende Rolle ein, um die Sicherheit in einer Organisation darstellen und modellieren zu können. Mit dem GSTOOL stellt das BSI eine Software bereit, die die Anwender bei der Erstellung, Verwaltung und Fortschreibung von IT-Sicherheitskonzepten entsprechend dem IT-Grundschutz effizient unterstützt. Nach Erfassung benötigter Informationen steht dem Anwender ein umfangreiches Berichtssystem zur Verfügung, mittels dessen er strukturierte Auswertungen über alle erfassten Daten durchfüh-

[211] Die Ziele, Ideen und Konzeption von IT-Grundschutz können eingesehen werden unter: https://www.bsi.bund.de/cln_183/ContentBSI/grundschutz/kataloge/allgemein/einstieg/01001.html#1_2.

[212] Vgl. http://www.bsi.bund.de/gshb/zert/ISO27001/schema.htm.

[213] Weitere Ausführungen unter: http://www.bsi.de/gshb/zert/.

ren und diese auch auf Papier oder elektronisch ausgeben kann. Das GSTOOL unterstützt insbesondere bei folgenden Aufgaben im Rahmen der Sicherheitskonzeption:

- Erfassung von IT-Systemen, Anwendungen, Netzen usw.,
- Modellierung und Schichtenmodell nach IT-Grundschutz,
- Basissicherheitscheck / Maßnahmenumsetzung,
- Risikoanalyse auf der Basis von IT-Grundschutz,
- Kostenauswertung,
- Schutzbedarfsfeststellung,
- Berichterstellung,
- Revisionsunterstützung.

Im GSTOOL werden organisatorische Regeln und technische Verfahren transparent dargestellt. Auf dieser Grundlage kann das Zusammenspiel von Organisation und Technik, dem bei AAL eine herausragende Bedeutung zukommt, modelliert werden.

Außerdem unterstützt das GSTOOL dabei, eine Risikoanalyse und eine Risikobewertung durchzuführen, den Schutzbedarf zu ermitteln und einen Risikobehandlungsplan aufzustellen. Eine bewährte Methode ist ein Durchspielen von Risiken aufgrund eines Angreifermodells[214], dem man bestimmte intellektuelle, soziale oder ökonomische Eigenschaften mitgibt, um ein System zu „hacken“. Die Umsetzung der Maßnahmen, die sich insbesondere an den Schutzbedarfsfeststellungen orientiert, wird dann dokumentiert. Die typischen Schutzmaßnahmen für typische Risikosituationen bzw. Schutzbedarfe werden aus den IT-Grundschutz-Katalogen in der Datenbank ausgewählt, in der sich auch deren Bearbeitungsstadien dokumentieren lassen. Bei untypischen Risikoeinschätzungen sind Abweichungen in den Schutzmaßnahmen möglich. Dabei bedürfen aber Abweichungen und Ergänzungen einer zusätzlichen Begründung und eines Nachweises darüber, dass eine alternative Schutzmaßnahme mindestens dasselbe Schutzniveau erreicht wie eine Standardmaßnahme.

4.3.2 ITIL und COBIT

Als ein weitverbreitetes Standardvorgehen zur ganzheitlichen Planung und zum Controlling des Zusammenspiels von Organisation und Technik sind ITIL (Information Technology Infrastructure Library) und COBIT (Control Objectives for Information and Related Technology) zu nennen. So wie für die Analyse der Datensicherheit die IT-Grundschutz-Kataloge ver-

[214] Im Rahmen von AAL kann es durchaus Sinn machen, auch Betroffene als „Angreifer“ zu modellieren, beispielsweise für den Fall, dass Betroffene sich nicht normal verhalten, sondern ein „AAL-“ oder „sensorgerechtes Leben“ inszenieren. Aus Datenschutzsicht ist es dabei grundsätzlich problematisch, wenn die Technik den Betroffenen automatisch überführt.

fügbar sind, so findet man für ITIL und COBIT Unterstützung durch Checklisten für den Betrieb und die Konfiguration von technisch-organisatorischen Prozessen. ITIL und COBIT werden in den IT-Grundschutz-Katalogen ebenfalls empfohlen.[215]

Ein Vorgehen nach ITIL ist mittlerweile Standard, um einen komplexen IT-Betrieb, wie er in einem Rechenzentrum vorherrscht, oder einen Betrieb von Infrastrukturen, für die ein hoher oder sehr hoher Schutzbedarf besteht und wie es im Umfeld von AAL typischerweise der Fall ist, überprüfbar sicher zu machen. Selbst wenn Pflege- oder Medizin-Dienstleister den IT-Betrieb nicht in Eigenregie durchführen, sondern im Sinne einer Auftragsdatenverarbeitung an einen oder mehrere IT-Dienstleister auslagern („outsourcen“), was ein typischer Fall sein dürfte, muss dem für die Datenverarbeitung nach wie vor verantwortlichen Pflege- oder Medizin-Dienstleister klar sein, welche Anforderungen an die Beherrschung von Prozessen und an die Datensicherheit für einen sicher funktionierenden IT-Betrieb gestellt werden müssen, und welche Aspekte in den Verträgen entsprechend aufzunehmen und zu regeln sind. Standardmäßig sollte sich ein Medizin-Dienstleister für ein Rechenzentrum entscheiden, das nach IT-Grundschutz zertifiziert ist. Konzeptionell unerlässlich ist, dass in den Dokumentationen und Verträgen sämtliche Risiken – insbesondere diejenigen, die technisch und organisatorisch fortbestehen oder die nur durch Abschluss von Versicherungen kompensiert werden können oder in Kauf genommen werden müssen – aufgeführt sind und letztlich von einer Instanz zu verantworten sind. Das Konzept der Schutzziele hilft, dass alle relevanten Risiken der Datensicherheit und des Datenschutzes einer Betrachtung unterzogen werden können.

Nicht nur für den Entwurf des AAL-Systems ist die Berücksichtigung der Schutzziele wichtig, sondern auch bei allen anstehenden Veränderungen. Das „Change Management“ nach ITIL zielt darauf ab, dass Änderungsanforderungen in definierten Prozessen geordnet und unter Vermeidung von unnötigen Risiken umgesetzt werden. Sowohl für den Entwurf von AAL-Systemen als auch für ein kontrolliertes Change Management sind Referenzwerte für die sechs elementaren Schutzziele bzw. die von diesen Schutzzielen adressierten Schutzmaßnahmen abzuleiten. Gegen diese Ziele ist dann zu prüfen, bevor ein System installiert wird oder Changes bei bestehenden Systemen durchgeführt werden, unter der Fragestellung: Wie wirkt sich die Einführung einer weiteren Komponente auf das System im Hinblick auf Verfügbarkeit, Integrität, Vertraulichkeit, Transparenz, Intervenierbarkeit und Nichtverkettbarkeit des gesamten Systems und dessen Komponenten aus? Sind die dazu notwendigen Tests einzelner Komponenten sowie des gesamten Systems durchgeführt und dokumentiert? Sind die Komponenten und das gesamte System dokumentiert? Ist die Sicherstellung der Nichtverkettbarkeit möglicherweise durch den Einbau einer weiteren, aus AAL-Sicht zunächst als unscheinbar gewerteten Komponente gebrochen? So kann der Einbau eines Energieverbrauchmessgeräts, etwa im Rahmen von Smart Metering, dazu führen, dass sich ansonsten getrennte Aktivitäten von Systemen und Menschen in Kausalzusammenhänge

[215] Siehe auch http://wiki.de.it-processmaps.com/index.php/ITIL-Checklisten.

bringen lassen. Man kann möglicherweise auch erkennen, welche Sensorik in einem mit AAL-Techniken ausgestatteten Haushalt verbaut ist. Es muss fortgesetzt eine Technikfolgenabschätzung im Rahmen eines Datenschutzmanagementsystems für das gesamte System durchgeführt werden.

4.4 Ergebnisse und offene Fragen

Beim Entwurf eines sicheren und datenschutzgerecht funktionierenden AAL-Systems sollten die folgenden sechs elementaren Schutzziele berücksichtigt werden: Verfügbarkeit, Integrität, Vertraulichkeit sowie Transparenz, Intervenierbarkeit und Nichtverkettbarkeit. Der spätere Betrieb einer derart zugeschnittenen AAL-Komponente bzw. eines AAL-Gesamtsystems lässt sich dann umso leichter anhand der von den Schutzzielen vorgegebenen Schutzmaßnahmen prüfen, regulieren und steuern. Es ist zu betonen, dass allein mit der Erfüllung der Anforderungen der Datensicherheit die Anforderungen speziell des Datenschutzes noch nicht erfüllt sind. Beispielsweise reicht es für die Erfüllung der Datenschutzanforderungen nicht aus, Verschlüsselungstechniken beim Übertragen oder Speichern von Daten einzusetzen.

Der „AAL-Würfel Datenschutz“ soll dabei helfen, die folgenden Komponenten in einen überschaubaren Gesamtzusammenhang zu stellen:

- die in AAL-Systemen typischerweise erzeugten Daten einschließlich deren Schutzbedarfs sowie des daraus folgenden Schutzbedarfs der IT-Systeme,
- die Akteure, die diese Daten in Verantwortung verarbeiten, und
- die Schutzziele, mit denen u.a. wesentliche gesetzliche Anforderungen an Transparenz, Zweckbindung und Betroffenenrechte erfüllt werden.

Methodisch empfiehlt es sich, sich bei der Planung, der Implementierung, dem Betrieb und der Prüfung an die Vorgaben des IT-Grundschutzes zu halten. Mindestens zwei Herausforderungen müssen dabei im AAL-Umfeld unter erschwerten Bedingungen bewältigt werden: Wie erzeugt man Transparenz bezüglich der für die Betroffenen wesentlichen Aspekte der Datenverarbeitung auch gegenüber solchen Personen, die kein Verständnis von der Technik haben, die zudem überwiegend im Hintergrund abläuft? Und wie gestaltet man gerade in solchen Fällen technische Abläufe, ohne dass beispielsweise ein zeitweises Abschalten einer Systemkomponente zu einer lebensbedrohlichen Situation z.B. dadurch führt, dass der Betroffene vergisst, das System wieder anzuschalten?

Juristisch ist zu klären, welche Anforderungen wie konkret rechtlich festgeschrieben werden sollten. Dies ist insbesondere in den Spannungsfeldern relevant, die zwangsläufig durch die Wechselwirkungen zwischen den sechs elementaren Schutzzielen unmittelbar oder durch sie umsetzende Maßnahmen entstehen. Dabei ist zu beachten, dass sich die Schutzziele nicht nur auf die technische Gestaltung von AAL-Anwendungen und AAL-Systemkomponenten einschließlich der technisch-organisatorischen Maßnahmen auswirken,

sondern auch etwa Rechtsnormen, die Einsetzung von Treuhändern, Geschäftsmodelle oder Versicherungsangebote betreffen können.

Offen ist, inwieweit die Erkenntnisse, die in einer fortgeführten Diskussion der Rechtsfragen zusammen mit Praktikern gewonnen werden sollten, auch in die technische Standardisierung von AAL-Anwendungen oder AAL-Systemkomponenten einfließen können.

5 Haftungsrechtliche Anforderungen und Fragestellungen

Bei jeder Art von technischen Systemen sind die haftungsrechtlichen Ansprüche im Fall von Mängeln und Fehlfunktionen zu untersuchen. Im AAL-Bereich ist dies umso relevanter, als es um besonders sensible Daten geht. Aus dem Haftungsbereich, der sich bei Ambient Assisted Living durch eine hohe Komplexität bedingt durch die Vielzahl von Beteiligten, ineinander verschränkte Dienstleistungen und vielfältige Rechtsbeziehungen der Beteiligten untereinander auszeichnet, ergeben sich viele juristische Fragen, die für jeden konkreten Einzelfall zu analysieren wären.

In diesem Kapitel kann nur ein grober Überblick über die wesentlichen rechtlichen Regelungen und Anforderungen geben werden: Zunächst werden die Grundlagen der vertraglichen Haftung erläutert (siehe Abschnitt 5.1). Anschließend wird für AAL-Anwendungen die Haftung nach dem Datenschutzrecht (siehe Abschnitt 5.2) untersucht, gefolgt von der Haftung nach dem Medizinproduktegesetz (siehe Abschnitt 5.3) und der Produkthaftung (siehe Abschnitt 5.4). Als Letztes kommt die Arzthaftung in Betracht (siehe Abschnitt 5.5). Die aus den vorherigen Ausführungen abgeleiteten Ergebnisse und offenen Fragen sind in Abschnitt 5.6 zusammengefasst.

5.1 Vertragliche Haftung

Gesetzlich geregelte Schuldverhältnisse sehen unter bestimmten Voraussetzungen bei der Verletzung einer aus einem solchen Schuldverhältnis bestehenden Pflicht grundsätzlich einen Anspruch auf Schadensersatz vor, so auch beim Kauf, bei einem Dienstvertrag oder bei einem Werkvertrag. Der Betroffene kann dann Ersatz des durch die Verletzung entstandenen Schadens verlangen, §§ 280, 281 BGB. Der Käufer einer AAL-Anwendung kann bei einer Pflichtverletzung nach §§ 280, 281 BGB i.V.m. §§ 437, 440 BGB Schadensersatz verlangen, bei einem zugrundeliegenden Werkvertrag nach §§ 280, 281 BGB i.V.m. §§ 631 ff. BGB.

Außerdem kommen bei dem Vorliegen von Mängeln (bzw. bei fehlenden Eigenschaften) Gewährleistungsrechte zur Anwendung, die im Falle eines Kaufs in § 437 BGB oder im Falle eines Werkvertrags in § 634 BGB gesondert geregelt sind. Bei vorvertraglichen Beziehungen können sich Ansprüche aus „culpa in contrahendo“[216] (im Folgenden: c.i.c.) ergeben, § 311 Abs. 2 und 3 BGB. Daneben kommt eine deliktische Haftung in Betracht, die exemplarisch im Rahmen der Haftung nach den Vorschriften des Datenschutzrechts (siehe Abschnitt 5.2) dargestellt wird.

Insoweit ergeben sich keine Besonderheiten und offene Fragen.

[216] „Culpa in contrahendo“: Verschulden bei Vertragsschluss.

5.2 Haftung nach dem Datenschutzrecht

§ 7 BDSG enthält eine eigenständige datenschutzrechtliche Haftungsnorm, die auf sämtliche verantwortliche Stellen im öffentlichen und im nicht-öffentlichen Bereich anwendbar ist (siehe Abschnitt 5.2.1). Dabei handelt es sich um eine Haftung für vermutetes Verschulden. Eine umfassende Gefährdungshaftung sieht das BDSG nur für öffentliche Stellen im Rahmen der automatisierten Datenverarbeitung vor, § 8 BDSG.[217]

Ein Rückgriff auf andere (vertragliche oder deliktische) Anspruchsgrundlagen ist durch diese Haftungsnormen nicht ausgeschlossen.[218] So kommen Ansprüche aus Verletzungen von Schutz- oder Nebenpflichten im vertraglichen oder vorvertraglichen Bereich (§ 280 Abs. 1 i.V.m. § 241 Abs. 2 BGB bzw. c.i.c. nach § 280 Abs. 1 i.V.m. §§ 241 Abs. 2, 311 Abs. 2 BGB, siehe Abschnitt 5.2.2) sowie allgemein deliktische Ansprüche (§§ 823 ff. BGB, siehe Abschnitt 5.2.3) und ggf. wettbewerbsrechtliche Ansprüche (§§ 1 ff. Gesetz gegen den unlauteren Wettbewerb (UWG)) in Betracht.

Daraus abgeleitete Ergebnisse und offene Fragen enthält Abschnitt 5.2.4.

5.2.1 Haftung nach § 7 BDSG

Voraussetzung einer Haftung ist, dass eine verantwortliche Stelle dem Betroffenen durch eine nach dem BDSG oder anderen Vorschriften über den Datenschutz unzulässige oder unrichtige Erhebung, Verarbeitung oder Nutzung seiner personenbezogenen Daten einen Schaden zufügt.[219] Dabei liegt die Beweislast für das Verschulden entgegen dem generellen Grundsatz nicht bei dem Geschädigten, sondern beim Schädiger, dem es obliegt, einen Entlastungsbeweis zu führen.[220] Hierfür reicht – entgegen dem sonst üblichen Maßstab des § 276 BGB – die nach den Umständen des Falls gebotene Sorgfalt, um sich zu exkulpieren.

Je größer die potenziellen Risiken für den Betroffenen sind, umso effektiver müssen die Vorkehrungen sein, die diesen vor Schäden schützen. Medizinische Daten bedürfen daher einer ungleich sorgsameren Behandlung als weniger sensible Daten.[221] Die Beweisführung der

---

[217] Däubler, in: Däubler / Klebe / Wedde / Weichert (Hrsg.), Bundesdatenschutzgesetz Kompaktkommentar, 3. Auflage, 2010, § 7 Rn. 2, der bei dieser Differenzierung Bedenken im Hinblick auf den Gleichheitssatz des Art. 3 Abs. 1 GG hat, dass die Schutzbedürftigkeit der Betroffenen keineswegs geringer ist, wenn ihre Daten statt im öffentlichen im nicht-öffentlichen Bereich verarbeitet werden.

[218] Däubler, in: Däubler / Klebe / Wedde / Weichert (Hrsg.), Bundesdatenschutzgesetz Kompaktkommentar, 3. Auflage, 2010, § 7 Rn. 1.

[219] Däubler, in: Däubler / Klebe / Wedde / Weichert (Hrsg.), Bundesdatenschutzgesetz Kompaktkommentar, 3. Auflage, 2010, § 7 Rn. 10 und 13.

[220] § 7 Satz 2 BDSG.

[221] Däubler, in: Däubler / Klebe / Wedde / Weichert (Hrsg.), Bundesdatenschutzgesetz Kompaktkommentar, 3. Auflage, 2010, § 7 Rn. 14 und 15.

Pflichtverletzung obliegt dagegen dem Geschädigten.[222] Nach herrschender Meinung umfasst die Ersatzpflicht keine immateriellen Schäden.[223]

5.2.2 Vertragliche und vertragsähnliche Ansprüche

Bei bestehender vertraglicher Beziehung können sich Ansprüche aus der Verletzung einer Pflichtverletzung (§§ 280, 281 BGB, s.o.) bzw. bei vorvertraglichen Beziehungen aus c.i.c. (§ 311 Abs. 2 und 3 BGB, s.o.) ergeben. Liegt ein solches vertragliches oder vorvertragliches Verhältnis vor, stellt eine vertragswidrige Datenverarbeitung jedenfalls die Verletzung einer vertraglichen Nebenpflicht bzw. einer vorvertraglichen Schutzpflicht dar, die, sofern nicht ausdrücklich vertraglich vereinbart, sich aus den §§ 241 Abs. 2, 242 BGB i.V.m. dem Recht auf informationelle Selbstbestimmung des Betroffenen ergibt.

Personenbezogene Daten dürfen von speichernden Stellen im Rahmen der Zweckbestimmung eines Vertrags oder eines vertragsähnlichen Vertrauensverhältnisses verarbeitet und genutzt werden, § 28 Abs. 1 Nr. 1 BDSG. Eine schuldhafte Verletzung der damit verbundenen Pflichten, z.B. die Nichterfüllung von Auskunftspflichten, kann zu Ansprüchen aus positiver Forderungsverletzung führen. Das Verschulden wird nach der Beweislastumkehr des § 280 Abs. 1 Satz 2 BGB vermutet. Dabei muss auch für Erfüllungsgehilfen nach § 278 BGB gehaftet werden. Im Schadensfall ist die speichernde Stelle verpflichtet, den Betroffenen so zu stellen, als wenn sie ihre Schutz- und Obhutspflichten erfüllt hätte (§ 249 Abs. 1 BGB). Immaterieller Schadensersatz ist gem. § 253 BGB ersatzfähig. Die vertragsrechtlichen Grundsätze gelten in gleicher Weise für Ansprüche aus c.i.c. nach § 280 Abs. 1 i.V.m. §§ 241 Abs. 2, 311 Abs. 2 BGB.

5.2.3 Deliktsrechtliche Ansprüche

In Betracht kommen außerdem die zentralen Schadensersatzansprüche aus § 823 Abs. 1, § 823 Abs. 2 BGB i.V.m. Datenschutzvorschriften und § 826 BGB.

Nach § 823 Abs. 1 BGB ist schadensersatzpflichtig, wer vorsätzlich oder fahrlässig das Leben, den Körper, die Gesundheit, die Freiheit, das Eigentum oder ein sonstiges Recht eines anderen widerrechtlich verletzt. Unter die von § 823 Abs. 1 BGB genannten Schutzgüter fällt anerkanntermaßen als sog. Rahmenrecht auch das allgemeine Persönlichkeitsrecht.[224] Werden personenbezogene Daten entgegen den einschlägigen Vorschriften der Datenschutzgesetze erhoben, verarbeitet oder genutzt, liegt grundsätzlich ein Eingriff in das zum Persönlichkeitsrecht gehörende Recht auf informationelle Selbstbestimmung und damit eine

[222] Vgl. Niedermeier / Schröcker, in: RDV 2002, 217, 219.

[223] Däubler in: Däubler / Klebe / Wedde / Weichert (Hrsg.), Bundesdatenschutzgesetz Kompaktkommentar, 3. Auflage, 2010, § 7 Rn. 19; Gola / Schomerus, Bundesdatenschutzgesetz, 10. Auflage, 2010, § 7 Rn. 12.

[224] Niedermeyer / Schröcker, in: RDV 2002, S. 217, 220.

Rechtsgutverletzung vor. Bei einem solchen Eingriff in das allgemeine Persönlichkeitsrecht kann eine angemessene Entschädigung auch für die erlittenen immateriellen Nachteile verlangt werden (§ 253 BGB).[225]

Eine zum Schadenersatz verpflichtende Handlung liegt auch vor, wenn ein Schutzgesetz rechtswidrig und schuldhaft verletzt wird (§ 823 Abs. 2 BGB). Zu diesen Gesetzen gehören die meisten Strafbestimmungen (z.B. § 203 StGB) und auch die allgemeinen Datenschutzgesetze.[226] § 826 BGB kommt als Generalklausel in Betracht bei vorsätzlicher sittenwidriger Schädigung.[227] Nach dem Datenschutzrecht bestehende Schadensersatzansprüche nach § 7 f. BDSG werden bislang äußerst selten geltend gemacht. Hintergrund ist, dass der Bundesgesetzgeber einem Vorschlag der europäischen Datenschutzrichtlinie 95/46/EG bislang nicht gefolgt ist, eine verschuldensunabhängige Haftung des Datenverarbeiters einzuführen.[228]

5.2.4 Haftung nach dem Datenschutzrecht: Ergebnisse und offene Fragen

Im Ergebnis bestehen zwar ausreichende Haftungstatbestände für den AAL-Bereich, da neben den spezifischen datenschutzrechtlichen Haftungsnormen auch die allgemeinen Haftungsnormen des Zivilrechts Anwendung finden. Allerdings wird es für einen Betroffenen angesichts der für ihn wegen der großen Komplexität kaum durchschaubaren AAL-Systeme schwierig sein, diejenigen der beteiligten Dienstleister ausfindig zu machen, denen ein Verschulden durch Vorsatz oder Fahrlässigkeit anzulasten ist, und darüber möglicherweise sogar noch einen Nachweis zu erbringen.

---

[225] Däubler, in: Däubler / Klebe / Wedde / Weichert (Hrsg.), Bundesdatenschutzgesetz Kompaktkommentar, 3. Auflage, 2010 § 7 Rn. 30; ausführlich dazu auch Niedermeyer / Schröcker, in: RDV 2002, S. 217, 222 ff.

[226] Dazu Simitis, in: Simitis (Hrsg.), BDSG, 6. Auflage, 2006, § 7 Rn. 68.

[227] In Verbindung mit einem Deliktstatbestand besteht darüber hinaus ein Beseitigungsanspruch des Betroffenen analog § 1004 BGB (quasinegatorischer Unterlassungsanspruch). Dieser Anspruch auf Beseitigung des Störzustands (z.B. unrichtige Datenweitergabe) setzt nicht notwendig ein schuldhaftes Verhalten der speichernden Stelle bzw. von deren Mitarbeitern voraus. Konkret bedeutet dies, dass die speichernde Stelle die Berichtigung bzw. Löschung der Informationen bei Dritten veranlassen muss, die unzulässig Informationen von ihr erhalten haben. Daneben besteht auch ein Unterlassungsanspruch analog § 1004 BGB, wenn der Betroffene die Verletzung seines Persönlichkeitsrechts zu befürchten hat.

[228] Unabhängiges Landeszentrum für Datenschutz / Humboldt-Universität Berlin, TAUCIS – Technikfolgenabschätzung Ubiquitäres Computing und Informationelle Selbstbestimmung, Studie im Auftrag des Bundesministeriums für Bildung und Forschung, S. 266 m.w.N.
Art. 23 der europäischen Datenschutzrichtlinie 95/46/EC „Haftung“ lautet:
„(1) Die Mitgliedstaaten sehen vor, daß jede Person, der wegen einer rechtswidrigen Verarbeitung oder jeder anderen mit den einzelstaatlichen Vorschriften zur Umsetzung dieser Richtlinie nicht zu vereinbarenden Handlung ein Schaden entsteht, das Recht hat, von dem für die Verarbeitung Verantwortlichen Schadenersatz zu verlangen.
(2) Der für die Verarbeitung Verantwortliche kann teilweise oder vollständig von seiner Haftung befreit werden, wenn er nachweist, daß der Umstand, durch den der Schaden eingetreten ist, ihm nicht zur Last gelegt werden kann.“

Vor dem Hintergrund, dass die automatisierte Datenverarbeitung im Bereich von AAL zu einem bisher so nicht bestehenden Ausmaß in allen Lebensbereichen des Betroffenen führt und durch die Einbindung einer Vielzahl von Dienstleistern mit diversen technischen Systemen eine hohe Komplexität entsteht, ist jedoch zu prüfen, ob die rechtliche Einführung einer verschuldensunabhängigen Haftung der Datenverarbeiter geboten ist. Bei einer verschuldensunabhängigen Haftung müsste der Betroffene das Verschulden oder die Nachlässigkeit der Datenverarbeiter nicht nachweisen. Zumindest wäre eine Beweislasterleichterung sinnvoll. Weiterhin sollten praktische Lösungen erarbeitet werden, die es einem Betroffenen erleichtern, im Falle eines Schadens seine Rechte geltend zu machen. Da es häufig schwierig ist, einen Schaden monetär zu beziffern, könnten hier Pauschalen zum Einsatz kommen.

5.3 Haftung nach dem Medizinproduktegesetz

Bei AAL-Systemen, die mit medizinischen Daten arbeiten, könnte es sich um Medizinprodukte handeln, für die es eine eigene Haftungsnorm im Medizinproduktegesetz gibt. Im Folgenden wird zunächst eine Definition des Begriffs Medizinprodukt gegeben (siehe Abschnitt 5.3.1). Weiterhin wird die Problematik bei der Einordnung von AAL-Systemen als Medizinprodukt aufgezeigt (siehe Abschnitt 5.3.2). Die Konsequenzen für Hersteller von Medizinprodukten ergeben sich aus Abschnitt 5.3.3. Schließlich fasst Abschnitt 5.3.4 Ergebnisse und offene Fragen zur Haftung nach dem Medizinproduktegesetz zusammen.

5.3.1 Definition von Medizinprodukten

Viele zu medizinischen Zwecken einsetzbare AAL-Systeme könnten als Medizinprodukte einzustufen sein, mit der Konsequenz, dass sie den Regelungen des Medizinproduktegesetzes (MPG) und der zugehörigen Verordnungen bzw. der europäischen Rechtsakte, auf denen die nationalstaatlichen Regelungen beruhen,[229] unterworfen sind.

Die gesetzliche Definition von Medizinprodukten in § 3 Nr. 1 MPG ist weit gefasst:

„Medizinprodukte sind alle einzeln oder miteinander verbunden verwendeten Instrumente, Apparate, Vorrichtungen, Software, [...] oder andere Gegenstände einschließlich der vom Hersteller speziell zur Anwendung für diagnostische oder therapeutische Zwecke bestimmten und für ein einwandfreies Funktionieren des Medizinproduktes eingesetzten Software, die vom Hersteller zur Anwendung für Menschen mittels ihrer Funktionen zum Zwecke

a) der Erkennung, Verhütung, Überwachung, Behandlung oder Linderung von Krankheiten,

b) der Erkennung, Überwachung, Behandlung, Linderung oder Kompensierung von Verletzungen oder Behinderungen,

[229] Siehe z.B. Übersicht bei Quaas / Zuck, § 45 Rn. 2.

c) der Untersuchung, der Ersetzung oder der Veränderung des anatomischen Aufbaus oder eines physiologischen Vorgangs oder

d) der Empfängnisregelung

zu dienen bestimmt sind und deren bestimmungsgemäße Hauptwirkung im oder am menschlichen Körper weder durch pharmakologisch oder immunologisch wirkende Mittel noch durch Metabolismus erreicht wird, deren Wirkungsweise aber durch solche Mittel unterstützt werden kann."

Die Grenzziehung zu anderen Produkten erfolgt dabei zum einen in der Abgrenzung zu Arzneimitteln, die für die hiesige Betrachtung aber nicht relevant ist,[230] zum anderen durch die Zweckbestimmung, die das Produkt durch den Hersteller bekommt.[231]

Die bisher diskutierten Ideen und Anwendungsszenarien für AAL-Systeme, die vom Hersteller zum Einsatz bei der Überwachung des Gesundheitszustands im weitesten Sinne vorgesehen sind, erfüllen regelmäßig die Voraussetzungen, um vom Gesetz als Medizinprodukt kategorisiert zu werden. Die im Rahmen dieser Vorstudie zu betrachtenden Assistenzsysteme für den Einsatz bei und für Menschen höheren Alters dienen ganz überwiegend primär oder zumindest partiell medizinischen Zwecken. Zu denken ist hier z.B. an Systeme zur Sturzprävention oder -meldung sowie permanentes Monitoring des Gesundheitszustands mit Rückmeldungen an den Betroffenen, Pflegepersonen oder den Arzt. Diese Anlagen sind von solchen Systemen abzugrenzen, die ausschließlich anderen Zwecken dienen, z.B. dem persönlichen Komfort (Regulierung der Raumtemperatur) oder der Erleichterung des Alltags (intelligenter Kühlschrank), die mangels Einsatzzwecks im medizinischen Bereich nicht dem MPG unterfallen.

5.3.2 Problem: Einordnung als Medizinprodukt

Schon bisher war die Grenzziehung zwischen Medizinprodukten und Nicht-Medizinprodukten oft schwierig und nur einzelfallbezogen durchführbar.[232] Bisher wurden als Produkte zur Erkennung und Überwachung von Krankheiten, Verletzungen oder Behinderungen vor allem Diagnostika und medizinisch-technische Geräte (CT-, MRT-, Röntgengeräte) subsumiert, die ausschließlich oder in erster Linie zum Einsatz im medizinischen Bereich vorgesehen waren.

---

[230] Die negative Abgrenzung von Medizinprodukten mit physikalischer Wirkung und Arzneimitteln mit pharmakologischer, metabolischer oder immunologischer Wirkung wird in der Literatur umfangreich dargestellt. Siehe u.a. Deutsch, Medizinrecht Rn. 1624 m.w.N.; Ratzel, in: Rieger / Dahm / Steinhilper (Hrsg.), Heidelberger Kommentar Arztrecht – Krankenhausrecht – Medizinrecht, Stand Juli 2008, Kap. 3590, Rn. 3 ff.

[231] Ratzel, in: Rieger / Dahm / Steinhilper (Hrsg.), Heidelberger Kommentar Arztrecht – Krankenhausrecht – Medizinrecht, Stand Juli 2008, Kap. 3590, Rn. 3 ff.; Rehmann, in: Rehmann / Wagner, § 3 MPG, Rn. 1.

[232] Rehmann, in: Rehmann / Wagner (Hrsg.), § 3 MPG, Rn. 1 m.w.N.

Im AAL-Bereich wird der Einsatz unterschiedlichster Sensoren diskutiert. Dabei wird überdacht werden müssen, ob und wie Geräte und Module, die vom Hersteller nicht zu medizinischen Zwecken in den Verkehr gebracht werden, den Regelungen für Medizinprodukte unterworfen werden müssen. Soweit bildgebende oder anderweitig unmittelbar die Person „messende“ Sensoren zum Einsatz kommen (Kamera, Sturzsensor im Raum, Wärmebildkamera zur Erfassung der Körpertemperatur, Bewegungssensoren und GPS in Mobiltelefonen), ist eine Zuordnung als Medizinprodukt eher naheliegend. Offen ist aber, ob auch Sensoren, die nicht einmal unmittelbar mit der Person zusammenhängende Daten erheben, den strengen Regelungen des MPG unterfallen sollen, wenn diese Daten zum Monitoring des Gesundheitszustands verarbeitet werden. Zu denken ist hier beispielsweise an Strom- und Wasserzähler[233], deren Messdaten durch Sammeln und Auswerten Rückschlüsse auf Veränderungen des Tagesrhythmus und damit verbundener gesundheitlicher Verhältnisse zulassen.

Grundsätzlich wäre hier im Interesse der betroffenen Personen und zu deren Schutz eine Regulierung und Qualitätskontrolle im Rahmen der Prüfrichtlinien für Medizinprodukte wünschenswert. Andererseits sollte eine Überregulierung verhindert werden, die Hersteller sämtlicher im „intelligenten Haus“ verwendeter Geräte in Zugzwang bringt, ihre Informationstechnik einschließlich aller Haushaltsgeräte und Unterhaltungselektronik etc. nach dem MPG zertifizieren zu lassen.

5.3.3 Konsequenzen für Hersteller eines Medizinprodukts

Für die Hersteller ergeben sich aus einer Einordnung eines AAL-Systems oder dessen Komponenten als Medizinprodukt diverse Konsequenzen, von denen im Folgenden die Wichtigsten dargestellt werden.

Die Verantwortlichkeit für das erstmalige Inverkehrbringen trägt der Hersteller, sein Bevollmächtigter oder derjenige, der ein Produkt erstmals in den Europäischen Wirtschaftsraum einführt, § 5 Abs. 1 MPG.

Abb. 10: CE-Zeichen für zertifizierte Medizinprodukte

[233] Vgl. Ideen des Projekts SmartAssist, http://www.itm.uni-luebeck.de/projects/smartassist/; Rothenpieler / Becker / Fischer, in: Tagungsband der 6th IFIP WG 9.2, 9.6/11.4, 11.6, 11.7/PrimeLife International Summer School, 2011.

Medizinprodukte bedürfen der Zertifizierung. Dabei ist das Produkt vor dem Inverkehrbringen mit einem CE-Zeichen zu versehen (siehe Abb. 10).

Art und Umfang der Zertifizierung richten sich nach der Klassifizierung des Medizinprodukts.[234] Produkte der Klasse I mit geringem Risikopotenzial können dabei vom Hersteller selbst zertifiziert werden, soweit sie nicht im sterilen Zustand in den Verkehr gebracht werden oder mit Messfunktionen ausgestattet sind.[235] Letzteres wird aber gerade bei den oft in AAL-Systemen zur Anwendung kommenden Sensoren und Sensornetzwerken der Fall sein. Für diese Systeme ist eine Zertifizierung unter Beteiligung einer benannten Stelle im Sinne des § 15 ff. MPG erforderlich. Rezertifizierungen sind im 5-Jahres-Turnus erforderlich.

Der Gegenstand der Zertifizierung bzw. der Umfang des AAL-Systems muss jeweils genau festgelegt sein. Der Umfang kann von einzelnen Komponenten bis hin zum Zusammenspiel der Komponenten mit der Betriebs- und Auswertungssoftware des Gesamtsystems reichen. Generell stellt § 10 MPG zunächst auf das Vorhandensein einer CE-Kennzeichnung der Einzelteile ab. Für Behandlungseinheiten, die aus Modulen mit CE-Kennzeichen zusammengestellt werden, ist kein Konformitätsfeststellungsverfahren erforderlich. Andere Zusammenstellungen müssen dagegen ein solches Verfahren durchlaufen, § 10 Abs. 1, 2 MPG.

Um ein reibungsloses und sicheres Zusammenwirken der Komponenten sicherzustellen, sind gegebenenfalls weitere Standardisierungen von Schnittstellen anzustreben oder bestehende Schnittstellen in entsprechende Standards für Medizinprodukte zu übernehmen. Bei Standards, die der Kommunikation und dem Datenaustausch zwischen Komponenten und Beteiligten dienen, sollte bereits bei deren Entwicklung bedacht werden, die rechtlichen Belange – insbesondere des Datenschutzrechts, das Anforderungen an die datenschutzgerechte Gestaltung von Informationstechnik stellt (siehe Abschnitt 3.3.5) – frühzeitig zu berücksichtigten. Entsprechende Vorgaben sollten auf europäischer Ebene definiert werden und in harmonisierte Normen im Sinne des § 8 MPG einfließen.

Verantwortliche für das Inverkehrbringen von Medizinprodukten (siehe § 5 Abs. 1 MPG: Hersteller, Bevollmächtigter, Importeur) müssen einen Sicherheitsbeauftragten für Medizinprodukte bestellen, § 30 Abs. 1 MPG.

Soweit ein AAL-System als Medizinprodukt anzusehen ist, sind bezüglich der Werbung möglicherweise Einschränkungen zu berücksichtigen, die über das Maß des üblichen Verbraucherschutzes nach dem UWG und anderen Gesetzen hinausgehen, vgl. § 4 Abs. 2 MPG, § 1 Abs. 1 Nr. 1a i.V.m. § 11 HWG.

---

[234] Näher zur Klassifizierung: Pannenbecker, in: Terbille, Münchener Anwaltshandbuch Medizinrecht, § 9 Rn. 278. siehe auch: Guidelines for the Classification of Medical Devices, MEDDEV 2.4/1 rev. 8 July 2001, abrufbar unter: http://ec.europa.eu/enterprise/medical_devices/meddev/meddev_index_en.htm.

[235] Quaas / Zuck, Medizinrecht, § 45 Rn. 6; Deutsch / Spickhoff, Medizinrecht, Rn. 1637.

Bezüglich der Haftung enthält das MPG keine besonderen Haftungsnormen, die eine Gefährdungshaftung für Medizinprodukte als solche begründen würden.[236] Anwendbar sind die allgemeinen Haftungsregeln der §§ 823 ff. BGB (s.o.). Die Normen des MPG und der auf dessen Grundlage erlassenen Verordnungen stellen dabei Schutzgesetze im Sinne des § 823 Abs. 2 BGB dar.[237] Anwender haften daher nur bei Verschulden.[238] Bei Herstellern gelten für die vertragliche Haftung nach dem BGB die üblichen Grundsätze mit der Maßgabe, dass der Patient oder Nutzer in den Schutzbereich von Verträgen zwischen Hersteller und Vertreiber bzw. Anwender eingeschlossen ist.[239] Daneben gelten für Hersteller die Regelungen des Produkthaftungsgesetzes (siehe Abschnitt 5.4).[240]

5.3.4 Haftung nach dem MPG: Ergebnisse und offene Fragen

Auch wenn das MPG keine gesonderten Haftungsregelungen enthält, kann es im Rahmen des § 823 Abs. 2 BGB als Maßstab herangezogen werden, weil für Medizinprodukte insoweit bestimmte Qualitätsstandards gelten, die der Sensibilität des medizinischen Bereichs angemessen sind. Offen ist aber, welche Teile einer AAL-Anwendung als Medizinprodukt einzustufen sind und welche nicht. Hier ist eine Klärung im Sinne der Rechtssicherheit erforderlich, um sowohl Herstellern und Betreibern als auch den Betroffenen deutlich zu machen, wann die Qualitätsstandards des MPG einzuhalten sind und wann darauf verzichtet wird.

5.4 Produkthaftung

Die zivilrechtliche Produkthaftung kann auf verschiedenen Anspruchsgrundlagen beruhen. Es kommen Ansprüche aus Vertragsverletzungen (siehe oben Abschnitte 5.1 und 5.2.2), eine verschuldensunabhängige Produkthaftung nach dem Produkthaftungsgesetz (siehe Abschnitt 5.4.1) und Ansprüche aus unerlaubter Handlung nach §§ 823 ff. BGB (sog. Produzentenhaftung, siehe Abschnitt 5.4.2) in Betracht. Abschnitt 5.4.3 fasst die Ergebnisse und offenen Fragen zusammen.

---

[236] Quaas / Zuck, Medizinrecht, § 47 Rn. 1; Deutsch / Spickhoff, Medizinrecht, Rn. 1669.

[237] Deutsch / Spickhoff, Medizinrecht, Rn. 1670.

[238] Quaas / Zuck, Medizinrecht, § 47 Rn. 1.

[239] Deutsch / Spickhoff, Medizinrecht, Rn. 1673.

[240] Deutsch / Spickhoff, Medizinrecht, Rn. 1673.

5.4.1 Produkthaftung nach dem Produkthaftungsgesetz

Das Produkthaftungsgesetz (ProdHaftG) sieht eine verschuldensunabhängige Haftung des Herstellers für Schäden aus dem Gebrauch oder Verbrauch seines Produkts vor, wenn die Schädigung ihre Ursache in einem Fehler dieser Sache hat.[241]

Der Schadensersatzpflichtige muss Hersteller im Sinne des § 4 ProdHaftG sein. Hersteller ist auch, wer nur einen Teil oder einen Grundstoff des Endprodukts hergestellt hat oder sich durch Kennzeichnung auf dem Produkt als Hersteller ausgibt. Wird das Produkt in den Europäischen Wirtschaftsraum eingeführt, so gilt auch der Importeur als Hersteller. Sollte der Hersteller nicht festgestellt werden können, so haftet der Lieferant dem Kunden. Soweit mehrere Hersteller oder Lieferanten für den Schaden haften, haften sie als Gesamtschuldner nebeneinander.

Der Schaden muss gemäß § 1 Abs. 1 Satz 1 ProdHaftG zudem auf einem Fehler des Produkts beruhen. Ein Fehler liegt dann vor, wenn ein Produkt nicht die erforderliche Sicherheit bietet. Ein Produktfehler liegt vor, wenn das Produkt zum Zeitpunkt des Inverkehrbringens nicht den berechtigten Sicherheitserwartungen der Allgemeinheit entspricht. Damit sind Konstruktionsfehler, Fabrikationsfehler und Instruktionsfehler vom Fehlerbegriff des ProdHaftG umfasst, nicht jedoch Produktbeobachtungsfehler[242]:

- Ein Konstruktionsfehler liegt vor, wenn bei der Planung des Produkts gegen technische Erkenntnisse verstoßen wird. Der Produzent muss alle zumutbaren Vorkehrungen treffen, um Konstruktionsfehler zu vermeiden, und zu diesem Zweck alle ihm zugänglichen technischen und wirtschaftlichen Erkenntnisse und Möglichkeiten ausnutzen und alle technisch möglichen Sicherheitsvorkehrungen treffen.
- Der Hersteller hat auch dafür zu sorgen, dass der Produktionsprozess zu einem sicheren Produkt führt und dass keine Fertigungsfehler diese Sicherheit beeinträchtigen. Um solche sog. Fabrikationsfehler zu vermeiden, muss die Fertigungsanlage regelmäßig überprüft und an den Stand der Technik angepasst werden.
- Instruktionsfehler entstehen durch fehlerhafte Gebrauchsanweisungen oder nicht ausreichende Warnungen vor bestimmten Eigenschaften des Produkts. Der BGH hat hierzu den Grundsatz aufgestellt, dass der Hersteller immer dann, wenn bei der Anwendung oder Verwendung des von ihm hergestellten Produkts mit einer Schädigung der Verwender zu rechnen ist, dafür sorgen muss, dass eine ausreichende Belehrung der Nutzer über mögliche Gefahrenquellen und die Grenzen der Produktanwendung vorge-

[241] § 1 Abs. 1 Satz 1 ProdHaftG.

[242] Ein Produktbeobachtungsfehler liegt vor, wenn der Hersteller seiner Produktbeobachtungspflicht (siehe Abschnitt 5.4.2), d.h. ein Beobachten des Produkts auf Fehler, die erst nach dem Inverkehrbringen auftreten, nicht oder nur unzureichend nachgekommen ist.

nommen wird. [243] Dabei sind Inhalt und Umfang der Instruktionen nach der am wenigsten informierten Nutzergruppe und damit nach der am meisten gefährdeten Nutzergruppe auszurichten.[244]

Da ein Verschulden des Herstellers nach dem Produkthaftungsgesetz keine Haftungsvoraussetzung ist, hat der Hersteller nicht die Möglichkeit, sich zu exkulpieren, wie dies § 831 Abs. 1 Satz 2 BGB für die deliktische Haftung grundsätzlich vorsieht. Dem Geschädigten wird jedoch nach den §§ 7 ff. ProdHaftG allein der materielle Schaden an anderen Schutzgütern ersetzt, nicht aber die fehlerhafte Sache selbst.

5.4.2 Produzentenhaftung nach den § 823 ff. BGB[245]

Die deliktische Produzentenhaftung nach § 823 Abs. 1 und 2 BGB knüpft an die schuldhafte Verletzung der Verkehrssicherungspflichten des Produzenten an, die von der Rechtsprechung entwickelt worden sind. Die haftungsbegründende Handlung des Herstellers oder Händlers ist das Inverkehrbringen eines fehlerhaften Produkts. Da der Fehlerbegriff dem des § 3 ProdHaftG entspricht, greifen im Wesentlichen dieselben Verkehrssicherungspflichten bzw. Fehlerkategorien wie im ProdHaftG, so dass sich auch hier die Frage nach Konstruktions-, Fabrikations- und Instruktionsfehlern stellt.[246] Hinzu kommt eine Produktbeobachtungspflicht.

Die deliktische Haftung ist im Gegensatz zur Haftung nach dem ProdHaftG jedoch verschuldensabhängig. Zugleich bestehen jedoch erleichterte Beweislastregeln für den Verbraucher.[247]

Alle Personen, die bei der Entstehung eines Fehlers ursächlich und schuldhaft beteiligt sind, haften als Gesamtschuldner. Daher beschränken sich Ersatzansprüche aus der Produkthaftung nicht auf den Hersteller des schadensstiftenden Produkts. Vielmehr können sie sich gegen jeden richten, der im Produktionsbereich eine Verkehrssicherungspflicht verletzt. Mithin ist für die Haftung im Einzelfall entscheidend, welche Organisations- und Kontrollpflichten jedem der an der Produktion oder am Inverkehrbringen des fehlerhaften Produkts Beteiligten obliegen.

---

[243] BGH NJW 86, 1863.

[244] Sprau, in: Palandt (Hrsg.), Bürgerliches Gesetzbuch (BGB), 69. Auflage, 2010, § 3 ProdHaftG Rn. 11.

[245] Gemäß § 15 Abs. 2 ProdHaftG bleibt die Haftung aufgrund anderer Vorschriften unberührt.

[246] Sprau, in: Palandt (Hrsg.), Bürgerliches Gesetzbuch (BGB), 69. Auflage, 2010, § 823 Rn. 166.

[247] Littbarski, in: Kilian / Heussen (Hrsg.), Computerrechts-Handbuch, Ergänzungslieferung 2009, Produkthaftung, Rn. 6.

5.4.3 Produkthaftung: Ergebnisse und offene Fragen

Für die Einführung und den Einsatz von AAL-Technik und -Dienstleistungen ist im Zusammenhang mit dem bestehenden Produkthaftungsrecht größtmögliche Rechtssicherheit für die Hersteller und die Anbieter erforderlich. Da sich AAL-Systeme in der Regel durch eine große Komplexität und eine Vielzahl Beteiligter auszeichnen, stellt sich insbesondere die Frage der Haftung bei mehreren Beteiligten im Innenverhältnis. Auch der jeweilige Umfang der Verkehrssicherungspflichten sollte festgelegt und den beteiligten Herstellern und Dienstleistern verdeutlicht werden. In diesem Zusammenhang wäre z.B. die Frage zu klären, inwieweit spezifisch auf die Gruppe der AAL-Nutzer eingegangen werden muss. Verwandt sind die praktischen Fragen, wie sich Instruktionsfehler vermeiden lassen, also die Gruppe der AAL-Nutzer befähigt wird, die eingesetzten AAL-Systeme sicher zu verwenden.

5.5 Arzthaftung

Der Bereich der ärztlichen Haftung ist primär durch eine Vielzahl maßgeblicher Gerichtsurteile geformt. Im Folgenden werden zunächst die Haftungsgrundlagen erläutert (siehe Abschnitt 5.5.1). Als haftungsrelevant könnten sich insbesondere Pflichtverletzungen im vertraglichen Bereich (siehe Abschnitt 5.5.2) oder die unzulänglich geprüfte Verwendung von Daten aus AAL-Systemen (siehe Abschnitt 5.5.3) erweisen. Anschließend führt Abschnitt 5.5.4 die Ergebnisse und offenen Fragen zusammen.

5.5.1 Haftungsgrundlagen

Im Bereich der ärztlichen Haftung hat sich ein breites, im Wesentlichen von der Judikatur beherrschtes Rechtsgebiet entwickelt. Besondere gesetzliche Regelungen zur Arzthaftung bestehen nicht. Vielmehr ist auf die allgemeinen zivilrechtlichen Haftungsregelungen des Vertrags- und Deliktsrechts zurückzugreifen. Neben Ansprüchen aus dem Behandlungsvertrag bzw. der Verletzung von vertraglichen (Neben-)Pflichten kommen Ansprüche aus § 823 BGB in Betracht. In der Praxis gleichen sich die vertraglichen und deliktischen Ansprüche hinsichtlich ihrer Voraussetzungen und Rechtsfolgen weitgehend, insbesondere seit mit der Schuldrechtsreform im Jahr 2002 Verjährungsfristen vereinheitlicht wurden und Ersatz immaterieller Schäden („Schmerzensgeld“) auch im Rahmen einer vertraglichen Haftung verlangt werden kann, § 253 Abs. 2 BGB.[248] Die unterschiedlichen Haftungsgrundlagen führen allerdings zu abweichenden Ergebnissen, soweit für ein Verschulden Dritter im Deliktsrecht – anders als bei vertraglichen Ansprüchen – aufgrund ordnungsgemäßer Auswahl und Überwachung eine Exkulpation nach § 831 BGB möglich ist.

[248] Bergmann, Arzthaftung, S. 7; Quaas / Zuck, § 13 Rn. 60 f.

Die Haftungsvoraussetzungen im ärztlichen Bereich entsprechen den allgemeinen aus dem Zivilrecht bekannten Tatbeständen:

- Der Patient muss einen Schaden an einem geschützten Rechtsgut erlitten haben (namentlich seiner Gesundheit),
- der Arzt muss einen Fehler oder eine Pflichtverletzung begangen haben,
- dieser Fehler ist kausal für den Schaden, und
- den Arzt trifft ein objektives Verschulden.

Bezüglich des Vorliegens eines Schadens an der Gesundheit des Patienten sind Besonderheiten beim Einsatz von AAL-Systemen nicht erkennbar. Beeinträchtigungen des allgemeinen Persönlichkeitsrechts bzw. des Rechts auf informationelle Selbstbestimmung wurden bereits bei den datenschutzrechtlichen Erörterungen behandelt (siehe Abschnitt 5.2).

Hinsichtlich denkbarer Fehler ist der Einsatz von AAL-Systemen näher zu betrachten. Ob ein konkretes Verhalten als fehlerhaft zu bewerten ist, hängt maßgeblich auch von dem zugrundeliegenden Pflichtenmaßstab ab. Ärzte haben bei ihrem Tun den medizinischen Standard einzuhalten.[249] Dieser richtet sich danach, wie ein besonnener und gewissenhafter Arzt handeln würde.[250] Eine Nachlässigkeit oder Unsitte, die sich allgemein im Verkehr eingenistet hat, ist nicht zugunsten des Arztes zu berücksichtigen.[251]

In Bezug auf den Einsatz von Informationstechnik gilt, dass diese einzusetzen ist, soweit dies dem medizinischen Standard entspricht, was umso eher anzunehmen ist, als deren Einsatz Diagnosefehler verhindern kann oder auf weitere erforderliche Diagnosemaßnahmen hinzuweisen im Stande ist.[252] Ist eine bessere oder modernere Ausstattung als der medizinische Standard vorhanden, ist diese zu verwenden, wenn dadurch die Heilungschancen verbessert oder unerwünschte Nebenwirkungen verhindert werden können.[253] Fehlt es an der erforderlichen Ausstattung und würde ein sorgfältiger und gewissenhafter Arzt die Behandlung angesichts fehlender Therapiemöglichkeiten ablehnen, kann die Pflicht bestehen, den Patienten an eine besser ausgestattete Einrichtung zu überweisen.[254]

Zur weiteren Beurteilung des Vorliegens eines Fehlers werden im Rahmen des Übernahmeverschuldens Fälle diskutiert, bei denen ein Arzt die Behandlung übernimmt, obwohl er vor der Behandlung erkennen musste, dass bei ihm die apparativen, organisatorischen oder

[249] Sprau, in: Palandt (Hrsg.), Bürgerliches Gesetzbuch (BGB), 69. Auflage, 2010, § 823 Rn. 147.

[250] BGH, NJW 1989, 2321, 2322.

[251] Taupitz, in: ÄB 2010, 1720.

[252] Taupitz, in: ÄB 2010, 1720, 1721.

[253] BGH, NJW 1988, 2949, 2950.

[254] BGH, NJW 1989, 2321, 2322.

fachlichen Voraussetzungen für die Behandlung nicht gegeben sind.[255] Bei AAL-Systemen ist dabei insbesondere sicherzustellen, dass der Arzt selbst die nötigen Einrichtungen besitzt, um mit den Systemen seiner Patienten zu kommunizieren, und diese Apparate hinreichend beherrscht.

5.5.2 Pflichtverletzungen im vertraglichen Bereich

Haftungsträchtig erscheinen im Bereich der vertraglichen Haftung insbesondere die vielfältigen denkbaren Nebenpflichten, die einen Arzt treffen können. Relevant ist zudem die Abgrenzung von Pflichten, die ausdrücklich vertraglich übernommen werden müssen. Hier stellen sich zwei Herausforderungen:

- Katalogisierung der sich möglicherweise ergebenden Pflichten im Rahmen einer eingehenden Analyse bestehender und geplanter AAL-Systeme unter Betrachtung der Besonderheiten der An- und Einbindung des Arztes an das konkrete System,
- Ermittlung des Umfangs, in dem die identifizierten Pflichten Ärzte oder andere an AAL-Systemen teilnehmende Heilberufler treffen.

Dabei sollte eine ausufernde Verpflichtung von Heilberuflern vermieden werden, soweit diese nicht ausdrücklich als vertragliche Haupt- oder Nebenpflicht übernommen wird. Zu den klärungsbedürftigen Fragen gehört insbesondere, in welchem Umfang und wie schnell auf eine durch ein AAL-System verursachte Meldung reagiert werden muss. Dabei ist zu berücksichtigen, dass es sich gerade nicht um ein vom Verpflichteten selbst bereitgestelltes und betriebenes Gerät handelt, sondern dieses – je nach Geschäftsmodell – von den Patienten selbst angeschafft und betrieben oder von Drittanbietern bereitgestellt wird.

Gegenwärtig im Fluss ist die Frage der Geschäftsmodelle, mit denen AAL-Systeme finanziert werden. Dies hat wesentlichen Einfluss auf die Bereitstellung der Systeme. Werden diese z.B. Teil des Leistungsspektrums gesetzlicher Krankenkassen, läge eine enge An- und Einbindung der Vertragsärzte näher als bei privat durch die Nutzer angeschafften und betriebenen Systemen.

5.5.3 Verwendung von Daten aus AAL-Systemen

Mit AAL-Systemen erhalten Patienten weit umfangreichere Möglichkeiten als bisher, selbst die Gesundheit und den Vitalstatus betreffende Daten zu erheben und zu speichern. Dies wirf die Frage auf, in welchem Umfang ein Arzt diese Informationen zur Diagnose nutzen darf oder gar muss. Für den Arzt ist dabei wichtig zu erfahren, ob die Geräte hinreichend geeicht und korrekt eingesetzt wurden. Für Systeme, die insbesondere für einen Einsatz im Gesundheitsbereich gedacht sind, könnte sich jedoch diese Frage angesichts der Anforde-

[255] Quaas / Zuck, § 13 Rn. 74.

rungen des Medizinproduktgesetzes (siehe Abschnitt 5.3) relativieren. Selbst wenn diese Voraussetzungen gegeben sind, darf ein Arzt nicht blind auf Messergebnisse vertrauen.[256] Jedenfalls könnten Messergebnisse von AAL-Systemen Anhaltspunkte für eine weiterführende Diagnostik seitens des Arztes begründen oder dessen eigene Diagnostik ergänzen.

Eine praktische Frage ergibt sich schließlich aus dem vertragsärztlichen Vergütungssystem, das gegenwärtig keine besonderen Vergütungstatbestände für zeitintensive und potenziell haftungsträchtige Auswertungen von Daten aus AAL-Systemen vorsieht.

5.5.4 Arzthaftung: Ergebnisse und offene Fragen

Ob die Einführung von AAL-Systemen zu einer erweiterten Haftung für Ärzte führt, hängt von den Geschäftsmodellen und der Einbindung der Ärzte in diese Systeme ab. Pflichten sollten dabei hinreichend klar im Vorwege definiert werden. Dies könnte vertraglich zwischen Arzt und Patient bzw. Anbieter oder als eindeutig beschriebener Teil einer Leistung nach dem GKV-Leistungskatalog geschehen.

Durch AAL-Systeme erhobene und vom Patienten bereitgestellte Daten und Messwerte dürfen nicht blindlings und ohne Kontrolle vom Arzt übernommen werden. Eine offene Frage besteht darin, wie der Arzt Fehlfunktionen der AAL-Systeme oder gar Manipulationen durch den Patienten oder durch Dritte an den Daten erkennen kann.

5.6 Ergebnisse und offene Fragen

Der Bereich des Haftungsrechts ist durch allgemeine Rechtsnormen dominiert, die für potenzielle Schadensfälle überwiegend angemessene Haftungsgrundlagen darstellen. Im Bereich des Datenschutzrechts könnte seitens des Gesetzgebers erwogen werden, die nach der europäischen Datenschutzrichtlinie 95/46/EG mögliche verschuldensunabhängige Haftung konsequent umzusetzen oder zumindest Beweiserleichterungen zugunsten der Betroffenen einzuführen. Hersteller und Anbieter werden durch die für Medizinprodukte geltenden Regelungen vor Herausforderungen gestellt. Dieser europarechtlich geprägte Regelungsbereich ist bisher auf typische medizinische Gerätschaften ausgelegt. Die Anwendung einzelner ursprünglich nicht für den medizinischen Einsatz gedachter Komponenten führt zu offenen Abgrenzungsfragen.

Die Haftung für Ärzte im Rahmen der von ihnen übernommenen Behandlung ist bereits hinlänglich geregelt. Im AAL-Bereich ist jedoch für jedes Behandlungsverhältnis zu klären, in welchem Umfang der Arzt eigene Pflichten dahingehend übernimmt, z.B. auf von AAL-Systemen gemeldete Ereignisse zu reagieren. Bei von Patienten bereitgestellten Daten aus AAL-Systemen hat der Arzt mögliche Fehlerquellen der von den Patienten erhobenen Daten

[256] Taupitz, in: ÄB 2010, 1720, 1221.

zu berücksichtigen und erforderlichenfalls eigene Messungen oder Untersuchungen durchzuführen.

6 Sozialversicherungsrechtliche Anforderungen und Fragestellungen

Für Informationstechnik und Dienstleistungen im AAL-Bereich, die der medizinischen Versorgung oder Pflege dienen, stellt sich in absehbarer Zeit die Frage, ob und für welche dieser AAL-Systeme und -Dienstleistungen die Kosten durch die Krankenkassen (und Pflegekassen) übernommen werden können. Diese Entscheidung ist diskriminierungsfrei zu treffen, so dass weder bestimmte Hersteller noch Patientengruppen bevorzugt werden. In Betracht kommt eine Einführung und Kostenübernahme einer AAL-Technik als Hilfsmittel (siehe Abschnitt 6.1). Daneben stellt sich die Frage der Abrechnungsfähigkeit des Einsatzes oder der Erbringung von AAL-Dienstleistungen im Zusammenhang mit einer ärztlichen Behandlung oder Dienstleistung (siehe Abschnitt 6.2). Abschnitt 6.3 fasst die Ergebnisse und offenen Fragen zusammen.

6.1 Einführung von AAL-Technik als Hilfsmittel

Abschnitt 6.1.1 erörtert, inwieweit AAL-Technik als Hilfsmittel gem. § 31 Abs. 1 SGB IX anzusehen ist. Der folgende Abschnitt 6.1.2 geht auf den Anspruch des Patienten auf Hilfsmittel ein.

6.1.1 AAL-Technik als Hilfsmittel

Nach § 27 Abs. 1 Satz 2 Nr. 3 SGB V umfasst die Krankenbehandlung auch die Versorgung mit Arznei-, Verband-, Heil- und Hilfsmitteln. Dabei haben die Versicherten gem. § 33 Abs. 1 SGB V einen Anspruch auf Versorgung mit Hilfsmitteln, die im Einzelfall erforderlich sind, um den Erfolg der Krankenbehandlung zu sichern, einer drohenden Behinderung vorzubeugen oder eine Behinderung auszugleichen, soweit die Hilfsmittel nicht als allgemeine Gebrauchsgegenstände des täglichen Lebens anzusehen sind.

Der Begriff „Hilfsmittel“ wird in § 31 Abs. 1 SGB IX dahingehend konkretisiert, dass es sich um technische Hilfen handelt, die von den Leistungsempfängern getragen, mitgeführt oder bei einem Wohnungswechsel mitgenommen werden können und unter Berücksichtigung der Umstände des Einzelfalls erforderlich sind. Ein Hilfsmittel muss nicht zwingend auf den Körper des Versicherten einwirken; es dient auch dann der Sicherung der ärztlichen Behandlung, wenn es die häusliche Behandlung durch eine Hilfsperson ermöglicht oder erheblich erleichtert.[257] Dabei ist die Krankenkasse zuständig für Maßnahmen, die nur bei der medizinischen Bekämpfung der Krankheit oder der Behinderung selbst ansetzen, nicht aber bei deren Folgen auf beruflichem, gesellschaftlichem oder privatem Gebiet. Das Wirtschaftlich-

[257] Wagner, in: Krauskopf (Hrsg.), Soziale Krankenversicherung, Pflegeversicherung, 69. Ergänzungslieferung, 2010, § 33 Rn. 7.

keitsgebot schließt außerdem die Leistungspflicht für solche Innovationen gegenüber einem noch voll funktionsfähigen Hilfsmittel aus, die nicht die Funktionalität, sondern in erster Linie Bequemlichkeit und Komfort bei der Nutzung betreffen.[258]

Hilfsmittel sind auch Geräte, die der Versicherte für die angeordnete Selbstüberwachung der Behandlungsbedürftigkeit einer Dauererkrankung benötigt.[259] Mithin fallen auch Geräte darunter, die den Erfolg einer Heilbehandlung bei Anwendung durch den Versicherten selbst sicherstellen sollen. Gegenstände mit Doppelfunktion, die Gebrauchsgegenstand und Hilfsmittel sind, verbleiben in der Leistungspflicht der GKV, wenn der auf die Hilfsmittelfunktion entfallende Teil der Herstellungskosten überwiegt.[260]

AAL-Systeme, die im medizinischen und pflegerischen Bereich zum Einsatz kommen bzw. kommen sollen, sind grundsätzlich geeignet, die Krankenbehandlung zu begleiten und deren Erfolg zu sichern. Monitoringsysteme z.B. werden gerade mit diesem Ziel eingesetzt. Auf der anderen Seite werden AAL-Systeme verwendet, um drohenden Behinderungen vorzubeugen und bestehende Behinderungen auszugleichen, wie Technik (z.B. Sensorik) zur Sturzprävention sowie Unfallprävention. Es zeigt sich, dass AAL-Systeme ganz oder teilweise in vielen Fällen als Hilfsmittel eingestuft werden können.

6.1.2 Anspruch des Patienten auf Hilfsmittel

Versicherte haben Anspruch auf Hilfsmittel nach § 33 SGB V i.V.m. §§ 2, 12 und 70 SGB V.[261] Nach dem Wirtschaftlichkeitsgebot des § 12 SGB V sind Leistungen nur erstattungsfähig, wenn sie ausreichend, zweckmäßig und wirtschaftlich sind; sie dürfen das Maß des Notwendigen nicht überschreiten.[262]

Bedeutung kommt insofern dem von den Spitzenverbänden aufgestellten Hilfsmittelverzeichnis zu. Das nach § 139 Abs. 1 SGB V zu erstellende Hilfsmittelverzeichnis des Spitzenverbandes der Krankenkassen ist zwar für die Krankenkassen nur eine unverbindliche Ausle-

---

[258] Wagner, in: Krauskopf (Hrsg.), Soziale Krankenversicherung, Pflegeversicherung, 69. Ergänzungslieferung, 2010, § 33 Rn. 7; BSG 06.06.2002, SozR 3-2500.

[259] Wagner, in: Krauskopf (Hrsg.), Soziale Krankenversicherung, Pflegeversicherung, 69. Ergänzungslieferung, 2010, § 33 Rn. 7.

[260] Wagner, in: Krauskopf (Hrsg.), Soziale Krankenversicherung, Pflegeversicherung, 69. Ergänzungslieferung, 2010, § 33 Rn. 15.

[261] Gemäß § 2 Abs. 1 Satz 3 SGB V haben die gesetzlichen Krankenkassen den medizinischen Fortschritt entsprechend dem Stand der Wissenschaft zu berücksichtigen. Hierdurch ist auch eine fortlaufende Anpassung des Leistungsspektrums der GKV gefordert. Auch das Wirtschaftlichkeitsgebot nach § 12 SGB V dürfte den Einsatz von AAL-Anwendungen befördern unter der Voraussetzung, dass diese als medizinisch notwendig anzusehen sind und der zusätzliche Aufwand beim Arzt einen zusätzlichen Nutzen für den Patienten bedeutet.

[262] § 12 Abs. 1 Satz 1 und 2 SGB V.

gungshilfe, bietet aber Anhaltspunkte für eine gleichmäßige Behandlung der Versicherten.[263] Das Hilfsmittelverzeichnis hat sich seit der Einführung 1989 zur „Quasi-Positivliste“ entwickelt[264] und entfaltet eine starke marktsteuernde Wirkung.

Neben dem Hilfsmittelverzeichnis erfolgt eine Regulierung des Marktes für Hilfsmittel durch die Heil- und Hilfsmittelrichtlinien des Gemeinsamen Bundesausschusses (GBA). In der Hilfsmittel-Richtlinie[265] des GBA sind die Voraussetzungen für die Verordnung von Hilfsmitteln geregelt. Danach können Hilfsmittel nur zu Lasten der Krankenkasse verordnet werden, wenn sie notwendig sind,

- den Erfolg der Krankenbehandlung zu sichern oder eine Behinderung auszugleichen,
- eine Schwächung der Gesundheit, die in absehbarer Zeit voraussichtlich zu einer Krankheit führen würde, zu beseitigen,
- einer Gefährdung der gesundheitlichen Entwicklung eines Kindes entgegenzuwirken oder
- Pflegebedürftigkeit zu vermeiden oder zu mindern.[266]

Durch die Richtlinie erfolgt danach eine formale Einschränkung der Verordnungen auf medizinisch notwendige Tatbestände.

6.2 Vergütung von ärztlichen AAL-Dienstleistungen

Neben der möglichen Einstufung von AAL-Systemen als Hilfsmittel und der Aufnahme in das Hilfsmittelverzeichnis ist für die Betrachtung einer Bezahlung ein Blick auf Vergütungsmöglichkeiten ärztlicher Dienstleistungen im AAL-Bereich zu werden. Die Grundlagen werden in Abschnitt 6.2.1 vorgestellt. Abschnitt 6.2.2 beschreibt die persönliche Leistungserbringungspflicht, während Abschnitt 6.2.3 die mögliche Einführung neuer Leistungen durch den Gemeinsamen Bundesausschuss untersucht.

---

[263] Wagner, in: Krauskopf (Hrsg.), Soziale Krankenversicherung, Pflegeversicherung, 69. Ergänzungslieferung, 2010, § 33 Rn. 24.

[264] Das Hilfsmittelverzeichnis hat sich seit der Einführung 1989 zur ‚Quasi-Positivliste’ mit marktsteuernder Wirkung entwickelt, so Frau Piossek, Leiterin des Bereichs „Krankenversicherung“ des BVMed, Statement abrufbar unter: http://www.bvmed.de/themen/CE-Kennzeichnung/pressemitteilung/BVMed-Konferenz_zum_Hilfsmittelverzeichnis_mit_IKK_und_MDS_am_14._Juni_2005.html.

[265] Richtlinie des Gemeinsamen Bundesausschusses über die Verordnung von Hilfsmitteln in der vertragsärztlichen Versorgung (Hilfsmittel-Richtlinie/HilfsM-RL) in der Neufassung vom 16. Oktober 2008, veröffentlicht im Bundesanzeiger 2009, Nr. 61 S. 462, in Kraft getreten am 7. Februar 2009.

[266] Richtlinie des Gemeinsamen Bundesausschusses über die Verordnung von Hilfsmittel in der vertragsärztlichen Versorgung, Neufassung vom 16.10.2008, abrufbar unter: http://www.g-ba.de/downloads/62-492-309/RL-Hilfsmittel-Neufassung-2008-10-16.pdf.

6.2.1 Einheitlicher Bewertungsmaßstab und Gebührenordnung

Bei einer Leistungserbringung gegenüber einem Versicherten der GKV wird der Katalog möglicher Leistungen durch den einheitlichen Bewertungsmaßstab (EBM) abschließend vorgegeben, § 87 Abs. 2 Satz 1 SGB V.[267] Der EBM wird auf Bundesebene zwischen der Kassenärztlichen Bundesvereinigung und den Spitzenverbänden der Krankenkassen durch Bewertungsausschüsse vereinbart. Leistungen, die im EBM nicht verzeichnet sind, können vom Kassenpatienten nicht beansprucht werden und dürfen vom Arzt nicht zu Lasten der GKV abgerechnet werden.

Die Abrechnung ärztlicher Leistungen gegenüber Privatversicherten erfolgt nach der Gebührenordnung für Ärzte (GOÄ). Neue Dienstleistungen im Zusammenhang mit der AAL-Technik sind bisher nicht in die Gebührenordnung aufgenommen.[268]

6.2.2 Persönliche Leistungserbringungspflicht

Ärzte sind nach § 28 SGB V grundsätzlich zur persönlichen Leistungserbringung verpflichtet.[269] So darf der Arzt gem. § 19 (Muster-)Berufsordnung für die deutschen Ärztinnen und Ärzte (MBO-Ä) nur für selbstständig erbrachte Leistungen Gebühren berechnen. Zwar heißt dies nicht, dass jeder einzelne Behandlungsschritt persönlich erbracht werden muss; dies gilt jedoch für diejenigen Schritte, die zum unverzichtbaren Kern der Behandlung gehören. Eine Aufgabenteilung durch mehrere Ärzte im Rahmen eines Leistungssplittings ist nach deutschem Recht nicht möglich und dementsprechend auch nicht abrechnungsfähig.[270]

6.2.3 Einführung neuer Leistungen durch den Gemeinsamen Bundesausschuss

Neue Untersuchungs- und Behandlungsmethoden dürfen grundsätzlich erst zu Lasten der Krankenkassen in der vertragsärztlichen Versorgung angewandt werden, wenn sie explizit vom GBA als verordnungsfähig zugelassen worden sind. § 135 Abs. 1 SGB V bestimmt diesbezüglich, dass neue Untersuchungs- und Behandlungsmethoden in der vertragsärztlichen und vertragszahnärztlichen Versorgung zu Lasten der Krankenkassen nur erbracht

---

[267] Auf das Abrechnungssystem im stationären Sektor (Diagnosis Related Groups – DRG) wird nicht gesondert eingegangen.

[268] Dierks, in: Dierks / Nitz / Grau (Hrsg.), Gesundheitstelematik und Recht, 2003, S. 150: Zwar ist u.U. eine Abrechnung nach der sog. Analogberechnung möglich; jedoch wird auch hier zur Rechtssicherheit eine Novellierung der Gebührenordnung empfohlen.

[269] Vgl. § 28 SGB V. Dieser Grundsatz muss im Vertragsrecht als auch im Rahmen stationärer Behandlung durch selbstliquidierende Ärzte beachtet werden, vgl. Voigt, Rechtsgutachten Telemedizin – Rechtliche Problemfelder sowie Lösungsvorschläge, S. 22.

[270] Voigt, Rechtsgutachten Telemedizin – Rechtliche Problemfelder sowie Lösungsvorschläge, S. 23. Einzige Ausnahme: § 15 Abs. 3 MBV-A: Vertragsärzte dürfen sich bei gerätebezogenen Untersuchungsleistungen zur gemeinschaftlichen Leistungserbringung unter den dort genannten Voraussetzungen zusammenschließen.

werden dürfen, wenn der GBA auf Antrag eines Unparteiischen nach § 91 Abs. 2 Satz 1 SGB V, einer Kassenärztlichen Bundesvereinigung, einer Kassenärztlichen Vereinigung oder des Spitzenverbandes Bund der Krankenkassen in Richtlinien nach § 92 Abs. 1 Satz 2 Nr. 5 SGB V Empfehlungen abgegeben hat über

- die Anerkennung des diagnostischen und therapeutischen Nutzens der neuen Methode sowie deren medizinischer Notwendigkeit und Wirtschaftlichkeit – auch im Vergleich zu bereits zu Lasten der Krankenkassen erbrachten Methoden – nach dem jeweiligen Stand der wissenschaftlichen Erkenntnisse in der jeweiligen Therapierichtung,
- die notwendige Qualifikation der Ärzte, die apparativen Anforderungen sowie Anforderungen an Maßnahmen der Qualitätssicherung, um eine sachgerechte Anwendung der neuen Methode zu sichern, und
- die erforderlichen Aufzeichnungen über die ärztliche Behandlung.

Nach dem Beschluss des GBA ist eine Umsetzung des Beschlusses in den EBM notwendig.

6.3 Ergebnisse und offene Fragen

Soll AAL-Technik in das Gesundheitssystem integriert werden, so muss dies auch im Bereich der Vergütung erfolgen. Die Vergütungsregeln in dem EBM[271] und der GOÄ[272] sollten daher so geändert werden, dass AAL-Systeme oder AAL-Anwendungen mitberücksichtigt werden, wo eine angemessene Vergütung fehlt.[273] Dabei ist zu klären, inwieweit ein abrechenbares Leistungssplitting der Dienstleistungen mehrerer Ärzte eingeführt werden sollte. Die selbstständige, persönliche und damit alleinige Leistungserbringung des Arztes im Rahmen einer Behandlung erscheint im AAL-Bereich nicht mehr angemessen.

[271] Verzeichnis, nach dem vertragsärztlich erbrachte, ambulante Leistungen der gesetzlichen Krankenversicherung abgerechnet werden. Es handelt sich somit um ein Vergütungssystem der ambulanten Versorgung in Deutschland.

[272] Die Gebührenordnung für Ärzte (GOÄ) regelt die Abrechnung aller medizinischen Leistungen außerhalb der gesetzlichen Krankenversicherung.

[273] Die Einführung von AAL-Systemen und -Dienstleistungen im stationären Sektor ist einfacher, da von Grundsatz jede Innovation auch für Kassenpatienten angewendet werden kann, solange der GBA diese nicht ausgeschlossen hat. Bezüglich der Abrechnungsfähigkeit gilt jedoch auch hier, dass eine Anpassung der Vergütungsvorgaben erforderlich ist. Vgl. dazu: Neumann / Hagen / Schönermark, Regulation der Aufnahme von innovativen nichtmedikamentösen Technologien in den Leistungskatalog solidarisch finanzierter Kostenträger, 2007, S. 40, abrufbar unter: http://portal.dimdi.de/de/hta/hta_berichte/hta210_bericht_de.pdf.

7 Delegation von Entscheidungen an AAL-Systeme

AAL-Systeme werden als Assistenz für ihre Nutzer konzipiert. „Assistenz“ kann je nach Lebenssituation Verschiedenes bedeuten: Bisher wurden Hilfestellungen durch Menschen erbracht. Vielleicht nimmt künftig ein AAL-System dem Betroffenen nicht nur einfache Haushaltstätigkeiten ab, sondern es präsentiert auch ausgewählte Informationen zur Vorbereitung von Entscheidungen, oder es agiert künftig sogar im Namen des Nutzers oder Dritten. Die rechtlichen Anforderungen einer Delegation von Entscheidungen an einen Menschen bleiben überschaubar (siehe Abschnitt 7.1). Sobald aber ein Assistenzsystem Einfluss auf Entscheidungen des Nutzers nimmt, wirkt es auf dessen Willensbildungsprozess ein. Letztlich ist entscheidend, dass die Tätigkeit des Systems transparent (siehe Abschnitt 7.2) ist, der Nutzer die Hoheit über die Entscheidungen (siehe Abschnitt 7.3) behält und die Interessen des Rechtsverkehrs hinsichtlich der Wirksamkeit der Erklärungen sichergestellt sind (siehe Abschnitt 7.4). Ergebnisse und offene Fragen finden sich in Abschnitt 7.5.

Nachfolgend wird für Aktionen von AAL-Systemen der Begriff des Tätigwerdens verwendet. Der Begriff „Handlung“ ist in der rechtlichen Terminologie bereits belegt. Zivilrechtlich sind juristische Handlungen als vom natürlichen Willen getragenes Verhalten definiert.[274] Im Strafrecht ist regelmäßig relevant, ob mehrere Handlungen eine Handlungseinheit bilden. Kleinstes Element ist dabei die Handlung im natürlichen Sinn, welche als Willensentschluss, der eine Körperbewegung hervorgerufen hat, definiert wird.[275] AAL-Systeme bringen jedoch gerade keine von einer (menschlichen) Willensentscheidung getragenes Verhalten hervor, so dass im Folgenden der Begriff der Tätigkeit verwendet wird. Soweit AAL-Systeme im Rechtsverkehr kommunizieren, soll von Erklärungen gesprochen werden, ohne diesen damit die Qualität einer Willenserklärung beizumessen.

7.1 Delegation an einen menschlichen Vertreter

Eine Delegation an einen menschlichen Vertreter ist in der bestehenden Rechtsordnung hinreichend abgebildet und wirft keine besonderen Rechtsfragen auf. Insoweit stellen die Regelungen der §§ 164 ff. BGB ein abgeschlossenes System einschließlich der Regelungen zur Haftungsverteilung für die gewillkürte Stellvertretung dar und werden durch die Regelungen der gesetzlichen Stellvertretung für Minderjährige und Betreute ergänzt. Die Frage der Vertretung durch einen selbst gewählten Vertreter bei einer datenschutzrechtlichen Einwilligung bzw. zur Wahrnehmung datenschutzrechtlicher Ansprüche wurde bereits für den Fall der datenschutzrechtlichen Einwilligung diskutiert; eine Änderung der noch in Teilen der Rechtsprechung und Lehre bestehenden Rechtsauffassung wurde angeregt (siehe Abschnitt 3.3.2.2.1).

---

[274] Schack, BGB AT, Rn. 53.

[275] Schönke / Schröder, vor § 52 ff. StGB Rn. 10; Lackner / Kühl, vor § 52 ff. StGB Rn. 3.

7.2 Transparenz als grundlegende Anforderung

Werden AAL-Systeme im Namen des Betroffenen tätig, müssen die hinterlegten Entscheidungsgrundlagen und, soweit möglich, auch die dahinterliegenden Algorithmen so transparent wie möglich ausgestaltet werden. Diese Anforderung ist nicht trivial: Bereits das Ausblenden von vermeintlich unwichtigen Informationen bei einer Suchanfrage wird mit großer Wahrscheinlichkeit Nutzerentscheidungen beeinflussen. Doch ein ungefiltertes Darstellen aller irgendwie im Zusammenhang stehenden Informationen ist ebenfalls nicht zielführend und bringt im Gegenteil gerade keine Hilfestellung und Assistenz für den Nutzer.

Allerdings ist die Transparenz eine wesentliche Voraussetzung, um den Nutzer überhaupt in die Lage zu versetzen, das System zumindest in einem gewissen Umfang zu kontrollieren bzw. die Übersicht über dessen Tätigwerden zu behalten.[276] Dies ist nicht zuletzt zwingend erforderlich, um die Verantwortlichkeit für das Tätigwerden des Systems übernehmen zu können und an vom System herbeigeführte Rechtsfolgen (z.B. bei durch das System aufgegebenen Bestellungen) gebunden zu sein. Dabei ist ein Zuviel an Information ebenso schädlich wie ein Vorenthalten oder Kürzen derselben. Eine auch für den Bereich von AAL-Systemen übertragbare Lösung dieses Dilemmas kann die für Datenschutzerklärungen von der Art. 29-Datenschutzgruppe[277] vorgeschlagene abgestufte Darstellung der Informationen[278] sein. Die Informationen werden dabei so aufgebaut, dass wesentliche, insbesondere kritische und für die Mehrzahl der Betroffenen relevante Informationen in verkürzter Form auf einer obersten Ebene der Benutzungsoberfläche dargestellt werden. Von dort können weitere Ebenen aufgeblättert werden, um die Gesamtheit der Informationen einzusehen. Denkbar sind aber auch andere Varianten, um die vollständigen Informationen für den Nutzer aufzubereiten, z.B. über die Verwendung von Bildern und Icons, um auf wichtige Informationen hinzuweisen, oder über die (zusätzliche) Ausgabe von Meldungen über einen Lautsprecher.

Im Folgenden werden wettbewerbsrechtliche Fragestellungen in Bezug auf Transparenz (siehe Abschnitt 7.2.1) sowie Verbraucherschutzaspekte (siehe Abschnitt 7.2.2) näher beleuchtet.

---

[276] Zu den technischen und juristischen Anforderungen an die Kontrolle von Vertretern u.a. bei der Wahrnehmung des Rechts auf informationelle Selbstbestimmung: Hansen / Raguse / Storf / Zwingelberg, 2010, S. 27 ff.

[277] Nach Art. 29 der Datenschutzrichtlinie 95/46/EC eingerichtete Arbeitsgruppe der Datenschutzbeauftragten der Mitgliedsstaaten und der Gemeinschaftsorgane, online: http://ec.europa.eu/justice/policies/privacy/workinggroup/.

[278] Art. 29-Datenschutzgruppe, Stellungnahme 10/2004 zu einheitlicheren Bestimmungen über Informationspflichten, WP 100, angenommen am 25. November 2004, abrufbar unter: http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2004/wp100_de.pdf.

7.2.1 Transparenz und wettbewerbsrechtliche Fragestellungen

Transparente Prozesse sind förderlich, um wettbewerbsrechtlich fragwürdige Situationen zu verhindern oder zumindest so auszugestalten, dass diese für Dritte bewertbar werden. Eine Verquickung mit Wirtschaftsinteressen des Herstellers oder Betreibers könnte z.B. dazu führen, dass in den Vorschlägen des AAL-Systems bestimmte Produkte bevorzugt werden. Das ist wirtschafts- und wettbewerbsrechtlich und für bestimmte Berufsträger (Ärzte, Apotheker) auch standesrechtlich zu würdigen. So ist zum Schutze des Wettbewerbs untersagt, mittels unsachgemäßer Beeinflussung die Entschließungsfreiheit der Marktteilnehmer zu beeinträchtigen, § 4 Nr. 1 UWG. Schutzzweck der Norm ist dabei, die Rationalität der Entscheidungen im Markt zu schützen. Daneben wird für AAL-Systeme regelmäßig auch § 4 Nr. 2 UWG einschlägig sein. Dieser bezweckt den Schutz von Verbrauchern in besonders schutzwürdigen Situationen wie z.B. geistiger oder körperlicher Gebrechlichkeit, Alter und geschäftliche Unerfahrenheit – mithin typische Szenarien, in denen AAL-Systeme künftig zum Einsatz kommen können.

In beiden Fallgestaltungen, d.h. bei unsachgemäßer Beeinflussung und bei Ausnutzung besonderer Situationen der Betroffenen, sind die Folgen von Beeinflussungen durch Hersteller und Betreiber von AAL-Systemen bereits frühzeitig zu erwägen. Mögliche Gegenmaßnahmen könnten insbesondere in einer Rechtspflicht zur transparenten Gestaltung der Auswahl- und Entscheidungsprozesse liegen. Als technisch zu realisierende Lösung ist eine Anpassung der Auswahlalgorithmen des AAL-Systems an die Gewohnheiten der Nutzer durch einen Lernprozess denkbar, z.B. indem bereits im Haushalt vorhandene Produkte verzeichnet und Entscheidungen der Nutzer in einer Lernphase aufgezeichnet und später fortgeführt werden. Durch die Perpetuierung von Nutzergewohnheiten würde eine Beeinflussung der Entscheidung durch die Hersteller von AAL-Systemen wirksam unterbunden. Daneben müssen den Nutzern allerdings Eingriffsmöglichkeiten vorbehalten sein, um das System an geänderte Umstände wie eine Diät oder andere Vorlieben zu programmieren.

Die Möglichkeit zur Manipulation von Entscheidungen des Systems zugunsten bestimmter Beteiligter wirft die Frage auf, welche Anforderungen an die Vorhersehbarkeit und Transparenz von Entscheidungen bestehen, die AAL-Systeme für die Nutzer treffen sollen. In einem Spannungsverhältnis zu Transparenzforderungen können dabei auch rechtlich schutzwürdige Interessen der Anbieter treten. Anbieter könnten beispielsweise Geschäftsgeheimnisse geltend machen, um nicht die Methodik der Entscheidungsfindung offenzulegen und sich damit vor Nachahmung durch Konkurrenten oder vor illegalen Produktkopien zu schützen.

Auch könnten Hersteller von AAL-Systemen es deren Nutzern schwer machen, die Systeme zu einem späteren Zeitpunkt gegen Konkurrenzprodukte auszutauschen (sog. „Lock-in“). Stimmen Hersteller dagegen ihre Systeme dergestalt aufeinander ab, dass Nutzer zwar zwischen deren Geräten, nicht aber zum Produkt eines Konkurrenten wechseln können, würfe dies kartellrechtliche Fragen auf. Im Fall einer offen betriebenen Standardisierung bleibt dies jedoch regelmäßig unproblematisch. Eine umfassende Standardisierung von Schnittstellen

könnte zudem auch eine Interoperabilität mit Systemen anderer Hersteller sicherstellen und es ermöglichen, Anbieter von Dienstleistungen (z.B. Pflegedienste oder Lebensmittellieferungen) unter Beibehaltung des Systems zu wechseln.

7.2.2 Transparenz und Verbraucherschutz

Besondere Transparenzanforderungen im Verbraucherschutzrecht, namentlich die Belehrungspflichten und Widerrufsrechte zugunsten der Verbraucher im Fernabsatz oder elektronischen Geschäftsverkehr, fügen den bereitzuhaltenden und aufzubereitenden Informationen weitere hinzu, §§ 312c-312e, 355 Abs. 2 BGB, Art. 246 ff. EGBGB. Gerade bei einem Einsatz intelligenter Systeme auf beiden Seiten, also beispielsweise in Gestalt automatisierter Shopsysteme auf Seiten des Diensteanbieters und als AAL-System auf Seiten der Nutzer, stellt sich die Frage, wie mit den Informationspflichten umgegangen werden soll.[279] Gegenwärtig zielen diese auf die Belehrung der natürlichen Person ab. Ein Festhalten in Protokollierungsdateien des AAL-Systems wäre nur bedingt geeignet. Die Pflichten sollen den Verbraucher vor Abgabe seiner Erklärung in die Lage versetzen, informiert zu entscheiden.[280] Dabei hat der Anbieter sicherzustellen, dass der Verbraucher die Information zur Kenntnis nehmen kann.

Soweit der Nutzer ein AAL-System einsetzt, das autonom tätig wird, ist eine Unterrichtung der natürlichen Person des Nutzers kaum noch möglich – ggf. ist anbieterseitig nicht einmal festzustellen, ob als Gegenüber ein autonomes System tätig wird. Hier ist zwischen den Pflichten der Beteiligten abzuwägen und eine Ausgewogenheit herzustellen, die den Anbietern keine unmöglichen Pflichten auferlegt. Gegebenenfalls ist mittelfristig eine Änderung des den Informationspflichten zugrundeliegenden europäischen Rechts anzuregen.

7.3 Entscheidungshoheit des Nutzers

Die soeben geschilderten Anforderungen an die Transparenz der Systeme sind zugleich eine Voraussetzung für jegliche Kontrolle. Der Nutzer ist in die Lage zu versetzen, die Kontrolle über das System zu behalten. Kontroll- und Eingriffsmöglichkeiten sollten dabei auf die Möglichkeiten des Nutzers abgestimmt werden. Zur nachträglichen Kontrolle sollte eine bevorzugt revisionssicher zu gestaltende Protokollierung vorgehalten werden, die der Nutzer oder ein von ihm beauftragter Vertrauter auswerten kann. Soweit das System im Namen des Nutzers nach außen in den Rechtsverkehr wirkt, ist dem Nutzer Gelegenheit zu geben, dieses Tätigwerden zu regulieren und ggf. auch Einzelheiten einzustellen bis hin zum Freigeben einzelner Entscheidungen.

---

[279] Siehe auch Ausschuss für Bildung, Forschung und Technikfolgenabschätzung, „Zukunftsreport – Ubiquitäres Computing“, BT-Drs. 17/405, S. 120 f.

[280] Grünberg, in: Palandt (Hrsg.), Bürgerliches Gesetzbuch (BGB), 69. Auflage, 2010, § 312 BGB Rn. 5.

7.4 Interesse des Rechtsverkehrs an wirksamen Entscheidungen

Soweit AAL-Systeme nach außen hin tätig werden, sind der Rechtsverkehr und die Gesamtheit der Teilnehmer am Rechtsverkehr potenziell betroffen. Das Bedürfnis nach Rechtssicherheit verlangt, dass die Wirksamkeit von Willenserklärungen bewertbar bleibt. Damit ist bereits zu klären, welche Entscheidungen überhaupt ein technisches System selbst treffen und im Namen des Nutzers gegenüber anderen Personen (oder deren Agenten) vertreten darf.

Auch Mischformen, in denen die Nutzer teilweise von AAL-Systemen und teilweise von Menschen ihres Vertrauens unterstützt werden, sind in der jeweiligen Wirkung auf rechtliche Fragen zu prüfen, gerade wenn sich später herausstellt, dass der Nutzer nicht mit dem Agieren des AAL-Systems oder seiner Stellvertreter einverstanden ist. Die Regelungen des bürgerlichen Rechts halten in den §§ 164 ff. BGB Lösungen vor, deren Anwendbarkeit auf AAL-Systeme zu prüfen wäre.

Fraglich ist dabei, in welchem Umfang AAL-Systeme als Vertreter im Rechtssinne fungieren können. Die Vertretungsregelungen des BGB sind für menschliche Vertrauenspersonen uneingeschränkt anwendbar, soweit es sich nicht um höchstpersönliche Rechtsgeschäfte (z.B. Eheschließung, Testamentserrichtung) handelt. Zur Frage, ob die datenschutzrechtliche Einwilligung als höchstpersönliches Rechtsgeschäft zu sehen ist, siehe oben Abschnitt 3.3.2.2.1. Menschlichen Bevollmächtigten ist es möglich, Willenserklärungen im Namen des Vertretenen abzugeben. Dabei ist eine Willenserklärung die Äußerung eines auf die Herbeiführung einer Rechtswirkung gerichteten Willens.[281] Ob auch elektronische Systeme (eigene) Willenserklärungen abgeben können, ist in der Literatur umstritten.[282] Gegenwärtig wird angenommen, dass eine menschliche Handlung erforderlich ist und elektronische Agenten keine Willenserklärungen abgeben können.[283] Diese Auffassung steht u.a. mit dem Wortlaut der Regelungen des BGB im Einklang, wonach ein Vertreter zumindest beschränkt geschäftsfähig sein muss und als Vertreter ohne Vertretungsmacht zumindest formal haften können muss, vgl. §§ 165, 179 BGB.

AAL-Systeme, die Erklärungen gegenüber Dritten abgeben, als Boten im Sinne des BGB zu sehen, die lediglich eine fremde Erklärung übermitteln, ist angesichts der Inhaltsbestimmung der Erklärung, die oft erst durch das System erfolgt, ebenfalls nicht vertretbar.[284]

In Anbetracht der rasanten Entwicklung intelligent agierender Systeme stellen einige Autoren Überlegungen darüber an, welche rechtlichen Handlungsmöglichkeiten solchen Systemen

---

[281] Jauernig, vor § 116 BGB Rn. 2; Cornelius, in: MMR 2002, S. 353, 354.

[282] Cornelius, in: MMR 2002, S. 353, 354 m.w.N.

[283] Cornelius, in: MMR 2002, S. 353, 354; Ausschuss für Bildung, Forschung und Technikfolgenabschätzung, „Zukunftsreport – Ubiquitäres Computing“, BT-Drs. 17/405, S. 120.

[284] Cornelius, in: MMR 2002, S. 353, 354.

durch die Rechtsordnungen eingeräumt werden können oder müssen, um die hinzuwachsenden tatsächlichen Möglichkeiten abzubilden.[285] Die Frage, ob autonom agierenden Systemen zu einem gewissen Grad eine Rechtsfähigkeit zugestanden werden kann oder muss, würde sich aber nicht nur auf den Bereich von AAL-Systemen beschränken, sondern wäre allgemein zu führen und wird daher hier ausgeklammert.

In Betracht kommt schließlich eine sogenannte Computererklärung. Deren rechtliche Begründung beruht auf der Zurechnung des nach außen kommunizierten Erklärungsgehalts zum Nutzer. Dabei wird unterstellt, dass die Inbetriebnahme des Geräts eine hinreichend konkrete Willensbetätigung des Nutzers in Bezug auf spätere Erklärungen verkörpert.[286] Im Bereich der in den Szenarien skizzierten AAL-Systemen stellen sich hier gesonderte Fragen, die einer näheren Erörterung bedürfen: Wie wirkt es sich aus, dass gebrechliche Menschen zwar bei der Inbetriebnahme mitgewirkt haben und dies zu diesem Zeitpunkt auch konnten, aber zwischenzeitig nicht mehr fähig sind, überhaupt eigene Willenserklärungen abzugeben oder zumindest solche dieser Komplexität und Reichweite? Auch das Andauernlassen des Betriebs des AAL-Systems kann bei sukzessivem Wegfall der Entscheidungsfähigkeit nicht als eigenständige Handlung mit Erklärungsgehalt gewertet werden. Hier könnte auf die fortdauernde Billigung durch einen an die Stelle des Nutzers getretenen Vertreter (z.B. Betreuer) abzustellen sein.

Daneben ist die Frage zu erörtern, wie das Tätigwerden von Systemen zu beurteilen ist, die auf Geheiß Dritter, z.B. einer Krankenkasse oder eines Pflegedienstes, in Betrieb genommen wurden, wenn ein vom Nutzer in Betrieb genommenes Gerät für solche Dritte tätig wird. Hier wird vermehrt auf die transparente Gestaltung der Systeme bzw. deren Dokumentation zu achten sein, so dass die widerstreitenden Interessen erkennbar werden. Insbesondere sind die Verantwortlichen für einzelne Formen des Tätigwerdens von Systemen zu identifizieren und das jeweilige Tätigwerden eindeutig zu einem Verantwortlichen zurechenbar zu gestalten. Eine solche Gestaltung läge z.B. vor, wenn ein AAL-System auch von Mitbewohnern zur Haushaltsoptimierung genutzt wird oder wenn z.B. in einem Heim vom AAL-System auch originäre Aufgaben des Heims übernommen werden. Auch ist denkbar, dass ein System nicht nur für den Nutzer gegenüber Dritten auftritt, z.B. wenn AAL-Systeme autonom bestimmte Verordnungen (systembezogen: Fehlermeldung und Wartungsauftrag, ggf. auch bezogen auf den medizinischen Bereich: Bestellung von zur Neige gehenden Heil- und Hilfsmitteln) zu Lasten einer gesetzlichen Krankenkasse durchführen dürften, was freilich entsprechende Änderungen des SGB erforderte. In einem solchen Fall würden dann die Sozialleistungsträger unmittelbar verpflichtet. Daher ist das Tätigwerden für Dritte stets als solches eindeutig zu kennzeichnen und in Protokollierungsdateien beweissicher festzuhalten.

---

[285] Hildebrandt, in: Koops / Jaquet-Chiffelle (Hrsg.), S. 45 ff.

[286] Ausschuss für Bildung, Forschung und Technikfolgenabschätzung, „Zukunftsreport – Ubiquitäres Computing“, BT-Drs. 17/405, S. 120.

Zum Schutz der Interessen des Rechtsverkehrs kann als potenzieller Lösungsansatz das im Zivilrecht bewährte Institut des Ersatzes des negativen Interesses erwogen werden. Hier wurde bereits im BGB das Interesse an einem Schutz der freien Willensbildung mit dem Interesse des auf eine versehentlich falsch abgegebene Erklärung vermittelt, vgl. §§ 122, 179 Abs. 2 BGB. Eine Übertragbarkeit auf das Tätigwerden von AAL-Systemen für dessen Nutzer im Rechtsverkehr erscheint naheliegend, bedürfte jedoch einer näheren Prüfung.

7.5 Ergebnisse und offene Fragen

Eine Delegation von einzelnen Aufgaben an AAL-Systeme ist in vielen Fallkonstellationen denkbar. Entscheidungsprozesse müssen dabei transparent und nachverfolgbar ausgestaltet sein. Die Transparenz ist dabei wesentliche Voraussetzung dafür, dass der Nutzer die Hoheit über die in seinem Namen vorgenommenen Handlungen behält. Schließlich müssen im Interesse des Rechtsverkehrs wie im Interesse des Nutzers selbst die vorgenommenen Aktionen im Regelfall verbindlich sein bzw. im Ausnahmefall einer Unwirksamkeit die Interessen aller Betroffenen hinreichend geschützt werden. Betroffene sind in einem solchen Fall neben dem Nutzer auch dessen Mitbewohner, Vertragspartner, Versicherer, Dienstleister und der Rechtsverkehr.

Die Transparenzanforderungen sind so zu normieren, dass Nutzern die Wahrnehmung von Entscheidungen und die Kontrolle des Systems ermöglicht werden. Ob dies bereits zur Lösung der dargestellten wettbewerbsrechtlichen Fragen genügt, ist sodann anhand der konkreten Realisierung zu beurteilen.

Soweit ein AAL-System künftig naheliegenderweise auch im Namen Dritter wie Krankenkassen Erklärungen abgeben wird, ist sicherzustellen, dass der Vertretene deutlich erkennbar wird und eine beweissichere Protokollierung dieser Erklärung im System für die Betroffenen einsehbar ist.

8 Einbeziehung von internationalen Akteuren und grenzüberschreitenden Datenflüssen

Da AAL-Systeme nicht für sich allein stehen, sondern häufig mit anderen Systemen zusammenwirken und auf eine Kommunikationsinfrastruktur (z.B. Telekommunikations- oder Internet-Verbindungen) zurückgreifen, sind viele Parteien als Hersteller oder Betreiber in das gesamte Verfahren einbezogen. Das Gesamtverfahren muss sich dabei nicht auf Deutschland beschränken, so dass internationale Akteure und Datenflüsse betroffen sein können. Die damit verbundenen Auswirkungen auf das anzuwendende Recht und die im Streitfall zuständigen Gerichte müssen geklärt werden. Sachverhalte mit Auslandsberührung sind sowohl hinsichtlich der zuständigen Gerichtsbarkeit als auch bezüglich des auf den Einzelfall anwendbaren Rechts ganz überwiegend durch internationale Verträge oder europäische Normen geregelt.

Im Rahmen dieser Vorstudie werden wesentliche Prinzipien und Kernfragen dargestellt, die im Zusammenhang mit AAL-Systemen bei grenzüberschreitenden Sachverhalten auftreten. Dabei wird zunächst auf datenschutzrechtliche Fragen (siehe Abschnitt 8.1) eingegangen, bevor – jedoch nur exemplarisch – allgemeine Rechtsfragen bei der Einbeziehung von internationalen Akteuren angesprochen werden (siehe Abschnitt 8.2). Schließlich fasst Abschnitt 8.3 die Ergebnisse zusammen und führt offene Fragen auf.

8.1 Rechtsfragen im grenzüberschreitenden Datenverkehr

Der Austausch personenbezogener Daten über nationale Grenzen hinweg ist meist Bestandteil von internationalen Beziehungen. Damit der Schutz der Persönlichkeitsrechte auch im internationalen Geschäftsverkehr gewahrt bleibt, sind für Datenverarbeitungen, die nicht ausschließlich im Geltungsbereich des BDSG stattfinden, einige Besonderheiten zu beachten. Es gilt dabei regelmäßig die Frage zu klären, welches nationale Datenschutzrecht auf die Verarbeitung personenbezogener Daten anzuwenden ist (siehe Abschnitt 8.1.1) und wie der Schutz der Persönlichkeitsrechte bei Übermittlung von Daten ins Ausland gewährleistet wird (siehe Abschnitt 8.1.2). Daneben gibt es Besonderheiten bei Telemedien (siehe Abschnitt 8.1.3).

8.1.1 Feststellung des anwendbaren Datenschutzrechts[287]

Das anwendbare Datenschutzrecht ergibt sich aus § 1 Abs. 5 BDSG: Solange die Datenverarbeitung von Stellen, die im Europäischen Wirtschaftsraum ansässig sind,[288] verantwortlich

[287] Ausführlich dazu auch die Studie des ULD „Datenschutz in Online-Spielen“, Leitfaden mit Praxishinweisen für Hersteller und Betreiber, im Auftrag des Bundesministeriums für Bildung und Forschung, S. 48 ff., abrufbar unter: https://www.datenschutzzentrum.de/dos/.

[288] D.h. EU-Staaten sowie Island, Norwegen und Liechtenstein.

durchgeführt wird, ist nach § 1 Abs. 5 Satz 1 BDSG das Bundesdatenschutzgesetz dann anzuwenden, wenn die Verarbeitung durch eine Niederlassung im Bundesgebiet erfolgt.[289] Für Daten verarbeitende Stellen außerhalb des Europäischen Wirtschaftsraums, die Daten in Deutschland erheben, verarbeiten oder nutzen, ist gemäß § 1 Abs. 5 Satz 2 BDSG das Bundesdatenschutzgesetz bei solchen Verarbeitungen anzuwenden, bei denen die Daten verarbeitende Stelle auf Mittel zugreift, die sich in Deutschland befinden.[290]

Eine grundsätzliche Ausnahme von der Anwendung des BDSG auf alle auf deutschem Boden stattfindenden Datenverarbeitungen gilt für den Transit von Daten. Werden Daten auf Datenträgern durch Deutschland transportiert oder ausschließlich über Server in Deutschland weitergeleitet, greift für diese Weiterleitungen das BDSG nicht.[291]

8.1.2 Übermittlung von Daten in das Ausland

Übermittelt eine Daten verarbeitende Stelle personenbezogene Daten aus Deutschland heraus an eine Stelle in einem anderen Staat, trägt sie die Verantwortung dafür, dass diese Übermittlung die Persönlichkeitsrechte der betroffenen Personen nicht verletzt. Je nach der Grundlage der Datenübermittlung und je nachdem, in welchen Staat übermittelt wird, sind unterschiedliche Anforderungen zu beachten. Die Anforderungen an Datenübermittlungen an EU-Länder und Vertragsstaaten des Europäischen Wirtschaftsraums werden in Abschnitt 8.1.2.1 skizziert, während Abschnitt 8.1.2.2 kurz auf Datenübermittlungen an Drittstaaten eingeht.

8.1.2.1 Datenübermittlungen an EU-Länder und Vertragsstaaten des EWR

Für die Übermittlung personenbezogener Daten an Stellen

- in anderen Mitgliedstaaten der Europäischen Union,
- in anderen Vertragsstaaten des Abkommens über den Europäischen Wirtschaftsraum oder

---

[289] Dabei ist der Begriff Niederlassung weit gefasst. Jede effektive und tatsächliche Ausübung einer Daten verarbeitenden Tätigkeit mittels einer festen Einrichtung in Deutschland führt grundsätzlich zur Anwendbarkeit des BDSG.

[290] Diese Auslegung ergibt sich aus Art. 4 Abs. 1c der Datenschutzrichtlinie 95/46/EG, vgl. der Landesbeauftragte für Datenschutz und Informationsfreiheit Nordrhein-Westfalen, https://www.ldi.nrw.de/mainmenu_Datenschutz/submenu_Datenschutzrecht/Inhalt/InternationalerDatenverkehr/Inhalt/Eingangsseite/Anwendungsbereich_BDSG.pdf.

[291] § 1 Abs. 5 Satz 4 BDSG. Weitere Voraussetzung ist, dass die Übermittlung im Rahmen einer Tätigkeit erfolgt, die ganz oder teilweise in den Anwendungsbereich des Rechts der Europäischen Gemeinschaften fällt, was jedoch praktisch immer der Fall sein dürfte, vgl. der Landesbeauftragter für Datenschutz und Informationsfreiheit Nordrhein-Westfalen, https://www.ldi.nrw.de/mainmenu_Datenschutz/submenu_Datenschutzrecht/Inhalt/InternationalerDatenverkehr/Inhalt/Eingangsseite/Anwendungsbereich_BDSG.pdf.

- der Organe und Einrichtungen der Europäischen Gemeinschaften

gelten dieselben Erlaubnisnormen wie für Übermittlungen im Inland. Dies bedeutet, dass, sofern keine spezielleren Erlaubnisse oder Verbote bestehen – z. B. § 77 SGB X – und keine Einwilligung des Betroffenen vorliegt, die Übermittlungstatbestände des zweiten bzw. dritten Abschnitts des BDSG greifen.[292]

8.1.2.2 Datenübermittlungen an Drittstaaten

Datenübermittlungen an Drittstaaten dürfen gemäß § 4b Abs. 2 BDSG nur stattfinden, wenn sowohl ein Erlaubnistatbestand des nationalen Gesetzes vorliegt, d.h. insbesondere ein Übermittlungstatbestand des zweiten bzw. dritten Abschnitts des BDSG eingreift, als auch der Betroffene kein schutzwürdiges Interesse an dem Ausschluss der Übermittlung hat.

Ein entgegenstehendes schutzwürdiges Interesse ist z. B. regelmäßig anzunehmen, wenn bei den empfangenden Stellen ein angemessenes Datenschutzniveau nicht gegeben ist.[293] Ein angemessenes Datenschutzniveau setzt eine Gesetzgebung voraus, die die wesentlichen Datenschutzgrundsätze festlegt, wie sie auch in der europäischen Datenschutzrichtlinie 95/46/EG enthalten sind. Keine Vorbehalte bestehen dann, wenn die Europäische Kommission durch eine sogenannte Angemessenheitsentscheidung attestiert hat, dass diese Staaten ein angemessenes Datenschutzniveau gewährleisten.[294]

Die Gewährleistung eines angemessenen Datenschutzniveaus kann auch durch die Nutzung einer der beiden Standardvertragsklauseln der Europäischen Kommission erreicht werden. Bei Anwendung einer dieser Standardvertragsklauseln wird angenommen, dass bei der empfangenden Stelle ein angemessenes Datenschutzniveau herrscht.[295]

Bei Datenübermittlungen an sonstige Drittstaaten muss die Daten übermittelnde Stelle grundsätzlich selbst das Datenschutzniveau des Staates überprüfen.[296]

Sollen personenbezogene Daten in einen Staat ohne angemessenes Datenschutzniveau übermittelt werden, ist § 4c BDSG zu beachten, der eine Übermittlung z.B. mit Einwilligung des Betroffenen zulässt.

---

[292] § 4b Abs. 1 BDGS, Gola / Schomerus, Bundesdatenschutzgesetz, 10. Auflage, 2010, § 4b Rn. 3.

[293] Gola / Schomerus, Bundesdatenschutzgesetz, 10. Auflage, 2010, § 4b Rn. 7.

[294] § 4b Abs. 2 Satz 2 BDSG. Auf der Webseite der Europäischen Kommission sind die Staaten, für die Angemessenheitsentscheidungen getroffen wurden, aufgelistet: http://ec.europa.eu/justice/policies/privacy/.

[295] Gola / Schomerus, Bundesdatenschutzgesetz, 10. Auflage, 2010, § 4b Rn. 16; zum angemessenen Schutzniveau in den USA und der Safe-Harbor-Entscheidung der Europäischen Kommission siehe Gola / Schomerus, § 4b Rn. 16, sowie 32. Tätigkeitsbericht des ULD, Textziffer 11.4, abrufbar unter: https://www.datenschutzzentrum.de/material/tb/tb32/kap11.htm#114.

[296] § 4b Abs. 3 und 5 BDSG; soweit möglich, bemühen sich die Datenschutzaufsichtsbehörden, Unternehmen in Fragen des Datenschutzniveaus in Drittstaaten zu beraten.

8.1.3 Besonderheiten für Telemedien[297]

Besonderheiten gelten im Zusammenhang mit dem räumlichen Anwendungsbereich der Datenschutzbestimmungen für Telemedien. Auch das TMG[298] geht davon aus, dass maßgeblich der Niederlassungsort des Diensteanbieters ist.[299] Der Anwendungsbereich ist demnach unabhängig von dem Ort, an dem der Telemediendienst angeboten wird. Der Diensteanbieter unterliegt dem Recht des Mitgliedstaates, in dem er seine Niederlassung hat. Für in Deutschland (auch) niedergelassene Telemediendiensteanbieter gilt daher grundsätzlich das deutsche Recht, selbst wenn die jeweiligen Dienste in einem anderen Mitgliedstaat der Europäischen Union oder in Liechtenstein, Island und Norwegen angeboten oder erbracht werden.

In einem anderen Mitgliedstaat der EU oder des EWR niedergelassene Telemedienanbieter unterliegen den rechtlichen Bestimmungen des jeweiligen Mitgliedstaates. Unabhängig davon ist in § 3 Abs. 3 Nr. 4 TMG geregelt, dass die in Abs. 2 gewährleistete Freiheit des Dienstleistungsverkehrs von Telemedien die nationalen Datenschutzbestimmungen nicht außer Kraft setzen. Hier ist vielmehr die Regelung des § 1 Abs. 5 BDSG zu berücksichtigen. Im Ergebnis ist daher § 1 Abs. 5 BDSG als Kollisionsregelung anzuwenden und führt dazu, dass auch die §§ 11 ff. TMG international Anwendung finden (siehe Abschnitt 3.4.1.3).

Insoweit bestehen ausreichende Vorschriften und Kollisionsnormen.

8.2 Rechtsfragen bei Einbeziehung von internationalen Akteuren

Im AAL-Bereich ist es möglich, dass einer der Beteiligten seinen Sitz oder Wohnort im Ausland hat oder aber der sonst im Inland lebende Nutzer sich im Zeitpunkt der Inanspruchnahme im Ausland aufhält. So ist es z.B. denkbar, dass ein in Deutschland ansässiger Nutzer eine Servicezentrale in Ausland nutzt, da diese für ihn das kostengünstigste Angebot hat, oder ein Nutzer seinen Hausarzt auch während seines Urlaubsaufenthalts im Ausland in Anspruch nehmen möchte. Denkbar ist auch, dass ein in Deutschland ansässiger Dienstleister sich eines dritten Unternehmers bedient, der seinen Sitz im Ausland hat.

Bereits die Frage des anwendbaren Rechts im Bereich des Datenschutzes (siehe Abschnitt 8.1.1) ist nicht immer einfach zu beantworten, da womöglich mehrere nationale Rechtsnormen gleichzeitig Anwendung finden müssen. Diese Problematik gilt generell bei der Einbeziehung von internationalen Akteuren (siehe Abschnitt 8.2.1). Exemplarisch werden zwei medizinische Fragestellungen herausgegriffen (siehe Abschnitt 8.2.2), die allenfalls die Viel-

---

[297] Ausführlich dazu auch die Studie des ULD „Datenschutz in Online-Spielen“, Leitfaden mit Praxishinweisen für Hersteller und Betreiber, im Auftrag des Bundesministeriums für Bildung und Forschung, S. 48 ff., abrufbar unter: https://www.datenschutzzentrum.de/dos/.

[298] In entsprechender Umsetzung der Richtlinie 2000/31/EG (EG-Telemedienrichtlinie).

[299] Heckmann, in: juris PraxisKommentar Internetrecht, Abschnitt 1.3, Rn. 4.

falt weiterer juristischer Fragen erahnen lassen. Ergebnisse und offene Fragen sind in Abschnitt 8.3 zusammengefasst.

8.2.1 Anwendbares Recht – nicht immer leicht zu bestimmen

Im Europäischen Wirtschaftsraum ist die Dienstleistungsfreiheit gem. Art. 56-62 des Vertrags über die Arbeitsweise der Europäischen Union (AEUV) gewährleistet, so dass grenzüberschreitende Dienstleistungen im Raum der EU unproblematisch sind. Aufgrund der gewährleisteten Dienstleistungsfreiheit müssen Dienstleistungen unabhängig von dem EU-Dienstleistungsort erbracht werden können. Außerhalb des Europäischen Wirtschaftsraums gilt die Dienstleistungsfreiheit nicht.

Grundsätzlich stellt sich die Frage des anwendbaren Rechts und der Gerichtsbarkeit, sollte es zu Streitigkeiten kommen. Dies betrifft insbesondere Haftungsfragen bei grenzüberschreitenden Dienstleistungen.[300]

8.2.2 Fragestellungen aus dem medizinischen Bereich

Es werden exemplarisch zwei Fragen aus dem medizinischen Bereich vorgestellt: zum einen die berufsrechtliche Frage, ob ein ausländischer Arzt, der als Dienstleister einer AAL-Anwendung fungieren soll, eine Zulassung nach deutschem Recht benötigt (siehe Abschnitt 8.2.2.1), zum anderen die Frage nach einer etwaigen örtlichen Beschränkung aufgrund der Röntgenverordnung (siehe Abschnitt 8.2.2.2).

8.2.2.1 Zulassungsvoraussetzungen nach § 10b Bundesärzteordnung

Aus berufsrechtlicher Sicht stellt sich die Frage, ob ein ausländischer Arzt als Dienstleister einer AAL-Anwendung eingesetzt werden kann bzw. ob dieser eine Zulassung nach deutschem Recht benötigt. Aufgrund der in der EU geltenden Dienstleistungsfreiheit muss zwischen Ärzten aus der EU und aus Drittländern unterschieden werden.

Nach § 10b Abs. 1 Bundesärzteordnung (BÄO) dürfen Staatsangehörige eines Mitgliedstaates der Europäischen Union, die zur Ausübung des ärztlichen Berufs in einem der übrigen Mitgliedstaaten der Europäischen Union aufgrund einer nach deutschen Rechtsvorschriften abgeschlossenen ärztlichen Ausbildung oder aufgrund eines ärztlichen Ausbildungsnachweises berechtigt sind, als Dienstleistungserbringer vorübergehend und gelegentlich den ärztlichen Beruf im Geltungsbereich dieses Gesetzes ausüben. Der Absatz 2 dieser Vorschrift bestimmt, dass ein Dienstleistungserbringer im Sinne des Absatzes 1, wenn er zur Erbringung von Dienstleistungen erstmals von einem anderen Mitgliedstaat nach Deutschland

[300] Schädlich, Rechtliche Aspekte internationaler Telemedizin, in: Rechtliche Aspekte der Telemedizin, S. 45 f.

wechselt, den zuständigen Behörden in Deutschland vorher schriftlich Meldung zu erstatten hat. Es ist zu prüfen, in welchen Konstellationen bei AAL-Systemen und -Anwendungen mit Einbindung von internationalen Akteuren von einer inländischen Tätigkeit des ausländischen Arztes im Sinne der genannten Vorschrift auszugehen ist. Sofern dies bejaht würde, wäre zu klären, ob die Vorschrift mit den europäischen Vorgaben konform ist.

Bei außereuropäischen Ärzten stellen sich bereits Fragen der Zulassung als Arzt, da die Berufsausübung in Deutschland eine entsprechende Zulassung voraussetzt.

8.2.2.2 § 3 Abs. 4 Satz 1 Nr. 3 und 6 der Röntgenverordnung

Der Betrieb einer Teleradiologie setzt eine Genehmigung voraus, die nur unter der folgenden Voraussetzung erteilt: Es muss gewährleistet sein, dass am Ort der technischen Durchführung ein Arzt mit den erforderlichen Kenntnissen im Strahlenschutz vorhanden ist, der insbesondere die zur Feststellung der rechtfertigenden Indikation erforderlichen Angaben ermittelt und an eine gesetzlich bestimmte Person weiterleitet sowie den Patienten aufklärt (§ 3 Abs. 4 Satz 1 Nr. 3 Röntgenverordnung (RöV)) und diese gesetzlich bestimmte Person oder in begründeten Fällen eine andere Person nach § 24 Abs. 1 Nr. 1 RöV innerhalb eines für eine Notfallversorgung erforderlichen Zeitraums am Ort der technischen Durchführung eintreffen kann (§ 3 Abs. 4 Satz 1 Nr. 6 RöV). Dies bedeutet: Ein Radiologe muss immer binnen weniger Minuten vor Ort sein können.[301]

Es stellt sich die Frage, ob dieser Standard gehalten werden muss bzw. ob Ausnahmen zulässig sein sollten, die im Bereich des Einsatzes von AAL-Anwendungen im medizinischen Bereich zum Tragen kommen könnten.

8.3 Ergebnisse und offene Fragen

Bei der Einbindung von internationalen Akteuren und grenzüberschreitenden Datenflüssen ist es nicht trivial, das jeweils anwendbare Recht und die Gerichtsbarkeit zu bestimmen. Dies ist sowohl wichtig für den Betroffenen als auch für Hersteller und Anbieter, die rechtskonform agieren wollen und Klarheit über die jeweiligen Verantwortlichkeiten benötigen. Besonders relevant ist dies bei Haftungsfragen in Bezug auf grenzüberschreitende Datenflüsse.

Weiterhin ist zu klären, inwieweit das ärztliche Berufsrecht an internationale Konstellationen angepasst werden sollte.

[301] Schädlich, Rechtliche Aspekte internationaler Telemedizin, in: Rechtliche Aspekte der Telemedizin, S. 139.

9 Zugriffe von Dritten auf die Daten im AAL-System

Wie eingangs in den Szenarien am Beispiel verdeutlicht (siehe Abschnitt 2.1.7), ist es nicht unwahrscheinlich, dass künftig über Zugriffe auf die Daten im AAL-System durch Dritte diskutiert wird. Hier kommen insbesondere Zugriffe von Strafverfolgungsbehörden (siehe Abschnitt 9.1) sowie Zugriffe von Versicherungen (siehe Abschnitt 9.2) in Betracht. Anschließend werden die Ergebnisse und offenen Fragen in Abschnitt 9.3 zusammengefasst.

9.1 Zugriffe von Strafverfolgungsbehörden

Große Datenbestände über einen großen Teil der Bevölkerung bergen grundsätzlich die Gefahr, Begehrlichkeiten von Strafverfolgungsbehörden oder anderen Sicherheitsbehörden zu wecken.[302] Strafverfolgungsbehörden können mittels ihrer Befugnisse unter bestimmten Voraussetzungen die Beschlagnahme von den in den Rechenzentren gespeicherten Daten bewirken.

Die wichtigste Möglichkeit der Strafverfolgungsbehörden zur Sicherung von Beweismitteln stellt die Durchsuchung nach den §§ 102, 103 StPO und die sich meist daran anschließende Beschlagnahme von aufgefundenen Gegenständen gem. § 94 StPO dar. Eine Beschlagnahme bzw. eine Auswertung der Daten ist nur dann nicht erlaubt, wenn Daten einem Arzt anvertraut sind, §§ 53 Abs. 1, 95 StPO. Die beim Arzt gespeicherten Patientendaten unterliegen dem Beschlagnahmeverbot nach § 97 Abs. 1 StPO, welches das Vertrauensverhältnis zwischen dem zeugnisverweigerungsberechtigten Arzt und dem Betroffenen schützt. Das Beschlagnahmeverbot erstreckt sich jedoch nur auf Gegenstände, die sich im Gewahrsam des Zeugnisverweigerungsberechtigten, d.h. beim Arzt, befinden. Bei Gewahrsam eines externen Dritten findet das Beschlagnahmeverbot keine Anwendung.[303] Strittig ist, ob das Beschlagnahmeverbot fortbesteht, wenn der Gewahrsamsinhaber wiederum ein Arzt ist, der aber nicht dem Behandlungsteam für den betroffenen Patienten angehört.

Patienten können auch von einer Beschlagnahme betroffen sein, wenn sich die Strafverfolgung gar nicht auf sie richtet, beispielsweise wenn in einem Rechenzentrum, das auch, aber nicht ausschließlich AAL-Daten verarbeitet, die Server beschlagnahmt und alle Daten gesichtet werden. Hinzu kommt, dass bei einer Speicherung der Daten im Ausland (siehe Kapitel 8) auch dortige Strafverfolgungsbehörden oder weitere Behörden auf die Daten zugreifen

---

[302] Vgl. z.B. ULD: Unabhängiges Landeszentrum für Datenschutz / Humboldt-Universität Berlin, TAUCIS – Technikfolgenabschätzung Ubiquitäres Computing und Informationelle Selbstbestimmung, Studie im Auftrag des Bundesministeriums für Bildung und Forschung, S. 198: „Gleichzeitig ist zu beobachten, dass staatliche Stellen sukzessive ihre Erhebungsbefugnisse ausweiten, indem sie Zugriff auf die von Unternehmen gewonnenen Kundendaten nehmen. Ein Beispiel ist der staatliche Zugriff auf Kontoinformationen bei den Kreditinstituten nach § 93 Abs. 7 und 8 und 93b AO sowie § 24 KWG. Ein anderes Beispiel ist der Online-Zugriff auf die Kundendaten der TK-Unternehmen nach § 112 TKG."

[303] Dies ist beispielsweise zu beachten bei der Einschaltung Dritter z.B. zur Archivierung von Patientendaten.

können, ohne dass die Betroffenen in Deutschland eine effektive Möglichkeit zum Rechtsschutz haben.

In vielen Fällen kann der Betroffene es gar nicht merken, ob Dritte auf die Daten zugreifen oder zugegriffen haben. Selbst wenn eine Beschlagnahme von Servern dazu führt, dass bestimmte Komponenten im AAL-System oder bestimmte Funktionen (zeitweise) nicht zur Verfügung stehen, kann der Betroffene nicht sicher sein, wodurch der Ausfall verursacht wurde.

Insoweit ist zu prüfen, ob durch die zunehmende Einschaltung Dritter, wie sie gerade im AAL-Bereich und durch die Einrichtung von entsprechenden Infrastrukturen zu erwarten ist, noch ein ausreichendes Schutzniveau zum Schutz des Vertrauensverhältnisses zwischen Patient und Arzt vorhanden ist oder ob es diesbezüglich einen Anpassungsbedarf gibt.

9.2 Zugriffe von Versicherungen

Private Versicherungen übernehmen Risiken, die die Gesundheit und die Lebensführung der Person betreffen. Die Versicherungsprämie richtet sich nach der Wahrscheinlichkeit des Eintritts des Schadensfalls. Insoweit ist es für die Kalkulation des Risikos für den Versicherer interessant, Informationen über Verhaltensweisen sowie die Lebensführung des Versicherten zu erhalten, um so sein Versicherungsrisiko präziser bewerten zu können.

Bei einer stärkeren Verbreitung von im Hintergrund zur unauffälligen Unterstützung laufenden Systemen liegen künftig erheblich mehr Daten zur Lebensführung in digitaler Form vor und können somit leicht gesammelt, verarbeitet und miteinander in Bezug gebracht werden. Aus solchen kombinierten Daten lassen sich im Regelfall mehr Informationen ableiten als aus einzelnen Quellen.[304] Dabei können klassische Informationsquellen wie Kundendatenbanken mit Informationen aus Quellen, die durch den Einsatz von Sensortechnik neu zur Verfügung stehen, kombiniert werden. So wäre es technisch möglich, beispielsweise die Einkaufsgewohnheiten eines Versicherten mit seiner Krankengeschichte und seinen Freizeitaktivitäten abzugleichen, um die Prämie der Krankenversicherung festzulegen. Menschen, deren Lebensgewohnheiten als riskant oder ungesund identifiziert werden (oder die ihre Daten nicht offenlegen wollen), müssten dann z.B. einen höheren Versicherungsbeitrag zahlen.[305]

In diesem Zusammenhang sind Szenarien sowohl von Unternehmensseite als auch von staatlicher Seite denkbar. Der Druck muss nicht zwangsläufig direkt von der Versicherung ausgeübt werden, denn wenn ein Teil der Nutzer Verhaltensweisen und (gesunde) Lebensführung freiwillig durch Offenbarung der vorliegenden Daten nachweist und etwa Rabatte

[304] Vgl. auch Ausschuss für Bildung, Forschung und Technikfolgenabschätzung, „Zukunftsreport – Ubiquitäres Computing“, BT-Drs. 17/405, S.125.

[305] Das Szenario wurde fast wörtlich der o.g. Technikfolgeabschätzung „Zukunftsreport – Ubiquitäres Computing“, BT-Drs. 17/405, S. 125, entnommen.

oder Boni erhält, entsteht dadurch ein Druck auf die Mitversicherten zum Offenlegen ihrer Daten.

Hier gilt es, das Datenschutzrecht an die neuen Möglichkeiten der Datennutzung anzupassen.

9.3 Ergebnisse und offene Fragen

Es zeigt sich, dass AAL-Daten durchaus für verschiedene Parteien interessant sein können.

Ein Beschlagnahmeschutz gegenüber Strafverfolgungsbehörden ist nur dann wirkungsvoll gegeben, wenn sich die Daten im Schutzbereich des behandelnden Arztes befinden. Sobald Dienstleister eingeschaltet werden, die (auch) AAL-Daten verarbeiten, greift der Beschlagnahmeschutz nicht mehr. In einem internationalen Kontext ist offen, wie Betroffene einen effektiven Schutz gegen einen Zugriff durch Dritte erhalten können oder welche Möglichkeiten des Rechtsschutzes sie nach solchen Zugriffen in Anspruch nehmen können. Dies bedarf einer rechtlichen Prüfung.

Für den Fall, dass Versicherungen einen Zugriff auf die AAL-Daten begehren, ist es nötig, dass rechtlich eine diskriminierende oder missbräuchliche Nutzung im Versicherungsverhältnis untersagt wird. Es würde nicht ausreichen, dass Versicherungen auf Basis von Einwilligungen der Betroffenen den Zugriff erhalten, weil im Versicherungsverhältnis nicht von einer Freiwilligkeit der Einwilligung ausgegangen werden kann.

10 Ergebnisse und Handlungsempfehlungen

Die Vorstudie zeigt, dass zahlreiche rechtliche Fragen zu klären sind, um für die Betreiber und Anbieter die erforderliche Rechtssicherheit und für die Nutzer das erforderliche Vertrauen zu schaffen. Im Folgenden werden die Ergebnisse und aus den jeweiligen Ausführungen resultierenden offenen Fragen, die in den Kapiteln 3 bis 9 erarbeitet wurden, zusammengefasst. Zunächst beschreibt Abschnitt 10.1 die Anforderungen an AAL-Systeme aus der rechtlichen und technischen Perspektive des Datenschutzes. Diesbezügliche Fragen des ärztlichen Berufsrechts werden in Abschnitt 10.2 erläutert. Abschnitt 10.3 konzentriert sich auf die Ergebnisse aus dem Haftungsbereich. In Abschnitt 10.4 liegt der Schwerpunkt auf dem Sozialversicherungsrecht. Ergebnisse und Fragen der Stellvertretung und Delegation von Rechten an ein AAL-System werden in Abschnitt 10.5 dargestellt. Abschnitt 10.6 geht auf die Einbeziehung von internationalen Akteuren ein. Schließlich behandelt Abschnitt 10.7 etwaige Zugriffe von Dritten auff AAL-Daten.

10.1 Datenschutz – Anforderungen aus Recht und Technik

Da der Fokus der Vorstudie auf der Erarbeitung von Anforderungen und Fragen aus dem Datenschutzbereich lag, bietet sich an, die gewonnenen Ergebnisse je nach Themenfeld feiner zu strukturieren.

So werden die zentralen Fragen zur Gestaltung der Einwilligung in Abschnitt 10.1.1 und die der möglichen Kontrolle in Abschnitt 10.1.2 aufgeführt. Mit der Frage von Regelungen im Vorfeld des Personenbezugs befasst sich Abschnitt 10.1.3. In Abschnitt 10.1.4 geht es um Regelungen zur Profilbildung. Die Schwierigkeiten in Bezug auf die datenschutzrechtliche Verantwortung sind in Abschnitt 10.1.5 dargestellt. Abschnitt 10.1.6 widmet sich der Gewährleistung von Betroffenenrechten. Anforderungen an Transparenz- und Informationspflichten ergeben sich aus Abschnitt 10.1.7. Die spezielleren Bereiche der Anbindung an soziale Netzwerke sowie der Betroffenheit Dritter, z.B. von Mitarbeitern, werden in den Abschnitten 10.1.8 und 10.1.9 skizziert. Das Feld der technisch-organisatorischen Vorgaben und Lösungen wird in Abschnitt 10.1.10 untersucht.

Weiterhin erörtert Abschnitt 10.1.11 die staatliche Infrastrukturverantwortung. Abschnitt 10.1.12 geht darauf ein, inwieweit Datenschutz als Akzeptanz- und Wettbewerbsfaktor gestärkt werden kann. Schließlich behandelt Abschnitt 10.1.13 die Förderung der Integration des Datenschutzes in die Prozessorganisation der Unternehmen sowie die Etablierung von Codes of Conduct.

10.1.1 Einwilligung

Die bestehende Rechtslage ist insoweit unbefriedigend, als die geltenden Anforderungen an eine wirksame Einwilligung nach § 4a BDSG, die regelmäßig die Grundlage der Datenverarbeitung im Bereich AAL ist, die bestehenden Risiken der neuen Technik nicht ausreichend abbilden. Die Einwilligung in der gegenwärtigen Form stößt angesichts der neuen, im Regel-

fall im Hintergrund arbeitenden Technik an ihre Grenzen. Aus diesem Grund sind bei der Einwilligungsregelung des BDSG Anpassungen notwendig. Dabei dürfen einerseits keine Hürden aufgebaut werden, die die Praxis überfordern, andererseits muss ein hinreichender der Schutz der betroffenen Personen gesichert sein.

Zu denken ist dabei zum Beispiel an eine zeitliche Begrenzung der Einwilligung, an eine Abstufung des Einwilligungsumfangs und des Einwilligungszwecks, an eine entsprechend angepasste Information und Aufklärung der Betroffenen und ggf. an eine Standardisierung der Einwilligung. Sofern der Grad der Informiertheit bei der Einwilligung hinter dem heute geforderten Niveau zurückbliebe, wären als Kompensation weitere verfahrensbezogene Zulässigkeitsbedingungen aufzustellen, um den Betroffenen vor Zwangslagen und unbedachten Erklärungen zu schützen.

So sollte schon bei dem Entwurf der Systeme ein stärkeres Gewicht auf Gestaltungs- und Verarbeitungsregeln gelegt werden, d.h. insbesondere auf die Grundsätze der Transparenz, der Zweckbindung, der Erforderlichkeit und der Datenvermeidung und Datensparsamkeit. Im Ergebnis sollten daher

- zusätzliche Transparenzanforderungen entwickelt und bestehende Anforderungen konkretisiert werden (beispielsweise in Bezug auf die Gestaltung von Datenschutzerklärungen und der Bereitstellung standardisierter Informationen über Datenstrukturen und Datenflüsse),
- spezifische Löschungsverpflichtungen erarbeitet und festgelegt werden,
- flankierende Maßnahmen zur Sicherung der Zweckbindung erarbeitet werden, um einen Missbrauch verhindern zu können,
- untersucht werden, wie der Grundsatz der Datenvermeidung und Datensparsamkeit bei der Systemgestaltung effektiv umgesetzt und vor allem verbindlicher gemacht werden kann, indem beispielsweise Sanktionsmöglichkeiten eingeführt und Best Practices zur Verfügung gestellt werden,
- eine Verpflichtung zur Gewährung von Wahlmöglichkeiten für den Nutzer geprüft werden und
- eine Berichtspflicht an die Aufsichtsbehörden erwogen werden.

Zur Gewährleistung der Transparenz gehört es, dass die Betroffenen in der Lage versetzt werden, die komplexen Vorgänge der elektronischen Verarbeitung ihrer Daten in Kombination mit der AAL-Infrastruktur einschließlich der eingebundenen Netze, Rechner und Systeme der Dienstleister zu verstehen. Dazu wird es immer häufiger der Vermittlung durch kundige Personen bedürfen, um solche komplexe Systeme anschaulich zu erklären. Künftig wird daher die Funktion eines Lotsen über die in seinem Bereich zum Einsatz kommende AAL-Technik erforderlich sein – nicht nur im Vorfeld der Einführung, d.h. im Zusammenhang mit der Erteilung der Einwilligung, sondern auch im Zusammenhang mit der Wahrung und Aus-

übung der Betroffenenrechte. Es sind daher Treuhänder bzw. Patenlösungen zu erarbeiten, die den Nutzern zu Seite gestellt werden können.

Des Weiteren könnte und sollte die Einwilligung auch durch technische Maßnahmen unterstützt werden. Um die Einführung solcher technischen Konzepte zumindest nicht durch bestehendes Recht zu behindern, müsste u.U. das Schriftformerfordernis des BDSG angepasst werden.

10.1.2 Kontrollmöglichkeiten

Ein wichtiger Aspekt bei der Bereitstellung von AAL-Systemen ist das Schaffen von Vertrauen nicht nur durch Transparenz, sondern auch durch Kontrollmöglichkeiten insbesondere der Nutzer selbst. Daneben ist eine Kontrolle durch interne und externe Kontrollinstanzen wie vor allem betriebliche Datenschutzbeauftragte und Datenschutzbehörden nötig. Im Ergebnis sind daher geeignete Mittel der Eigenkontrolle für die Nutzer zu erarbeiten und bereitzustellen. Weiterhin ist eine Stärkung der Vorabkontrolle zu prüfen. Eine spezifische Melde- und Dokumentationspflicht für AAL-Systeme gegenüber den Datenschutzbehörden kann helfen, Kontrolldefizite und kontrollfreie Räume zu vermeiden.

10.1.3 Regelungen im Vorfeld des Personenbezugs

Eine offene Frage ist weiter, wie Daten geschützt werden können, die noch nicht personenbezogen erhoben werden, bei denen aber möglicherweise zu einem späteren Zeitpunkt – sei es durch erworbenes Zusatzwissen des Verarbeitenden oder durch Auswertungen oder Verknüpfungen der Daten – ein Personenbezug herstellbar wird. So sollten Regelungen getroffen werden für Sammlungen von Sensordaten, Umgebungsdaten oder von pseudonymen Präferenzen, wenn die Möglichkeit oder gar die Absicht besteht, diese zu einem späteren Zeitpunkt mit Personenbezug zu versehen. Dabei ist auch die Frage zu klären, wie dem Risiko entgegenzuwirken ist, dass diese Daten von Dritten mit natürlichen Personen in Verbindung gebracht werden. Das könnte z.B. durch die Schaffung von Informationspflichten sowie Auskunfts- und Löschungsansprüchen im Vorfeld zum Personenbezug geschehen. Andere Möglichkeiten bestehen in einer Einschränkung der Übermittlung oder Veröffentlichung solcher Daten oder im Vermeiden oder zeitlichen Begrenzen von möglicherweise verkettenden Elementen in den Daten.

10.1.4 Regelungen zur Profilbildung

Ein Risiko für die informationelle Selbstbestimmung besteht bei AAL-Systemen durch eine mögliche Erstellung von detaillierten Persönlichkeits- und Verhaltensprofilen, d.h. durch eine Zusammenstellung von Daten, die eine Beurteilung wesentlicher Aspekte der Persönlichkeit erlaubt. Dies ist insbesondere dann relevant, wenn die Nutzer von AAL-Systemen von intelligenten Objekten umgeben sind und sich in intelligenten Umgebungen bewegen. Es sind

daher Regelungen erforderlich, die der Bildung von Persönlichkeitsprofilen möglichst enge Grenzen setzen.

10.1.5 Datenschutzrechtliche Verantwortung

Häufig wird im Zusammenhang mit AAL-Technik eine Vielzahl von Beteiligten eingebunden und Teilaufgaben werden ausgelagert, insbesondere im Zusammenhang mit der Einrichtung und Wartung der AAL-Technik. Dadurch wächst das Risiko für die Vertraulichkeit der verarbeiteten Daten. Zudem erschwert eine Aufteilung der Verantwortlichkeiten die Kontrolle der Datenverarbeitung durch die Betroffenen und die effektive Durchsetzung ihrer Betroffenenrechte. Zum einen müssen bei mehreren Beteiligten die Verantwortungen geklärt werden, um die Einhaltung der datenschutzrechtlichen Vorschriften zu gewährleisten. Zum anderen geht mit einem Outsourcing keine Verlagerung der Verantwortung einher; die Gesamtverantwortung liegt dann beim AAL-Anbieter, mithin bei der Pflegeeinrichtung oder dem Arzt, denen die Handlungen zugerechnet werden. Im Ergebnis sollten Instrumente geschaffen werden und zur Anwendung kommen, die die effektive Durchsetzung der Betroffenenrechte gewährleisten, z.B. durch erweiterte Informations-, Transparenz- und Auskunftspflichten. Im Zusammenhang mit einer Auftragsdatenverarbeitung sollten Instrumente entwickelt werden, die die Wahrnehmung der nicht-delegationsfähigen Verantwortung erleichtern. Auch eine Stärkung der Stellung des betrieblichen Datenschutzbeauftragten und die Einsetzung eines einheitlichen Ansprechpartners als zentraler Kontakt für die Betroffenen sind zu erwägen.

10.1.6 Gewährleistung der Betroffenenrechte

Nicht nur die Einbindung einer Vielzahl von Beteiligen kann eine effektive Wahrnehmung der Betroffenenrechte erschweren. Auch können die AAL-Systeme aufgrund ihrer Komplexität und der Tatsache, dass diese im Hintergrund laufen, die Gewährleistung der Betroffenenrechte erschweren. Zu klären bleibt daher eine Erweiterung der Betroffenenrechte der Nutzer durch weitergehende, konkretisierte Ansprüche auf Information, Auskunft, insbesondere auch über die Wirkungsweise der Systeme, sowie Widerspruch und Löschung. Außerdem ist zu prüfen, ob eine erweiterte Pflicht zur Dokumentation der eingesetzten Verfahren geboten ist als Grundlage für die Ausübung von Betroffenenrechten.

10.1.7 Transparenz- und Informationspflichten

Die Transparenz der Datenverarbeitung und der Verantwortlichen ist eine entscheidende Grundbedingung für die Einwilligung des Betroffenen und für die Beherrschbarkeit der Systeme durch die Anwender. Es sollten die Möglichkeiten untersucht werden, wie für die Nutzer Transparenz in Bezug auf die Verarbeitung ihrer personenbezogenen Daten geschaffen werden kann. Insoweit ist zu prüfen, inwieweit die Nutzer selbst umfassenden Einblick in die Datenerhebung, -verarbeitung und -nutzung erhalten können. Dies muss insbesondere personenbezogene Daten in Bereichen umfassen, in denen sich die Nutzer nur selten bewusst

darüber sind, dass Daten erhoben, verarbeitet oder genutzt werden. Hier könnten Lösungen erarbeitet werden, die den Nutzern die personenbezogenen Daten sichtbar machen. Zugleich sind Regelungen vorzusehen, die eine laufende Informiertheit der Betroffenen sicherstellen, wenn dieser dies wünscht. Zu klären in diesem Zusammenhang ist außerdem, wie eine einfache, verständliche und zusammengefasste Form der Informationen für alle zu erreichen ist. Dazu gehören insbesondere Informationen über die Zusammenführung von Daten, über die Erkenntnisse aus der Auswertung der Daten, über die tatsächlichen und rechtlichen Grenzen des Schutzes ihrer Daten sowie die daraus erwachsenden Konsequenzen.

Es sollten als Hilfestellung für die Praxis Datenschutz-Policies entworfen werden. Datenschutz-Policies sind Leitlinien, in denen sich ein Unternehmen auf die Einhaltung bestimmter Grundsätze verpflichtet, die nach außen in allgemein verständlicher Form bekannt gegeben werden.

10.1.8 Einbindung sozialer Netzwerke

Bei einer Verknüpfung von AAL-Anwendungen und sozialen Netzwerken besteht das Risiko, dass durch Sensoren erhobene Daten oder vom Nutzer eingegebene Gesundheitsdaten über das soziale Netzwerk einer größeren Öffentlichkeit zugänglich werden. Gerade bei der dominierenden Gestaltung sozialer Netzwerke durch zentrale Betreiber und die vorherrschende Finanzierung durch Werbung auf Basis der ausgewerteten Nutzerdaten sind solche Kopplungen problematisch. Zumindest sollten die Nutzer ausreichend über die Risiken aufgeklärt werden, und die Standardkonfiguration sollte sich am größtmöglichen Schutz der Nutzer und ihrer Daten orientieren.

10.1.9 Datenschutz von Beschäftigten und Besuchern

AAL-Systeme im häuslichen Bereich, die ein Monitoring des Nutzers vornehmen, können auch andere anwesende Personen überwachen, z.B. Beschäftigte von Pflegediensten oder Besucher. Deren Datenschutzanforderungen sind ebenso zu berücksichtigen wie die des Nutzers. Geklärt werden muss dazu, wie Dritte vor der Erfassung durch AAL-Systeme über eine Überwachung in bestimmten Räumen informiert werden und unter welchen Umständen ein Dritte betreffendes Monitoring für einen bestimmten Zeitraum ausgestellt werden kann. Den Forderungen nach einem verstärkten bzw. kodifizierten Beschäftigtendatenschutz wird gerade durch eine Gesetzesinitiative Rechnung getragen.

10.1.10 Technisch-organisatorische Lösungen

Es ist erforderlich, spezifische technisch-organisatorische Maßnahmen für AAL-Anwendungen zu entwickeln, um die allgemeinen Datenschutzgrundsätze, wie Datensparsamkeit und Datensicherheit, schon bei der Entwicklung von AAL-Anwendungen berücksichtigen zu können.

Ganz wesentlich ist hier Bedarf nach Forschung und Entwicklung zu Datenschutztechnik im Umfeld von AAL-Systemen, die die folgenden Problembereiche adressieren:

- Letztlich muss es dem Nutzer überlassen bleiben, die Kontrolle über sein Leben und dessen Umstände innezuhaben. Hier gibt es speziell für den AAL-Bereich einen starken Forschungsbedarf nach Möglichkeiten nutzergesteuerter Interventionstechniken.
- Es gilt sicher zu verhindern, dass die vielfach hochsensiblen Daten zu anderen als zu den ausgewiesenen und eingewilligten Zwecken genutzt werden. Hierfür sind Techniken der Datenseparierung und der bedingten Verkettbarkeit, wie sie etwa im Rahmen des Identitätenmanagements entwickelt wurden, zur Anwendungsreife zu bringen.
- Alle verantwortlichen Betreiber von AAL-Systemen müssen in die Lage versetzt sein, durch Transparenztechniken eine Prüffähigkeit für den von ihnen verantworteten Tätigkeitsbereich herzustellen. Die Systeme und deren Komponenten müssen kontrolliert betrieben werden als eine Grundvoraussetzung für einen beherrschbaren und beherrschten Betrieb.

10.1.11 Staatliche Infrastrukturverantwortung

Der Staat ist verpflichtet, durch rechtliche, organisatorische und technische Maßnahmen eine Infrastruktur zum Schutz der informationellen Selbstbestimmung aufzubauen. Diese Feststellung erhielt durch das Urteil des Bundesverfassungsgerichts zur Online-Durchsuchung besondere Bestätigung. Danach hat bei komplexen IT-Systemen jeder Mensch ein Recht auf Gewährleistung der Vertraulichkeit und der Integrität informationstechnischer Systeme.

Dies gilt auch für den AAL-Bereich: Bei der Gestaltung der informationstechnischen Abläufe müssen Rahmenbedingungen gefunden und realisiert werden, die systemseitig nicht nur funktionieren, sondern zugleich den Datenschutz strukturell gewährleisten. Diese Pflicht umfasst zunächst die Schaffung von adäquaten materiellen Regelungen, aber auch von Zulassungs- und Kontrollverfahren, bei denen Standards gesetzlich vorgegeben und behördlich sichergestellt werden. Schließlich kommt dem Staat selbst eine Informations- und Beratungspflicht zu. Dabei müssen oft Kompromisse zwischen den verschiedenen Interessen des Staates und weiteren Interessen aller Beteiligten gefunden werden. Der Gesetzgeber bleibt aufgefordert, die bisher unbefriedigende Rechtslage durch eine spezialgesetzliche Regelung zu verbessern. Im Interesse der Rechtssicherheit aller Beteiligten müssen Anforderungen, die sich aus dem grundrechtlichen Schutz der Persönlichkeit ergeben, gesetzlich festgelegt werden. Insbesondere bedarf es:

- einer Präzisierung des Einwilligungserfordernisses und des Einwilligungsverfahrens,
- der Festlegung der Notwendigkeit und des Umfangs von Beratung und Aufklärung,
- der Prüfung der Einführung einer Treuhänder- und / oder Patenlösung,
- der Prüfung einer Anpassung der Betroffenenrechte,
- der Begrenzung der Profilbildung,

- Regelungen zur Datenverarbeitung im Vorfeld eines Personenbezugs.

10.1.12 Stärkung des Datenschutzes als Akzeptanz- und Wettbewerbsfaktor

Wie demoskopische Erkenntnisse zeigen, zählt Datenschutz sowohl in Deutschland als auch international zu den grundlegenden Akzeptanzkriterien bei IT-Systemen.[306] Datenschutz als Akzeptanzfaktor ist gerade im Kontext von AAL von großer Bedeutung. Die Verletzung der rechtlichen und sicherheitstechnischen Vorgaben ist für die Unternehmen risikoträchtig: So kann das Bekanntwerden von Datenschutzmängeln zu massiven Imageschäden führen. Bei Datenschutzverstößen können im Übrigen auch Sanktionen der zuständigen Aufsichtsbehörde drohen.[307]

Eine Möglichkeit für Unternehmen, sich Datenschutz als Wettbewerbsvorteil nutzbar zu machen, besteht in der Zertifizierung von Produkten und Verfahren als konform mit Anforderungen des Datenschutzrechts. Eine Zertifizierung bzw. der Zertifizierung vorgelagerten Evaluierung oder Auditierung führt vor allen Dingen zur Transparenz der Unternehmensprozesse und zur Erhöhung der Rechtssicherheit in Bezug auf die Umsetzung der rechtlichen Verpflichtungen. Durch die Bescheinigung der Gesetzeskonformität wird das Vertrauen der Verbraucher gestärkt und dem Unternehmen eine verbesserte Stellung am Markt verschafft.

Zertifizierungen sind nicht nur als Wettbewerbsfaktor, sondern auch als Mittel zur Kontrolle und Kontrollierbarkeit datenschutzrechtlicher Anforderung effektiv. Angesichts des Umstands, dass repressiver Datenschutz immer auf den Einzelfall bezogen bleibt und dass dieser wegen der Komplexität und Vielfältigkeit der Datenverarbeitung kaum noch eine generalpräventive Wirkung entfalten kann, muss dieses Instrument als eines der präventiven Datenschutzwerkzeuge verstärkt zum Einsatz kommen.

Ein wichtiges Ziel ist es, sowohl die nötige Rechtssicherheit für die Betreiber als auch das nötige Vertrauen der Nutzer herzustellen. Eine effektive Maßnahme ist die Förderung und Durchführung von Zertifizierungen. Es empfiehlt sich daher, geeignete Zertifizierungsverfahren zu prüfen und ggf. zu entwickeln sowie einen öffentlich bereitgestellten Kriterienkatalog zu erarbeiten, dessen Beachtung sowohl im nationalen als auch im internationalen Bereich, d.h. bei grenzüberschreitenden Projekten, Rechtskonformität gewährleistet. Dabei müssten nationale und internationale Anforderungen auf Standardisierungsmöglichkeiten hin untersucht werden.

---

[306] Diese Thematik hat u.a. die Entwicklung des E-Commerce wesentlich mitbestimmt, vgl. Unabhängiges Landeszentrum für Datenschutz / Institut für Informatik der Universität Koblenz-Landau / Institut für Wirtschafts- und Verwaltungsinformatik der Universität Koblenz-Landau, SOAinVO – Chancen und Risiken von Serviceorientierten Architekturen in Virtuellen Organisationen, 2007, S. 13.

[307] So kann die Aufsichtsbehörde bei Datenschutzverstößen beispielsweise ein Bußgeld in Höhe von bis zu 300.000 Euro verhängen (vgl. § 43 BDSG). Besonders schwere Verstöße sind nach § 44 BDSG mit einer Freiheitsstrafe von bis zu 2 Jahren oder mit Geldstrafe bewehrt.

10.1.13 Förderung der Integration des Datenschutzes in die Prozessorganisation der Unternehmen sowie die Etablierung von Codes of Conduct

Eine besondere Rolle kommt, solange es keine gesetzlichen Regelungen gibt, der Selbstregulierung zu, mithin der Einführung von Codes of Conduct sowie der internen Prozessorganisation der Unternehmen.

Datenschutz ist eine Querschnittsaufgabe, die in jedem Bereich eines Unternehmens umzusetzen ist, da die Datenflüsse gleichermaßen mehrere, wenn nicht alle Bereiche des Unternehmens betreffen und damit die Anforderungen des Datenschutzes in der gesamten Organisation an den verschiedensten Stellen zu beachten sind. Um diesen Anforderungen zu genügen, sollten entsprechende Datenschutzprozesse festgelegt werden.

§ 38a Abs. 1 BDSG sieht vor, dass Berufsverbände und andere Vereinigungen, die bestimmte Gruppen von verantwortlichen Stellen vertreten, Entwürfe für Verhaltensregeln zur Förderung der Durchführung von datenschutzrechtlichen Regelungen der zuständigen Aufsichtsbehörde unterbreiten können. Zur Absicherung der Verarbeitung personenbezogener Daten kommen danach neben den staatlich gesetzten rechtlichen Vorschriften auch die von den jeweiligen Branchen formulierten Verhaltensregeln, sog. Codes of Conduct, in Betracht.

Unternehmen, die AAL-Technik anbieten, sind davon abhängig, dass Lösungen für den Schutz der Privatsphäre und zur Vertrauensbildung bei den Betroffenen getroffen werden. Eine Selbstregulierung der Unternehmen würde dem Staat die Durchsetzung staatlicher Regelungen erleichtern sowie das Vertrauen der Betroffenen in die Betreiber und die Geheimhaltung ihrer äußerst sensiblen Daten stärken. Daneben können allgemeine Datenschutzanforderungen an die fortschreitenden Entwicklungen der Datenverarbeitung flexibel und zügig konkretisiert und angepasst werden. Es ist jedoch festzuhalten, dass selbstregulierende Elemente keine Alternative zur gesetzlichen Absicherung der Grundkomponenten des Datenschutzes darstellen.

Es wird empfohlen, die Erstellung von Codes of Conduct im AAL-Bereich zu fördern.

10.2 Ärztliches Berufsrecht

Im AAL-Bereich kommt wegen der Einbindung von Heilberuflern die Schweigepflicht nach § 203 StGB zum Tragen. Dies erfordert in AAL-Systemen und -Anwendungen entsprechende Vorkehrungen zum Schutz vor unbefugten Zugriffen. Die Weitergabe der personenbezogenen Patientendaten an externe Dritten wie die Betreiber von AAL-Systemen stellt bereits eine Durchbrechung der ärztlichen Schweigepflicht dar. Dem Arzt ist die Weitergabe der Daten nur erlaubt, wenn er sich auf eine rechtliche Befugnis zur Durchbrechung der Schweigepflicht berufen kann. Eine solche Befugnis kann sich aufgrund der Einwilligung der Patienten oder aufgrund gesetzlicher Ermächtigungen ergeben. Es stellt sich die Frage, ob die Einführung von weiteren Offenbarungsbefugnissen geboten ist, die den Arzt rechtlich in die Lage versetzen würden, Patientendaten an AAL-Systeme weiterzugeben. Ein Vorbild könnten entsprechende Vorschriften in einigen Landeskrankenhausgesetzen sein, die die Einbeziehung

von externen Dienstleistern in die Datenverarbeitung unter bestimmten Voraussetzungen zulassen. Auf der anderen Seite entsteht das Problem, dass durch die weitergehende Einschaltung Dritter, wie sie gerade im AAL-Bereich und durch die Einrichtung von entsprechenden Infrastrukturen zu erwarten ist, sich auch die Risiken für die Patientendaten und damit für den Schutz des Vertrauensverhältnisses zwischen Patient und Arzt vervielfältigen. Im Fall einer Ausweitung von Offenbarungsbefugnissen sollten entsprechende strafbewehrte Geheimhaltungspflichten für die Betreiber und Mitarbeiter von AAL-Systemen nach dem Vorbild von § 203 Abs. 1 Nr. 6 StGB vorgesehen werden.

Bei einer Auftragsdatenverarbeitung der sensiblen Daten aus dem AAL-Bereich ist zu berücksichtigen, dass der Auftraggeber Verantwortlicher für die Datenverarbeitung bleibt. Daraus folgt, dass er ein gewisses Maß an Kontrolle und Einfluss in Bezug auf die Datenverarbeitung behalten muss. Dies stößt in der Praxis an Grenzen. Hier ist zu klären, wie sich die notwendige Beherrschbarkeit sicherstellen lässt. Auch ist zu prüfen, inwieweit ausgleichende Maßnahmen zur Kompensation, z.B. durch Einführung von Anzeigepflichten, zu fordern sind. Zudem sollte untersucht werden, ob die Anforderungen an das technische Verständnis von Ärzten und medizinischem Personal, das im Rahmen von AAL-Anwendungen notwendig ist, im Rahmen von Aus- und Fortbildungen eine wesentliche Rolle einnehmen muss.

Das Verbot ausschließlicher Fernbehandlung ist auf den Prüfstand zu stellen: Es sollte analysiert werden, in welchen Fällen und unter welchen Voraussetzungen eine Fernbehandlung ungefährlich für den Patienten ist und ermöglicht werden kann. Daneben ist zu klären, ob und inwiefern auch das Werbeverbot nach § 9 HWG gelockert werden sollte.

10.3 Haftung

Im Bereich des Haftungsrechts sind die vorhandenen Rechtsnormen für etwaige Schadensfälle auch bei AAL-Systemen anwendbar und stellen damit überwiegend angemessene Haftungsgrundlagen zur Verfügung. Angesichts der Komplexität von AAL-Systemen, die dazu führt, dass Betroffene im Schadensfall oft kaum durchschauen geschweige denn nachweisen können, auf welcher Seite ein Verschulden vorlag, wäre für den Bereich des Datenschutzrechts zu prüfen, Beweiserleichterungen zugunsten der Betroffenen einzuführen oder sogar eine verschuldensunabhängige Haftung, wie nach der europäischen Datenschutzrichtlinie 95/46/EG möglich, vorzusehen.

Praktische Fragen stellen sich in Bezug auf eine Haftung bei mehreren Beteiligten in einem AAL-System, da die jeweiligen Verantwortlichkeiten spätestens bei der Einführung des Systems deutlich und allen bewusst sein müssen. Im Rahmen der Verkehrssicherungspflicht müssen die Beteiligten dafür sorgen, dass die Nutzer oder Dritte nicht geschädigt werden. Dazu gehört, dass die Nutzer befähigt werden müssen, die AAL-Systeme sicher zu bedienen.

Offen ist, ob die Einführung von AAL-Systemen zu einer erweiterten Haftung für Ärzte führt. In jedem Fall sind die Pflichten aller Beteiligten in AAL-Systemen klar zu definieren, z.B. per

Vertrag zwischen dem Arzt und dem Patienten bzw. dem Arzt und dem Anbieter. Wichtig ist, dass der Arzt die Korrektheit der durch AAL-Systeme erhobenen Daten des Patienten prüft, bevor er darauf seine Diagnose und Behandlung gründet. Es müssen Methoden bereitgestellt werden, damit der Arzt Fehlfunktionen der AAL-Systeme und etwaige Manipulationen an den Daten erkennt.

10.4 Sozialversicherungsrecht

Sofern AAL-Technik zu den Leistungen gehören soll, die im Gesundheitssystem bezahlt werden, müssen entsprechende Vergütungsregeln geschaffen werden. Insbesondere wären dafür die entsprechenden AAL-Systeme oder AAL-Anwendungen im Einheitlichen Bewertungsmaßstab (EBM) sowie in der Gebührenordnung für Ärzte (GOÄ) zu integrieren. Zu untersuchen wären auch Möglichkeiten für ein abrechenbares Leistungssplitting verteilt auf mehrere beteiligte Ärzte, da zurzeit nur eine selbstständige, persönliche und damit alleinige Leistungserbringung eines Arztes im Rahmen einer Behandlung vergütet wird.

10.5 Stellvertretung und Delegation von Rechten an ein AAL-System

Es ist möglich, dass Nutzer einzelne Aufgaben an ihr AAL-System delegieren. Entscheidungsprozesse des AAL-Systems müssen dabei transparent und nachverfolgbar ausgestaltet sein. Eine Transparenz ist die wesentliche Voraussetzung dafür, dass der Nutzer die Hoheit über die in seinem Namen vorgenommenen Handlungen behält. Schließlich müssen im Interesse des Rechtsverkehrs, aber auch im Eigeninteresse des Nutzers selbst die vorgenommenen Aktionen im Regelfall verbindlich sein bzw. im Ausnahmefall einer Unwirksamkeit die Interessen aller Betroffenen hinreichend geschützt werden. Betroffene können in einem solchen Fall neben dem Nutzer selbst auch dessen Mitbewohner, Vertragspartner, Versicherer, Dienstleister und der Rechtsverkehr sein.

10.6 Einbeziehung von internationalen Akteuren

Grundsätzlich stellt sich die Frage des anwendbaren Rechts und der Gerichtsbarkeit, sollte es zu Streitigkeiten kommen. Dies gilt insbesondere für Haftungsfragen bei grenzüberschreitenden Dienstleistungen. Sachverhalte mit Auslandsberührung sind sowohl hinsichtlich der zuständigen Gerichtsbarkeit als auch bezüglich des auf den Einzelfall anwendbaren Rechts ganz überwiegend durch internationale Verträge oder europäische Normen geregelt. Hier ist die Erstellung einer Übersicht der gegenwärtigen Rechtslage zu empfehlen, die den Umfang dieser Vorstudie gesprengt hätte. Offen und damit zu untersuchen bleibt auch, inwieweit das ärztliche Berufsrecht der Anpassung bedarf.

10.7 Zugriffsrechte Dritter

Soweit es um Zugriffrechte der Strafverfolgungsbehörden auf AAL-Datenbestände durch Beschlagnahme geht, ist zu untersuchen, inwieweit durch das zu erwartende Outsourcen

von Gesundheitsdaten noch ein ausreichendes Schutzniveau beim Schutz des Vertrauensverhältnisses zwischen Patient und Arzt vorhanden ist oder ob es diesbezüglich Anpassungsbedarf gibt, z.B. durch einen erweiterten Beschlagnahmeschutz. Für den internationalen Bereich ist zu untersuchen, welche Möglichkeiten des Rechtsschutzes dem Betroffenen zur Verfügung stehen. Schließlich ist eine Verhinderung diskriminierender bzw. missbräuchlicher Nutzung von AAL-Datenbeständen im Versicherungsverhältnis erforderlich.

11 Literaturverzeichnis

Art. 29-Datenschutzgruppe	Stellungnahme 10/2004 zu einheitlicheren Bestimmungen über Informationspflichten, WP 100, 11987/04/DE, angenommen am 25. November 2004, abrufbar unter: http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2004/wp100_de.pdf.
Ausschuss für Bildung, Forschung und Technikfolgenabschätzung (Deutscher Bundestag)	Unterrichtung des Ausschusses für Bildung, Forschung und Technikfolgenabschätzung (18. Ausschuss) gemäß § 56a der Geschäftsordnung – Technikfolgenabschätzung – „Zukunftsreport – Ubiquitäres Computing“, BT-Drucksache 17/405, S. 120 f.
Das AALmagazin, Informationen zu intelligenten Assistenzsystemen für ein selbstbestimmtes Leben im Alter	Beitrag „AAL geht viele an“, Heft 1/2010, S. 10 f.
Bergmann, Karl-Otto	Die Arzthaftung – Ein Leitfaden für Ärzte und Juristen, Berlin, 2004.
BMBF/VDE, Innovationspartnerschaft AAL	Zielgruppen für AAL-Technologien und -Dienstleistungen, abrufbar unter: http://www.vde.de/de/Technik/AAL/Publikationen/Kongress-undFachbeitraege/documents/zielgruppen%20f%C3%BCr%20aal%20_tabelle_.pdf.
Camenisch, Jan / Lysyanskaya, Anna	Efficient Non-transferable Anonymous Multi-show Credential System with Optional Anonymity Revocation, in: Advances in Cryptology – Eurocrypt 2001, LNCS Vol. 2045, Springer, 2001, S. 93-118.
Clausen, Lars / Dombrowsky, Wolf R.	Warnpraxis und Warnlogik, in: Zeitschrift für Soziologie, 1984, S. 293 ff.
Cornelius, Kai	Vertragsabschluss durch autonome elektronische Agenten, in: MMR 2002, S. 353-358.
Däubler, Wolfgang / Klebe, Thomas / Wedde, Peter / Weichert, Thilo (Hrsg.)	Bundesdatenschutzgesetz Kompaktkommentar, Frankfurt am Main, 3. Auflage, 2010.
Deutsch, Erwin / Spickhoff, Andreas	Medizinrecht – Arztrecht, Arzneimittelrecht, Medizinprodukterecht und Transfusionsrecht, 6. Auflage, Berlin Heidelberg, 2008.

Dierks, Christian / Nitz, Gerhard / Grau, Ulrich (Hrsg.)	Gesundheitstelematik und Recht, Rechtliche Rahmenbedingungen und legislativer Anpassungsbedarf, Frankfurt am Main, 2003.
Driller, Elke / Karbach, Ute / Stemmer, Petra / Gaden, Udo / Pfaff, Holger / Schulz-Nieswandt, Frank	Ambient Assisted Living – Technische Assistenz für Menschen mit Behinderung, Freiburg, 2009.
Eckhardt, Jens	Wie weit reicht der Schutz des Fernmeldegeheimnisses (Art. 10 GG)?, in: DuD 2006, S. 365 ff.
Eichelberg, Marco	Die Bedeutung von Interoperabilität für AAL (Stand 30.07.2010). Der Vortrag ist abrufbar unter: http://www.ebn.din.de/sixcms_upload/media/2929/4_Eichelberg_Interoperabilitaet_AAL.pdf.
Federrath, Hannes / Pfitzmann, Andreas	Gliederung und Systematisierung von Schutzzielen in IT-Systemen; in: DuD 2000, S. 704 ff.
Fox, Dirk	Realisierung, Grenzen und Risiken der Online-Durchsuchung, in: DuD 2007, S. 827 ff.
Füllmich, Reiner	Zur Ablehnung künstlich lebensverlängernder medizinischer Maßnahmen durch nicht entscheidungsfähige Patienten, in: NJW 1990, S. 2301 ff.
Gola, Peter / Schomerus, Rudolf	Bundesdatenschutzgesetz, München, 10. Auflage, 2010.
Hansen, Marit	Linkage Control – Integrating the Essence of Privacy Protection into Identity Management Systems, in: Proceedings of eChallenges 2008, Amsterdam 2008, S. 1585-1592.
Hansen, Marit	User-controlled identity management: the key to the future of privacy?; in: International Journal of Intellectual Property Management Vol. 2, No. 4, Olney (UK), 2008, S. 325-344.
Hansen, Marit / Raguse, Maren / Storf, Katalin / Zwingelberg, Harald	Delegation for Privacy Management from Womb to Tomb – A European Perspective, in: Privacy and Identity Management for Life, 5th IFIP WG 9.2, 9.6/11.4, 11.6, 11.7/PrimeLife International Summer School, Nizza, Frankreich, 7.-11. September 2009, Revised Selected Papers, IFIP AICT 320, Springer, 2010, S. 18-33.

Hartmann, Armin / Fiebig, Madlen	Die Kombination ist die Innovation – Telemedizinische Vernetzung im Wohnungsbau und Klinikbereich. Das „WohnSelbst“ Projekt für ein gesundes Leben im eigenen Zuhause, in: BUS-Systeme, Berlin, 17. Jahrgang, 2010, S. 252 ff.
Hauck, Karl / Noftz, Wolfgang (Hrsg.)	Sozialgesetzbuch V, Gesetzliche Krankenversicherung, Loseblatt-Kommentar, Stand 2006.
Heckmann, Dirk	juris PraxisKommentar Internetrecht, Saarbrücken, 1. Auflage, 2007.
Hellmich, Stefanie	Location Based Services – Datenschutzrechtliche Anforderungen, in: MMR 2002, S. 152 ff.
Hoeren, Thomas	Das Telemediengesetz, in: NJW 2007, S. 801 ff.
Hoeren, Thomas / Sieber, Ulrich (Hrsg.)	Handbuch Multimedia-Recht, München, 21. Ergänzungslieferung, 2008.
International Conference of the Data Protection and Privacy Commissioners	Joint Proposal for a Draft of International Standards on the Protection of Privacy with regard to the processing of Personal Data. Madrid Resolution of the 31st International Conference of the Data Protection and Privacy Commissioners, adopted on 5 November, 2009, https://www.agpd.es/portalweb/canaldocumentacion/conferencias/common/pdfs/31_conferencia_internacional/estandares_resolucion_madrid_en.pdf.
Jauernig, Othmar (Hrgs.)	Bürgerliches Gesetzbuch mit allgemeinem Gleichbehandlungsgesetz, München, 2009.
Kilian, Wolfgang / Heussen, Benno (Hrsg.)	Computerrechts-Handbuch, Informationstechnologie in der Rechts- und Wirtschaftspraxis, München, 28. Ergänzungslieferung, 2010.
Koops, Bert-Jaap / Jaquet-Chiffelle, David-Olivier (Hrsg.)	New (Id)entities and the Law: Perspectives on Legal Personhood for Non-Humans, FIDIS Deliverable D17.2, Frankfurt 2008, abrufbar unter: http://www.fidis.net/fileadmin/fidis/deliverables/fidis-wp17-del17.2-new_entities_and_law_def.pdf.
Konferenz der Datenschutzbeauftragten des Bundes und der Länder	Ein modernes Datenschutzrecht für das 21. Jahrhundert, Eckpunkte, vorgelegt am 18.03.2010.

Krauskopf, Dieter (Hrsg.)	Soziale Krankenversicherung, Pflegeversicherung, Kommentar, München, 69. Ergänzungslieferung, 2010.
Lackner, Karl / Kühl, Christian	Strafgesetzbuch, Kommentar, Beck, 2007, abrufbar unter: http://beck-online.beck.de/?vpath=bibdata/komm/LackKoStGB_26/Buch/cont/LackKoStGB.htm.
Laufs, Adolf / Kern, Wilhelm (Hrsg.)	Handbuch des Arztrechts, München, 4. Auflage, 2010.
Link, Christian	Telemedizinische Anwendungen in Deutschland und in Frankreich, München, 2007.
Meints, Martin	Datenschutz nach BSI-Grundschutz? Das Verhältnis zwischen Datenschutz und Datensicherheit, in: DuD 2006, S. 13 ff.
Niederlag, Wolfgang / Dierks, Christian / Rienhoff, Otto / Lemke, Heinz U. (Hrsg.)	Rechtliche Aspekte der Telemedizin, Dresden, 2006.
Niedermeier, Robert / Schröcker, Stefan	Ersatzfähigkeit immaterieller Schäden aufgrund rechtswidriger Datenverarbeitung, in: RDV 2002, 217 ff.
Neumann, Ulrike / Hagen, Anja / Schönermark, Matthias P.	Regulation der Aufnahme von innovativen nichtmedikamentösen Technologien in den Leistungskatalog solidarisch finanzierter Kostenträger, 2007, abrufbar unter: http://portal.dimdi.de/de/hta/hta_berichte/hta210_bericht_de.pdf.
Palandt, Otto (Hrsg.)	Kommentar zum Bürgerlichen Gesetzbuch, 69. Auflage, München, 2010.
Patzak, Andreas / Beyerlein, Thorsten	Adressdatenhandel unter dem neuen BDSG, in: MMR 2009, S. 525 ff.
Perau, Guido	Betreuungsverfügung und Vorsorgevollmacht, in: MittRhNotK 1996, S. 285, 293 ff.
Petri, Thomas	Das Urteil des Bundesverfassungsgerichts zur „Online-Durchsuchung“, in: DuD 2008, S. 444 ff.
Quaas, Michael / Zuck, Rüdiger	Medizinrecht – Öffentliches Medizinrecht, Haftpflichtrecht, Arztstrafrecht, 2. Auflage, München, 2008.

Rehmann, Wolfgang / Wagner, Susanne (Hrsg.)	Medizinproduktegesetz (MPG) mit Erläuterungen, München, 2005.
Rieger, Hans-Jürgen / Dahm, Franz-Josef / Steinhilper, Gernot (Hrsg.)	Heidelberger Kommentar Arztrecht – Krankenhausrecht – Medizinrecht, Heidelberg, Stand Nov. 2008.
Roßnagel, Alexander (Hrsg.)	Handbuch des Datenschutzrecht, München, 2003.
Roßnagel, Alexander / Pfitzmann, Andreas / Garstka, Hansjürgen	Modernisierung des Datenschutzrechts, Gutachten im Auftrag des Bundesministeriums des Innern, 2001.
Roßnagel, Alexander	Das Telemediengesetz Neuordnung für Informations- und Kommunikationsdienste, in: NVwZ 2007, S. 743 ff.
Roßnagel, Alexander	Datenschutz in der künftigen Verkehrstelematik, in: NZV 2006, S. 285 ff.
Roßnagel, Alexander	Datenschutz in einem informatisierten Alltag, Gutachten im Auftrag der Friedrich-Ebert-Stiftung, Berlin 2007, abrufbar unter: http://library.fes.de/pdf-files/stabsabteilung/04548.pdf
Roßnagel, Alexander / Scholz, Philip	Datenschutz durch Anonymität und Pseudonymität, in: MMR 2000, S. 721-731.
Rost, Martin	Welches Gesetz gilt eigentlich?, Kiel, 2005, abrufbar unter: https://www.datenschutzzentrum.de/systemdatenschutz/meldung/sm91.htm/.
Rost, Martin / Bock, Kirsten	Privacy By Design und die Neuen Schutzziele – Grundsätze, Ziele und Anforderungen, in: DuD 2011, S. 30 ff.
Rost, Martin / Pfitzmann, Andreas	Datenschutz-Schutzziele – revisited, in: DuD 2009, S. 353 ff.
Rothenpieler, Peter / Becker, Claudia / Fischer, Stefan	Privacy concerns in a remote monitoring and social networking platform for assisted living, erscheint 2011 im Tagungsband der 6th IFIP WG 9.2, 9.6/11.4, 11.6, 11.7/PrimeLife International Summer School, Helsingborg, Schweden, 2.-6. August 2010.
Schack, Haimo	BGB – Allgemeiner Teil, Heidelberg, 2008.
Schleipfer, Stefan	Das 3-Schichten-Modell des Multimediadatenschutzrechts, in: DuD 2004, S. 727 ff.

Schönke, Adolf / Schröder, Horst (Hrsg.)	Strafgesetzbuch, Kommentar, München, 2010, abrufbar unter: http://beck-online.beck.de/?vpath=bibdata/komm/SchoenkeKoStGB_28/cont/SchoenkeKoStGB.htm
Simitis, Spiros (Hrsg.)	Bundesdatenschutzgesetz, Kommentar, Baden-Baden, 6. Auflage, 2006.
Taupitz, Jochen	Informationstechnologien – Haftungsschutz oder Haftungsfalle?, Ärzteblatt (ÄB) 2010, S. 1720 ff, abrufbar unter: http://www.aerzteblatt.de/v4/archiv/artikel.asp?src=heft&id=78778
Terbille, Michael (Hrsg.)	Münchener Anwaltshandbuch Medizinrecht, 1. Auflage, München, 2009.
Theißen, Sascha	Risiken informations- und kommunikationstechnischer (IKT-)Implantate im Hinblick auf Datenschutz und Datensicherheit, Karlsruhe, 2009.
Tinnefeld, Marie-Theres / Ehmann, Eugen / Gerling, Rainer W.	Einführung in das Datenschutzrecht, München, 4. Auflage, 2005.
Trill, Roland (Hrsg.)	Praxisbuch eHealth – Von der Idee zur Umsetzung, Stuttgart, 2009.
Udsching, Peter	SGB XI, Soziale Pflegeversicherung, Kommentar, München, 3. Auflage, 2010.
Unabhängiges Landeszentrum für Datenschutz / Institut für Informatik der Universität Koblenz-Landau / Institut für Wirtschafts- und Verwaltungsinformatik der Universität Koblenz-Landau	SOAinVO – Chancen und Risiken von Service-orientierten Architekturen in Virtuellen Organisationen, 2007, abrufbar unter: https://www.datenschutzzentrum.de/soa/.
Unabhängiges Landeszentrum für Datenschutz / Technische Universität Dresden	Verkettung digitaler Identitäten, Report im Auftrag des Bundesministeriums für Bildung und Forschung, Kiel, 2007, abrufbar unter: https://www.datenschutzzentrum.de/projekte/verkettung/.

Unabhängiges Landeszentrum für Datenschutz / Humboldt-Universität Berlin	TAUCIS – Technikfolgen-Abschätzung Ubiquitäres Computing und Informationelle Selbstbestimmung, Studie im Auftrag des Bundesministeriums für Bildung und Forschung, Kiel, 2006, abrufbar unter: https://www.datenschutzzentrum.de/taucis/.
Unabhängiges Landeszentrum für Datenschutz	Datenschutz in Online-Spielen, Leitfaden mit Praxishinweisen für Hersteller und Betreiber, Studie im Auftrag des Bundesministeriums für Bildung und Forschung, Kiel, 2010, abrufbar unter: https://www.datenschutzzentrum.de/dos/.
Voigt, Peer-Ulrich	Rechtsgutachten Telemedizin – Rechtliche Problemfelder sowie Lösungsvorschläge, Gutachten vom 15.10.2008, abrufbar unter: http://www.initiative-gesundheitswirtschaft.org/pressedownloads/gutachten/
Weichert, Thilo	Gentests und Persönlichkeitsrecht, Datenschutz und Datenhoheit, Vortrag im Rahmen des Wintersymposiums 2001/2002, „Von der Durchsichtigkeit des Menschen – Rechtsprobleme der Gendiagnostik“, abrufbar unter: https://www.datenschutzzentrum.de/material/themen/gendatei/gentests.htm#2c.
Weichert, Thilo	Medizinische Telematik und Datenschutz, Beitrag zum 111. Deutschen Ärztetag am 22.05.2008 in Ulm, abrufbar unter: https://www.datenschutzzentrum.de/medizin/gesundheitskarte/20080522-weichert-medizinische-telematik.html.
Weichert, Thilo	Auskunftsanspruch in verteilten Systemen, in: DuD 2006, S. 695 ff.
Weichert, Thilo	Vertraulichkeitsschutz durch IT-Sicherheit bei der elektronischen Gesundheitskarte, Vortrag anlässlich des BSI-Kongresses 10.-12. Mai 2005, abrufbar unter: https://www.datenschutzzentrum.de/vortraege/050510_weichert_bsi.htm.

Weichert, Thilo — Datenschutzrechtliche Anforderungen an zertifizierte IT-Produkte für den Bereich Telemedizin, Vortrag bei der Sommerakademie 2003, abrufbar unter: https://www.datenschutzzentrum.de/sommerakademie/2003/sak03wei.htm#4.

Weichert, Thilo — Cloud Computing und Datenschutz, Vortrag auf dem 4. Österreichischen IT-Rechtstag INFOLAW, 18.06.2010, Wien, abrufbar unter: https://www.datenschutzzentrum.de/cloud-computing/20100617-cloud-computing-und-datenschutz.html.

Wichert, Reiner — Configuration and Dynamic Adaptation of AAL Environments to Personal Requirements and Medical Conditions (Stand: 30.07.2010), abrufbar unter: http://www.aal.fraunhofer.de/publications/Configuration-and-adaptation-of-AAL-Environments.pdf.

12 Abkürzungsverzeichnis

AAL	Ambient Assisted Living
Abs.	Absatz
ÄB	Ärzteblatt
Abb.	Abbildung
AEUV	Vertrag über die Arbeitsweise der Europäischen Union
AG	Aktiengesellschaft
AGB	Allgemeine Geschäftsbedingungen
AICT	Advances in Information and Communication Technology
AO	Abgabenordnung
AP	Arbeitspaket
Art.	Artikel
BÄO	Bundesärzteordnung
BDSG	Bundesdatenschutzgesetz
BfDI	Bundesbeauftragter für den Datenschutz und die Informationsfreiheit
BGB	Bürgerliches Gesetzbuch
BGH	Bundesgerichtshof
BGHZ	Entscheidungen des Bundesgerichtshofs in Zivilsachen
BMBF	Bundesministerium für Bildung und Forschung
BMO-Ä	Berufsmusterordnung der Ärzte
BR-Drs.	Bundesratsdrucksache
BSG	Bundessozialgericht
BSI	Bundesamt für Sicherheit in der Informationstechnik
Bsp.	Beispiel
BT-Drs.	Bundestagsdrucksache
BVerfG	Bundesverfassungsgericht
BVerfGE	Entscheidung(en) des Bundesverfassungsgerichts
BVMed	Bundesverband Medizintechnologie e.V.
bzw.	beziehungsweise
CAN	Controller Area Network
c.i.c.	culpa in contrahendo
COBIT	Control Objectives for Information and Related Technology
CR	Computer und Recht
CT	Computertomographie
d.h.	das heißt

DRG	Diagnosis Related Groups
DSL	Digital Subscriber Line
DuD	Datenschutz und Datensicherheit
EBM	einheitlicher Bewertungsmaßstab
EDIFACT	United Nations Electronic Data Interchange For Administration, Commerce and Transport
EDV	elektronische Datenverarbeitung
EG	Europäische Gemeinschaft
EGBGB	Einführungsgesetz zum Bürgerlichen Gesetzbuche
etc.	et cetera
EU	Europäische Union
e.V.	eingetragener Verein
EWR	Europäischer Wirtschaftsraum
f.	folgende
ff.	fortfolgende
FIDIS	Future of Identity in the Information Society
GBA	Gemeinsamer Bundesausschuss
gem.	gemäß
GG	Grundgesetz
ggf.	gegebenenfalls
GKV	gesetzliche Krankenversicherung
GmbH	Gesellschaft mit beschränkter Haftung
GOÄ	Gebührenordnung für Ärzte
GOZ	Gebührenordnung für Zahnärzte
GPRS	General Packet Radio Service
GPS	Global Positioning System
GPV	gesetzliche Pflegeversicherung
GSM	Global System for Mobile Communications
HilfsM-RL	Hilfsmittel-Richtlinie
Hrsg.	Herausgeber
HWG	Heilmittelwerbegesetz
i.d.R.	in der Regel
IFIP	International Federation for Information Processing
IP	Internet Protocol
i.S.d.	im Sinne des

ISDN	Integrated Services Digital Network
IT	Informationstechnik
ITIL	Information Technology Infrastructure Library
i.V.m.	in Verbindung mit
JZ	JuristenZeitung
KV	Kassenärztliche Vereinigung
KWG	Gesetz über das Kreditwesen
LBS	Location Based Services
LG	Landgericht
LNCS	Lecture Notes in Computer Science
MBO-Ä	(Muster-)Berufsordnung für die deutschen Ärztinnen und Ärzte
MDK	Medizinischer Dienst der Krankenversicherung
MittRhNotK	Mitteilungen der Rheinischen Notarkammer
MMR	Multimedia und Recht
MPG	Medizinproduktegesetz
MRT	Magnetresonanztomographie
m.w.N.	mit weiteren Nachweisen
NJW	Neue Juristische Wochenschrift
Nr.	Nummer
NVwZ	Neue Zeitschrift für Verwaltungsrecht
NZV	Neue Zeitschrift für Verkehrsrecht
o.g.	oben genannt
PDA	Personal Digital Assistant
PRIME	Privacy and Identity Management for Europe
ProdHaftG	Produkthaftungsgesetz (Gesetz über die Haftung für fehlerhafte Produkte)
RDV	Recht der Datenverarbeitung
Rn.	Randnummer
RöV	Röntgenverordnung
S.	Seite
SächsDSG	Sächsisches Datenschutzgesetz
SGB	Sozialgesetzbuch
SMS	Short Message Service
s.o.	siehe oben
s.u.	siehe unten

SOAinVO	Chancen und Risiken von Service-orientierten Architekturen in Virtuellen Organisationen
sog.	sogenannt
SozR	Sozialrecht
St.	Sankt
StGB	Strafgesetzbuch
StPO	Strafprozessordnung
TAUCIS	Technikfolgen-Abschätzung Ubiquitäres Computing und Informationelle Selbstbestimmung
TDG	Teledienstegesetz
TK	Telekommunikation
TKG	Telekommunikationsgesetz
TM	Telemedien
TMF	Technologie- und Methodenplattform für die vernetzte medizinische Forschung
TMG	Telemediengesetz
u.a.	unter anderem
ULD	Unabhängiges Landeszentrum für Datenschutz Schleswig-Holstein
UML	Unified Modeling Language
usw.	und so weiter
u.U.	unter Umständen
UWG	Gesetz gegen den unlauteren Wettbewerb
v.a.	vor allem
vgl.	vergleiche
Vol.	Volume
WG	Working Group
WP	Working Paper
z.B.	zum Beispiel