Datenschutz bei Ambient Assist Living (AAL) durch Anwendung der Neuen Schutzziele

Martin Rost
Unabhängiges Landeszentrum für Datenschutz Schleswig-Holstein, Kiel
martin.rost@datenschutzzentrum.de

Kurzfassung

Der Einsatz von „Ambient Assisted Living"-Technik (AAL) kann bedeuten, dass den Menschen die Wahrnehmung ihres Rechts auf informationelle Selbstbestimmung erheblich erschwert wird. Denn sie begeben sich mit AAL in die Hand industrialisierter Beobachtungen durch Maschinen und, derart vermittelt, dann letztlich in die Entscheidungshoheit von zumeist privaten Organisationen. Durch eine hohe Abhängigkeit von Technik und Organisation Freiheit zu gewinnen, zählt in Industriegesellschaften allerdings zur Normalität. Und: Sich als Mensch technikgestützt an Orten aufhalten zu können, an denen man sich am liebsten aufhält, also etwa lieber zuhause als in einem Pflegeheim, ist unbezweifelt ein zu berücksichtigender relevanter Aspekt informationeller Selbstbestimmung. AAL bedeutet aber auch die logische Weiterentwicklung der bereits in gang gesetzten Technisierung und Ökonomisierung der Betreuung von Menschen. Durch überstürzte, rein technikgetriebene Projektentwicklungen im Rahmen des AAL droht die Überschreitung einer Grenze, die unmittelbar die Würde des Menschen antastet. Darüber hinaus ist aus Datenschutzsicht auch der gesellschaftlich relevante Aspekt der Standardisierung des Normallebens auf der Grundlage von AAL-Messdaten zu betrachten. Solche aus Messdaten geformten Profile setzen Menschen unter einen freiheitsdeformierenden Rechtfertigungsdruck, sobald ihr Verhalten und Handeln vom Standardprofil abweicht. Die Umsetzung der „Neuen Datenschutz-Schutzziele" in den derzeit massiv anlaufenden AAL-Pilotprojekten könnte helfen, AAL in Deutschland auf den paradigmatisch richtigen Weg der Achtung der Würde des Menschen zu bringen.

1 Das Problem

Systeme, die den Kernbereich privater Lebensgestaltung beobachten und unter Umständen anhand dieser Beobachtungen Entscheidungen von möglicherweise sogar lebensrettender, damit auch: lebensbedrohlicher, Tragweite für Menschen treffen, berühren notwendig deren Recht auf informationelle Selbstbestimmung. Dieses Recht wird vom Bundesverfassungsgericht aus dem Artikel 2 Abs. 1 i.V.m. Artikel 1 Abs. 1 des Grundgesetzes abgeleitet. Die Würde des Menschen ist unantastbar. Sie gilt für einen jeden Menschen innerhalb der Reichweite des Grundgesetzes immer, ganz gleich, in welcher sozialen, medizinischen oder mentalen Verfassung ein Mensch sich befindet. Das Recht auf informationelle Selbstbestimmung von einzelnen Menschen muss gegenüber „starken" Organisationen, die sich letztlich an Kapitalverzinsung, Machtausbau, Rechtssicherheit oder Wissensgewinnung orientieren müssen, durchgesetzt werden. Die Tätigkeit des institutionalisierten Datenschutzes besteht deshalb darin, die Angemessenheit der Informationsverarbeitung und Kommunikation von Organisationen mit ihrer Klientel zu prüfen und zu bewerten. Eine Datenverarbeitung ist immer eine soziale Aktivität, die, auch bei unterstellt besten Motiven der Betreiber, gegenüber den Betroffenen nicht mit der Naturwüchsigkeit eines Wettergeschehens erfolgen darf bzw. von diesen ertragen werden muss.

Aus der Sicht des Datenschutzrechts ist es für die Belange des AAL maßgeblich auszuweisen, welche Instanz zu welchem Zeitpunkt die personenbezogenen Daten erhebt, sie kontrolliert und auswertet. Hier gilt zunächst einmal der Grundsatz „Meine Daten gehören mir." Sie gehören gerade nicht voraussetzungslos etwa der Organisation, die beispielsweise die Sensorik oder das Auswertungssystem beim Betroffenen betreibt und die die Daten in diesem Sinne technisch erzeugt und rechtlich erhebt.

Sofern für die Verarbeitung personenbezogener Daten keine gesetzliche Regelung vorliegt, die vorrangig wäre, kann die Verarbeitung rechtlich nur auf der Grundlage einer Einwilligung geschehen. An die Qualität der Einwilligung eines Betroffenen gegenüber der Organisation werden einige Anforderungen gestellt: So muss eine Person einsichtsfähig sein; die Einwilligung bedarf der Schriftform, sie muss freiwillig gegeben werden; die die Einwilligung beantragende, verantwortliche Stelle hat die Pflicht zur Aufklärung des Betroffenen und diese Aufklärung muss hinreichend bestimmt sein. Damit diese Anforderungen entsprechend umgesetzt werden können, muss das System, mit dem personenbezogene Daten erhoben und verarbeitet werden, seinerseits bestimmten Anforderungen genügen. Während die Einwilligung auf die Regelung der besonderen Umstände im Verhältnisses zwischen einem Betroffenen und einer Organisation abzielt, gibt es auch ganz generelle Erwartungen an den Betrieb solcher technischen Systeme, die normalerweise nicht explizit in Verträge aufgenommen werden.

Generell erwarten Menschen im Alltag, dass Organisationen insbesondere den Betrieb ihrer technischen Systeme beherrschen und dass es für die von dem Betrieb Betroffenen fair zugeht. Unter Beherrschbarkeit ist dabei nicht nur die Fähigkeit zu verstehen, dass der technisch notwendige Betrieb beherrscht wird, sondern dass eine Organisation auch die sie umgebenden rechtlichen, ökologischen und ergonomischen Rahmenbedingungen berücksichtigt. Nur dann dürfen Organisationen erwarten und voraussetzen, dass die von ihren Tätigkeiten abhängigen Betroffenen ihnen vertrauen. Gerade AAL-Systeme sind

angesichts ihrer Klientel in einem besonderen Maße darauf angewiesen, dass beanspruchtes Vertrauen auch gewährt wird.
Sowohl zur Regelung der konkreten Umstände einer Datenverarbeitung als auch zur Erfüllung der geschilderten alltäglich-allgemeinen Erwartungen eines Bürgers, Kunden oder im Falle von AAL eines Betreuten oder Patienten können die Schutzziele des Datenschutzes herangezogen werden.

2 Schutzziele

Sowohl für die Gestaltung spezifischer Einwilligungserklärungen als auch zur Erfüllung der generellen Erwartungen von Menschen an technische Infrastrukturen lassen sich die sogenannten *Schutzziele* nutzen. Die Schutzziele sind sowohl „normennah" als auch „technik- und organisationsnah" formuliert und auf einem allgemeinverständlichen Niveau verstehbar. Sie bilden zugleich ein Konzentrat der Anforderungen aus den nationalen und europäischen Datenschutzgesetzen und -richtlinien. Als die wesentlichen Schutzziele der Datensicherheit und des Datenschutzes, aus denen sich weitere Schutzziele methodisch ableiten lassen, gelten dabei die folgenden sechs [1,2]:

- **Verfügbarkeit**: Ein System soll seine spezifische Funktion in einem erwartbaren Rahmen erfüllen. Das bedeutet: Je lebenswichtiger eine AAL-Funktion ist, desto unwahrscheinlicher muss der Ausfall des Systems ausgelegt sein.
- **Integrität**: Ein System soll ausschließlich seine bestimmungsgemäße Funktion korrekt erfüllen, etwaige Nebenwirkungen müssen berücksichtigt sein.
- **Vertraulichkeit**: Systeme sollen ihre Funktionalität allein für den Betroffenen erbringen. Nicht zuständige, unbeteiligte Dritte dürfen keine Gelegenheit erhalten, von Daten eines AAL-Systems unbefugt Kenntnis zu bekommen. Das bedeutet u.a., dass Systeme physikalisch und IT-technisch hinreichend abgeschottet und Daten verschlüsselt sein müssen.
- **Transparenz**: Es muss für Betroffene und Betreiber eines Systems grundsätzlich jederzeit klar sein können, welche Daten erhoben werden, wem sie gehören, wie sie verarbeitet und von wem und zu welchem Zweck sie ausgewertet werden. Transparenz der Datenverarbeitung ist die unabdingbare Voraussetzung dafür, dass Betroffene, oder deren vertraute Stellvertreter, informiert in die Verarbeitung der Daten einwilligen oder dieser widersprechen können. Dies gilt insbesondere dann, wenn – wie zu erwarten – gesetzliche Regelungen fehlen.
- **Nichtverkettbarkeit**: Es muss technisch und organisatorisch sichergestellt werden, dass Daten nur für den Zweck verarbeitet und ausgewertet werden, für den sie erhoben wurden. Das bedeutet, dass Daten nicht ohne Zweckbestimmung erhoben und nicht für andere Zwecke, z.B. für Zwecke des gezielten Werbens oder für wissenschaftliche Forschung, verarbeitet werden dürfen. Es liegt auf der Hand, dass bei AAL die Verführung groß ist, beliebig viele personenbezogene, zweckunbestimmte Daten auf Vorrat zu erheben und zu speichern.
- **Intervenierbarkeit**: Der Betroffene muss so lange wie möglich und seiner Situation angemessen auch die operative Souveränität darüber innehaben, wirksam zu bestimmen, was in welchem Maße wann über ihn beobachtet wird und welche Auswirkungen diese Beobachtungen auf ihn haben (können). Schon bei der Konstruktion des ihn beobachtenden Systems muss vorgesehen werden, dass ein Betroffener die Erhebung und Kontrolle seiner Daten (zumindest vorübergehend) abschalten kann.

Die ersten drei genannten Schutzziele, *Verfügbarkeit, Integrität und Vertraulichkeit,* sind die konventionellen, seit den 80er Jahren gut verstandenen wesentlichen Schutzziele der Datensicherheit. Diese Ziele beziehen sich vor allem auf die Sicherung eines organisierten IT-Betriebs. Im Unterschied dazu nimmt Datenschutz den organisierten Betrieb zunächst aus der Perspektive der von diesem Betrieb betroffenen Personen wahr. So wie Datensicherheit ist auch Datenschutz in diesem ausgewiesenen Sinne der Schwerpunktsetzung im Zweifel parteiisch. Und dann wundert es wenig, wenn es zu Konflikten zwischen den Perspektiven des Primats der Datensicherheit oder des Primats des Datenschutzes kommen kann. Eine perfekt gesicherte Kommunikationsinfrastruktur ohne Datenschutz kann beispielsweise dazu führen, dass sich sämtliche Aktivitäten von Personen perfekt miteinander verbinden lassen, weil jede Person authentisiert wird und deren Aufenthalt, Tätigkeit und, im Falle von AAL zumeist auch deren soziale Einbindung und körperliche Verfassung, beobachtet, dokumentiert und protokolliert wird. Weil Datenschutz in Datensicherheit nicht aufgeht, haben sich die auf Datenschutz-Anforderungen hin zugespitzten speziellen Datenschutz-Schutzziele der *Transparenz, der Intervenierbarkeit und der Nichtverkettbarkeit* herausgebildet. Sowohl Datenschutz als auch Datensicherheit betrachten somit zwangsläufig die gleichen sechs Schutzziele, weil sie aufeinander bezogen sind. Allerdings betrachten sie diese aus zwei Perspektiven mit entsprechend unterschiedlich zugespitzten Aufgabenstellungen und Gewichtungen. Die Schutzziele müssen im Hinblick auf deren Bedeutung bzw. Wirkung für die betroffenen Personen bzw. für die Organisationen jeweils spezifiziert und profiliert werden. Insofern gilt: Sowohl Personen als auch Organisationen haben ihre je eigenen Interessen der Risikominimierung.
Datenschutz agiert als generalisierter Anwalt der Schutzinteressen von Personen gegenüber Organisationen in latent asymmetrischen Machtkonstellationen. Und gerade im Bereich von AAL-Systemen ist diese Machtasymmetrie zwischen Betreuten und Betreuenden ganz besonders ausgeprägt, wobei das Selbstverständnis der Betreuenden erfahrungsgemäß oftmals geradezu bedrohlich naiv ist im Sinne von „aber wir wollen doch nur helfen!". Das mag als Charakterisierung der individuellen Motivationslage auf sehr viele Betreuer zutreffen. Doch die strukturell treibende Kraft hinter den AAL-Entwicklungen ist die Notwendigkeit, die Betreuung von Menschen kostengünstiger als bislang erbringen zu können.

3 Schutzmassnahmen

Zum methodischen Konzept der Schutzziele gehört eine ganze Reihe von Komponenten und Maßnahmen zur Umsetzung der Ziele. Als ein bekanntes, vorbildliches Beispiel zur Umsetzung speziell der Schutzziele der Datensicherheit gilt die „BSI-Grundschutz"-Methodik.

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. In einem anschließend zu erstellenden *Risikobehandlungsplan* wird dann festgelegt, welche festgestellten Risiken mit welchen Maßnahmen auf dem Stand der Technik (wie) behandelt werden müssen. Während mit den Daten auch die Systeme und deren Aktivitäten gemeint sind – die Systeme erben den Schutzbedarf der mit ihrer Hilfe verarbeiteten Daten -, so sind mit den Akteuren bzw. den Beteiligten auch deren Aktivitäten und Verantwortlichkeiten gemeint. Die Schutzziele und die Schutzmaßnahmen bieten dann die Referenzwerte und Instrumente auf, anhand derer die Daten und Systeme sowie die Aktivitäten der Akteure und die Ausgestaltung der Rechtsbeziehungen untereinander beobachtet und beurteilt werden können. Die Maßnahmen der Datensicherheit eines Systems finden sich in den BSI-Grundschutz-Katalogen.

Das Schutzziel der *Verfügbarkeit* wird gemäß Grundschutz im Wesentlichen durch Redundanz und Reparatur-Strategien umgesetzt. Dieses Schutzziel zu erreichen werden alle beteiligten Organisationen bereits aus haftungsrechtlichen Gründen anstreben.

Die wesentliche Schutzmaßnahme zur Sicherung der *Integrität* 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 Integritätchecks dadurch um, indem man Informationen anhand von Vorher/Nachher-Hashwert-Vergleichen auf deren Unversehrtheit hin testet. Die Häufigkeit solcher Tests und die Gestaltung der Bewertungen von Abweichungen sind organisatorisch festzulegen.

Die wesentlichen Schutzmaßnahmen zur Sicherung von *Vertraulichkeit* bestehen darin, Daten und Systeme voneinander zu separieren und dort, wo einem unbefugtem Zugriff zu geringe Hürden entgegenstehen, Daten zu verschlüsseln. Auf organisatorischer Ebene sind Funktions- bzw. Rollentrennungen für Programme, Maschinen, Menschen und Organisationseinheiten vorzunehmen.

Zur Darstellung von Maßnahmen aus der speziellen Datenschutzperspektive lässt sich, aufgrund der noch jungen konzeptionellen Durchbrüche in der Systematik der Schutzziele [vgl. 1], leider nicht auf umfangreich ausgearbeitete Gefährdungs- und Maßnahmen-Kataloge wie die des BSI-Grundschutzes verweisen. Deshalb ist die nachfolgende Darstellung der Maßnahmen etwas höher aufgelöst.

3.1 Transparenz-Maßnahmen

Das Maßnahmenbündel zur Sicherstellung der Herstellbarkeit von Transparenz betrifft im Wesentlichen die Prüffähigkeit von Prozessen und Daten in einem System. Und das läuft im Einzelnen auf eine Dokumentation der IT-Infrastruktur, der Daten und der Datenflüsse, der Schnittstellen nach Außen und der genutzten Datenformate, der Sicherheitsmaßnahmen und der Tests und Freigaben durch die verantwortliche Organisation(seinheit) hinaus. Diese Dokumentation muss dann für sachkundige Personen in angemessener Zeit nachvollziehbar sein. Sie ist nach jeder Änderung des Systems fortzuschreiben. Die „Datenschutzverordnung Schleswig-Holstein" (DSVO-SH) schreibt darüber hinaus vor, dass eine solche Dokumentation für „mindestens fünf Jahre nach der letzten automatisierten Verarbeitung personenbezogener Daten" aufzubewahren ist [vgl. 3]. Laut DSVO-SH zählt zur IT-Dokumentation:

- der Einsatzzweck sowie die Maßnahmen zur Datenvermeidung und Datensparsamkeit,
- die für den Einsatzzweck verwendeten informationstechnischen Geräte einschließlich des Standorts,
- 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,
- das Vorliegen einer Datenverarbeitung im Auftrag einschließlich der schriftlichen Vereinbarungen hierzu,
- die Maßnahmen zur Erfüllung von Auskunftsansprüchen von Betroffenen und
- die Maßnahmen für die Berichtigung, die Löschung und die Sperrung personenbezogener Daten.

Auch die Prozesse und Regeln sind zu dokumentieren. Das bedeutet: Sämtliche Aktivitäten, nicht nur die mit einem unmittelbar ersichtlich hohen Risiko für die Betroffenen, sind zu protokollieren. Das Protokollieren umfasst Konzepte, Monitoringsysteme und Protokolldaten. Hieraus 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 Protokolldaten getroffen wurden. Zu dokumentieren ist, welche technischen und organisato-

rischen 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 Sicherheitsmaßnahmen von der Daten verarbeitenden Stelle zu dokumentieren.
Die eingesetzten informationstechnischen Geräte und Programme sowie die in der Dokumentation festgelegten Sicherheitsmaßnahmen sind außerdem vor der Aufnahme der Verarbeitung personenbezogener Daten zu testen. Die Testmaßnahmen 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 dabei 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.

3.2 Interventions-Massnahmen

Dieses Schutzziel ist durch solche Maßnahmen umzusetzen, die dem Betroffenen die Ausübung der ihm zustehenden Rechte wirksam ermöglichen. Das bedingt letztlich einen operativen Zugriff auf Verfahren und Daten, sowohl bereits in der Erhebungs- als auch in der Speicherungs- und Weitergabe-Phase. Das bedeutet im Einzelnen, dass Organisationen, die AAL-Systeme betreiben, verfügen müssen über:

- einen SPOC (Single-Point-Of-Contact) für Betroffene, zur Adressierung einer Intervention mit Verfolgbarkeitsoption. Hier ist im Sinne der Transparenz dann entscheidend, dass dem Betroffenen beispielsweise nachgewiesen werden kann, dass Daten nicht nur im System bzw. der Datenbank selbst, sondern auch in sämtlichen Kopien/ Backups gelöscht wurden.
- eine Steuerung der Prozesse des Erhebens, Nutzens, Weitergebens, Löschens von personenbezogenen Daten, mit Prüfungs-Techniken jeweils auf dem aktuellen Stand. Vorhandene Daten und laufende Verfahren müssen im Grundsatz vom Betroffenen, oder auch von einem von ihm beauftragten Stellvertreter, ausgelöst werden können und einsehbar, änderbar, korrigierbar, sperrbar, löschbar sein.
- eine Möglichkeit, die es dem Betroffen unmittelbar ermöglicht, „das System der möglichst totalen Erfassung“ in seinem Privatbereich zumindest zeitweise abzustellen („Sex-Button“).

3.3 Nichtverkettbarkeits-Massnahmen

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

- angemessene Funktions- und Rollentrennungen zwischen und innerhalb von Organisationen mit Verantwortungszuweisungen an kompetente Belegschaftsangehörige, die sich in der technischen Infrastruktur wiederfinden. Dazu zählen Mandantenfähigkeit von Datenbanken und „Isolated Service Containers“, aber auch gehärtete Computersysteme, die möglichst keine Nebenfunktionen bieten. Hier kann bspw. der Einsatz virtueller Systeme sinnvoll sein.
- Konzepte, Implementierungen, Konfigurationen, über Regelungen für die Inbetriebnahme und Außerbetriebnahme von Programmen, mit Tests und Simulationen in den jeweiligen Phasen, nach Best-Practice Gesichtspunkten.
- Techniken, die lose Kopplungen ermöglichen („Interoperability“) und eng zugeschnittene Dienste bieten (Metadirectory, Federation-Services, Service-orientierte Architekturen etc.).
- Nutzerkontrolliertes Identitätsmanagement, das über eine technisch gestützte Pseudonymnutzung gewünschte Verkettungen und Entkettungen bewirkt (hier besonders wirkungsvoll die sogenannten „anonymen Credentials“).
- fallbezogene Einrichtung und Separierbarkeit von Subprozessen, damit sich partielle Interventionen durch Betroffene oder andere „Systemstörungen“ nicht über die Grenzen des Systems hinaus auswirken.
- Löschen von Daten und Prozessen, nachdem der Zweck erfüllt wurde.

4 Idealtypische AAL-Modelle

Nimmt man die gesamte Prozesskette der Verarbeitung personenbezogener Daten in einem AAL-System, die von der automatisierten Erhebung bis zur automatisierten Auswertung durch Dritte und Abspeicherung in Archiven der Sozialforschung reichen kann, in den Blick, dann macht es Sinn, anhand von zumindest drei idealtypischen Modellen den Schutzbedarf der AAL-Daten zu unterscheiden, von denen aus dann der Schutzbedarf des gesamten Systems abzuleiten ist:
Modell A: Der Betroffene (oder ein ihm persönlich Vertrauter) steuert die Sensorik und Auswertung der Daten und trifft die Entscheidungen, was wann und wie ausgelöst wird oder zu tun ist. Die Daten verbleiben dabei ausschließlich im Zugriff des Betroffenen (und/oder des von ihm eingesetzten Vertrauten). Hier ist das AAL-Einsatz-Paradigma im Wesentlichen das des Einsatzes eines Beobachtungssystems zur Steigerung des Komforts im Sinne einer Heimautomation, die versucht, sich automatisiert auf die Bedürfnisse des Nutzers einzustellen. Der Nutzer hat die volle Souveränität über das ihn beobachtende System und die Daten.
Modell B: Der Betroffene beauftragt einen professionellen Beobachter, der eine AAL-Dienstleistung erbringen soll. Als Auftragnehmer lässt sich an einen Wachdienst, einen Pflegedienstleister, einen Arzt oder ein Krankenhaus denken. Die auftragnehmenden Organisationen haben Zugriff auf die Sensordaten (oder auch einen tieferen Zugriff auf bspw. Konfigurationen des diese Daten erzeugenden Systems) und können zudem differenziert Aktionen auslösen, bspw. telefonisch den Betroffenen zurückrufen oder Zugriff auf die Videoüberwachung in den Räumen des Betroffenen nehmen. Die Daten, seien es die

Rohdaten der Sensorik oder seien es bereits vor Ort beim Betroffenen veredelte Auswertungs-Daten, verlassen die vom Betroffenen kontrollierte Umgebung und werden operativ (aber nicht rechtlich!) zur Verfügungsmasse der professionell agierenden Beobachtungs- und Bewertungsinstanz.

Denkbar sind Mischmodelle aus Modell A und B, etwa die Einrichtung von Eskalationsstufen, mit Vorprüfung eines Alarms durch Vertraute des Betroffenen, dann Ingangsetzen von Hilfemaßnahmen durch Pflegedienstleister. Oder man denke an Selbsthilfegruppen mit Mitgliedern, die bspw. über das Internet verbunden videogestützt „gegenseitig auf sich aufpassen".

Modell C: Professionelle Beobachter, die anonymisierte Sensorik-Rohdaten, die sie selbst erfasst oder von Dritten gemäß Modell B angeliefert bekommen haben können, zu eigenen Zwecken weiterverarbeiten. Die absehbaren Interessenten an solchen Daten können Statistikämter, Versicherungen, Sicherheitsbehörden, wissenschaftliche Institute der Medizin-, Pflege- oder Sozialwissenschaften, oder auch Systemhersteller für AAL-Komponenten sein.

Es ist offensichtlich, dass in Modell A die spezifischen Datenschutzziele Transparenz, Nichtverkettbarkeit und Intervenierbarkeit ungleich leichter umzusetzen sind als im Modell B. Das Modell A ist aus Datenschutzsicht deshalb zunächst einmal unproblematisch, weil der Betroffene im Prinzip die volle Kontrolle über alle IT-Aktivitäten und Datenerzeugungen behalten kann. Hier lässt sich der Schutzbedarf der Daten mit normal ansetzen. Im Modell B müssen dagegen umfangreiche Verträge geschlossen sowie IT-Planungen und Sicherheitsvorkehrungen getroffen werden, um Datenbestände und Datenflüsse gegen unbefugte Kenntnisnahmen und unbeabsichtigte bzw. unbefugte Auswertungen zu schützen. Hier ist von einem hohen oder vielfach sogar sehr hohen Schutzbedarf der Daten auszugehen, insbesondere wenn bspw. Interventions-, Vital- oder Verhaltensdaten über Internetleitungen fließen. Eine besondere Herausforderung wird dabei spielen, welche Instanz die Verantwortlichkeit für ein Gesamtsystem einer AAL-Installation übernimmt oder wie die Verantwortlichkeit für einzelne Komponenten aufgeteilt werden kann. Geboten ist, dass nur solche Komponenten eingesetzt werden dürfen, die bestimmten Schnittstellen- und Protokollstandards genügen, die datenschutz- und datensicherheitstechnisch zertifiziert sind und die zuletzt von einer vertrauenswürdigen Instanz getestet und abgenommen worden sind.

Im Modell C gibt es zwar, sofern die Anonymisierung korrekt durchgeführt wurde, keine unmittelbare personenbezogene Datenverarbeitung (mehr), sehr wohl jedoch eine mittelbare, die den Datenschutz materiell interessieren muss: Anhand statistisch gewonnener Kennzahlen entstehen zwangsläufig Profile menschlichen Lebens in Industriegesellschaften. Solche Profile werden ebenso zwangsläufig Einzug in die Mathematik zur Berechnung von Versicherungspolicen halten. Und auch Sicherheitsbehörden werden sich dafür interessieren, unter welchen Umständen sie eine AAL-Installation bei Tatverdächtigen für die eigene Aufklärungsarbeit anzapfen können. Und dass man auch Häftlinge mit AAL billiger „Zuhause betreuen" könnte, liegt ebenso auf der Hand.

Aus all dem folgt: Abweichungen von einem durch AAL-Daten als „normal ausgewiesenen Leben" können sich für Person nachteilig auswirken. Diese durch AAL-Systeme nachweisbaren Abweichungen können darin bestehen, dass Personen sich zu wenig bewegen, rauchen, trinken, zu wenig schlafen oder sich ungesund ernähren. Wie es heute schon Alltag ist. Nur dass es derzeit noch keine Sensorik gibt, die das erfasst und keine Systeme, die das automatisiert auswerten, und damit bspw. Krankenkassen noch keine Handhabe haben, eine Kostenübernahme zu verweigern. AAL-Systeme schneiden dies alles mit. Personen stehen dann, sogar im Kernbereich ihres privaten Lebens, unter einem permanenten Rechtfertigungsdruck, der das Recht auf informationelle Selbstbestimmung materiell latent unterhöhlt. Die Vermessung der Kommunikationen der Welt, die mit Facebook und Google inzwischen ein globalindustrialisiertes Ausmaß angenommen hat, findet in AAL einen weiteren Höhepunkt mit der Vermessung des privaten Lebens, sofern es nicht gelingt, rechtzeitig datenschutzrechtliche und datenschutztechnische Vorkehrungen zu treffen.

5 Fazit

AAL stellt eine der bislang größten Herausforderung an den Datenschutz überhaupt dar, weil AAL, bei allen damit einhergehenden Wohltaten für den Einzelnen, auf die Vermessung des privaten Kernbereichs von Menschen hinausläuft. Das kann sowohl für Einzelne als auch gesellschaftlich bislang unabsehbare Folgen haben, insbesondere für die Armen und Schwachen der Gesellschaft. Es findet ein gesellschaftlich riskantes TryAndError statt. Die Motive vieler „Macher", das gilt insbesondere für die aus der Altersforschung stammenden, die zum Teil seit vielen Jahren schon mit großem Verve zur Realisierung drängen, sind allesamt bester Art. Und die wirtschaftlichen Vorteile von AAL-Systemen zur industrialisierten Betreuung von Menschen sind, wie bei anderen gesellschaftliche Industrialisierungsprojekten auch, nicht bestreitbar. AAL wird deshalb kommen. Um den drängenden Herausforderungen für den Datenschutzes konstruktiv zu begegnen und das Vertrauen der Nutzer in die Systeme herzustellen, sollten die Schutzziele des Datenschutzes und der Datensicherheit bereits frühzeitig bei der Entwicklung und Implementierung von AAL-Anwendungen beachtet und umgesetzt werden. Deren Umsetzung sorgt auf Seiten der Organisationen, dass diese die Systeme im Sinne der auf das korrekte und faire Funktionieren angewiesenen Nutzer beherrschen und einsetzen.

6 Literatur

[1] Rost, M. / Pfitzmann, A.: Datenschutz-Schutzziele - revisited; in: DuD - Datenschutz und Datensicherheit, 33. Jahrgang, Heft 6, Juli 2009, S. 353-358

[2] Rost, M. / Bock, K.: Privacy By Design und die Neuen Schutzziele; in: DuD - Datenschutz und Datensicherheit, 35. Jahrgang, Heft 1, Januar 2011, S. 30-35

[3] Datenschutzverordnung Schleswig-Holstein, https://www.datenschutzzentrum.de/dsvo/