Umsetzung eines Konzepts zum Schutz von personenbezogenen Gesundheitsdaten für eine AAL-Plattform

Axel Helmer, Enno-Edzard Steen, Lars Rölker-Denker, Marco Eichelberg, Andreas Hein

F&E-Bereich Gesundheit
OFFIS – Institut für Informatik
Escherweg 2
26121 Oldenburg
axel.helmer@offis.de
enno-edzard.steen@offis.de
lars.roelker-denker@offis.de
marco.eichelberg@offis.de
andreas.hein@offis.de

Abstract: In diesem Beitrag werden technische Komponenten des niedersächsischen Forschungsverbundes Gestaltung altersgerechter Lebenswelten (GAL) vorgestellt, die einen Beitrag zur Berücksichtigung der rechtlichen Anforderungen des Datenschutzes und der informationellen Selbstbestimmung leisten. Im Wesentlichen sind dies die persönliche Elektronische Gesundheitsakte (pEGA) und das Monitoring Control System (MCS). Die Anforderungen an den Datenschutz begründen sich auf gesetzliche Anforderungen, Privacy by Design Ansätze und abgeleitete Ambient Assisted Living (AAL-)spezifische Anforderungen. Es wird gezeigt, dass pEGA und MCS im GAL-Projekt durch ihre Funktionalitäten wesentliche Beiträge zur Wahrung von Datenschutz und informationeller Selbstbestimmung leisten.

1 Einleitung

Durch assistierende Gesundheitstechnologien stehen über den einzelnen Menschen Daten in einem Maße zur Verfügung, wie es zuvor noch nie der Fall war. Die vor allem über Sensorsysteme – unter Umständen sieben Tage in der Woche und 24 Stunden am Tag – über lange Zeiträume messbaren Daten (z. B. Vitalparameter, Daten zur Bewegung und Ortsbestimmung) bergen im Hinblick auf einen angemessenen Schutz personenbezogener Daten und auf die informationelle Selbstbestimmung des Menschen ein hohes Risiko in sich. Da es Situationen geben kann, in denen eine Aufzeichnung und Auswertung dieser Daten nicht erwünscht oder datenschutzrechtlich bedenklich ist, wird dem Bewohner im GAL[1]-Projekt eine Möglichkeit zur Verfügung gestellt, das Monitoring kontrolliert deaktivieren und aktivieren zu können. Die persönliche Elektronische

[1]Der Forschungsverbund Gestaltung altersgerechter Lebenswelten dankt dem Niedersächsischen Ministerium für Wissenschaft und Kultur für die Förderung im Rahmen des Niedersächsischen Vorab (ZN 2701).

Gesundheitsakte (pEGA) des GAL-Projekts stellt Funktionalitäten zur Speicherung und Weiterleitung von persönlichen Gesundheitsdaten bereit, die einer vertieften datenschutzrechtlichen Untersuchung bedürfen. Sie enthält Mechanismen, die den Nutzer befähigen, seine Rechte hinsichtlich des Datenschutzes und der informationellen Selbstbestimmung wahrzunehmen. Die beiden Komponenten werden zusammen mit der GAL-Systemarchitektur im folgenden Abschnitt kurz vorgestellt.

2 Die GAL Plattform

Die GAL-Plattform kapselt eine Reihe von Komponenten aus dem Bereich des AAL. Aus Sicht des Datenschutzes sind vor allem die pEGA und das Monitoring Control System (MCS) von Belang. Im Folgenden werden diese beiden Komponenten kurz skizziert.

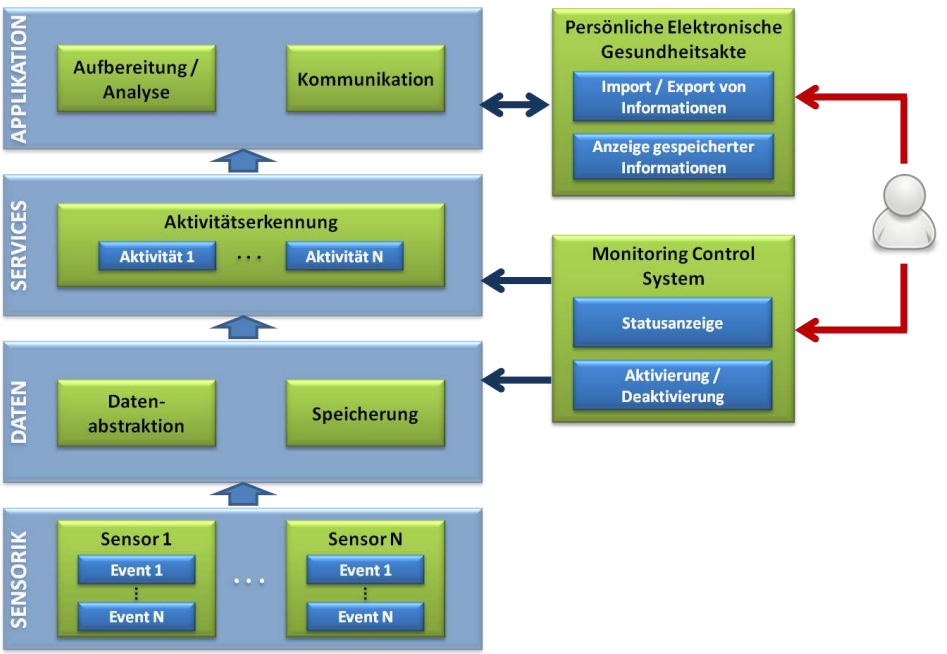

Abbildung 1: Der Nutzer kontrolliert mittels seiner Interaktionen über die persönliche Elektronische Gesundheitsakte und das Monitoring Control System die Datenflüsse innerhalb AAL-Plattform.

Beginnend mit der pEGA sollen elektronische Gesundheitsakten kurz definiert werden. Eine weithin akzeptierte Definition für elektronische Gesundheitsakten liefert Frank Warder in seinem gleichnamigen Buch [War05]:

*„Eine elektronische Gesundheitsakte, abgekürzt EGA, soll verteilt bei Leistungserbr*ingern und Patienten anfallende klinische und gesundheitsbezogene Daten eines Menschen

zusammenfassen und diese omnipräsent, lebenslang, unabhängig von Ort und Zeit allen am Behandlungsprozess Beteiligten (inkl. d*er Patienten) bedarfsgerecht präsentieren.“*

Diese Definition enthält keine Aussage darüber, wer die Verfügungsgewalt über die beschriebenen Daten innehat. Warder füllt diese Lücke in seiner folgenden Abgrenzung der elektronischen Gesundheitsakte zur elektronischen Patientenakte:

*„Wichtigstes Unterschei*dungsmerkmal der elektronischen Gesundheitsakte zur elektronischen Patientenakte ist dabei die alleinige Verfügungsgewalt des Patienten über seine *Akte und damit über seine medizinischen Daten.“*

In der gegebenen Definition wird darauf hingewiesen, dass die Daten unabhängig von Ort und Zeit präsentiert und an einer Stelle zusammengefasst werden. Damit wird weder eine Aussage über die Lokalisierung des Ortes getroffen, an dem die Daten physikalisch gespeichert sind, noch darüber, wem die Verantwortlichkeit für diese wichtige Aufgabe zufällt. Im Kontext von GAL werden die gesundheitsbezogenen Daten in einem „Residential Gateway“ im Wohnumfeld des Nutzers selbst gespeichert, dem damit auch die Rechte und Pflichten für die Verwaltung der Daten zufallen.

Abbildung 2: Bildschirmfotos der pEGA. a) Auswahl eines Nutzers, b) Medikamentenverwaltung, c) Rechteverwaltung

Die pEGA des GAL Projektes kann Daten wie etwa die aktuelle Medikation des Nutzers, seine Krankenhausaufenthalte, seine Blutgruppe etc. speichern und auf sein Verlangen an externe Akteure im Gesundheitswesen kommunizieren (siehe Abbildung 2). Der Nutzer kann die von ihm eingegebenen Daten ansehen, ändern und löschen. Weiterhin hat er die Möglichkeit, seine Daten für externe Personen freizugeben oder sich einen Export seiner wichtigsten Gesundheitsdaten erstellen zu lassen.

Weiterhin kann die pEGA auch Daten von anderen Assistenzsystemen aus dem häuslichen Bereich entgegennehmen. Dazu gehören auch die Daten der Aktivitätserkennung, mit deren Hilfe in der Entstehung begriffene Krankheiten eines Nutzers frühzeitig anhand entsprechender Verhaltensänderungen erkannt werden können. Bei diesen Datenflüssen innerhalb der AAL-Plattform setzt nun das bereits erwähnte MCS an (siehe Abbildung 1).

Das MCS ermöglicht dem Nutzer eine vorübergehende Deaktivierung der Datenaufzeichnung und –auswertung. Zum einen kann es Situationen geben, in denen der Nutzer keine Datenverarbeitung wünscht. In diesem Fall dient eine definierte Deaktivierungs- und Aktivierungsmöglichkeit dem Schutz des Systems vor anderen „Deaktivierungsoptionen“ wie dem Ziehen des Netzsteckers aus der Steckdose oder dem Verstellen von kalibrierten Komponenten. Zum anderen ist eine Deaktivierung erforderlich, wenn sich weitere Personen (Besucher, Dienstleister) in der Wohnung aufhalten und keine eindeutige Zuordbarkeit der Daten gewährleistet ist, um so das Recht dieser Personen auf informationelle Selbstbestimmung zu wahren.

Abbildung 3: Das Monitoring Control System besteht aus einer Fernbedienung (Oben Mitte), mit deren Hilfe der Nutzer die Verarbeitung seiner personenbezogenen Daten aktivieren oder deaktivieren kann. Das Display (oben links und rechts, sowie unten) zeigt den Status der Datenverarbeitung an.

Hauptbestandteile des MCS sind eine Statusanzeige (Abbildung 3) und ein Handsender im Sinne einer Fernbedienung (Abbildung 3). Konkret wurden hierfür Komponenten aus dem FS20-Funkschaltsystem der Firma ELV[2] gewählt. Die Kommunikation zwischen diesen beiden Komponenten und der MCS-Software erfolgt über die zugehörige Funkhaussteuerungszentrale. Der Nutzer kann die Datenverarbeitung mit Hilfe der Fernbedienung aktivieren und deaktivieren. Nachdem der Nutzer die entsprechende Taste der Fernbedienung gedrückt hat, werden der interne Status des MCS gemäß Nutzerwunsch aktualisiert und alle betroffenen Systemkomponenten hierüber informiert. Auf Grundlage dieser Statusaktualisierung können diese Systemkomponenten kontrolliert darauf reagieren, beispielsweise im Falle einer Deaktivierung mit der Unterbrechung ihrer Aufgaben oder mit dem Senden bzw. Verarbeiten von „Null"-Werten.

Der aktuelle Status wird dem Nutzer über die Statusanzeige signalisiert. Dabei bedeutet ein rotes Kreuz (Abbildung 3), dass die Datenverarbeitung aktuell deaktiviert ist, wohingegen ein grüner Haken (Abbildung 3) eine aktive Verarbeitung anzeigt.

Das MCS lässt sich mit Hilfe einer Konfigurationsdatei individuell einstellen. Diese Datei enthält unter anderem den Default-Status, d. h. den ersten Status nach dem Starten

[2] http://www.elv.de

des Systems. Außerdem ist in ihr angegeben, ob eine Reaktivierung eines durch den Nutzer deaktivierten Systems automatisch nach einer ebenfalls definierbaren Zeit erfolgt oder nur manuell durch den Nutzer möglich ist. Normalerweise sind lediglich zwei Tasten der Fernbedienung belegt (aktivieren, deaktivieren). Die Konfigurationsdatei ermöglicht aber auch die Belegung weiterer Tasten durch zusätzliche Funktionen, zum Beispiel die Deaktivierung für einen bestimmten Zeitraum.

Bevor nun eine Beschreibung der datenschutzrechtlichen Anforderungen und umzusetzenden Konzepte für pEGA und MCS erfolgen kann, sollen die Grundlagen des Datenschutzes und der informationellen Selbstbestimmung im Allgemeinen und, darauf aufbauend, im speziellen AAL-Kontext herausgearbeitet werden.

3 Grundlagen des Datenschutzes und der informationellen Selbstbestimmung

Die gesetzliche Basis für die Anwendung des Datenschutzes ist nach dem Subsidiaritätsprinzip auf verschiedenen gesetzlichen Ebenen verortet. Im Artikel 8 der Charta der Grundrechte der Europäischen Union heißt es zum „Schutz personenbezogener Daten“:

*„(1) Jede Person hat das Recht auf Schutz der sie betreffenden personenbezogenen D*aten.

(2) Diese Daten dürfen nur nach Treu und Glauben für festgelegte Zwecke und mit Einwilligung der betroffenen Person oder auf einer sonstigen gesetzlich geregelten legitimen Grundlage verarbeitet werden. Jede Person hat das Recht, Auskunft über die sie betreffenden erhobenen Daten zu erhalten und die Berichtigung der Daten zu erwirken.

(3) Die Einhaltung dieser Vorschriften wird von einer unabhängigen Stelle überwacht.“ [PRK00]

Dieses Grundrecht ist zudem seit dem Jahr 1995 in der Richtlinie 95/46/EG verankert. Im Jahr 2001 wurde dieser Richtlinie durch die Novellierung des Bundesdatenschutzgesetzes (BDSG) Rechnung getragen. Eine weitere Novelle im Jahr 2009 verschärfte die Umsetzung der Anforderungen noch. Das Bundesdatenschutzgesetz (BDSG) trägt ebenfalls der impliziten Verankerung des Datenschutzes im deutschen Grundgesetz (GG) Rechnung. In Artikel 1 Abs. 1 GG heißt es:

"Die Würde des Menschen ist unantastbar. Sie zu achten und zu schützen ist die Verpflichtung aller staatlichen Gewalt."

Und zudem in Artikel 2 Abs. 1 GG:

"Jeder hat das Recht auf freie Entfaltung seiner Persönlichkeit, soweit er nicht die Rechte anderer verletzt und nicht gegen die verfassungsmäßige Ordnung oder das Sittengesetz verstößt."

Die Grundlage für das BDSG und auch der Landesdatenschutzgesetze (LDSG) bildet zudem noch das informationelle Selbstbestimmungsrecht, das in dem Volkszählungsurteil von 1983 als Grundrecht anerkannt wurde. In dem Urteil heißt es:

„Das Grundrecht gewährleistet insoweit die Befugnis des Einzelnen, grundsätzlich selbst über die Preisgabe und Verwendung seiner persönlichen Daten zu bestimmen. Einschränkungen dieses Rechts auf "informationelle Selbstbestimmung" sind nur im *überwiegenden Allgemeininteresse zulässig.“*

Aufbauend auf der rechtlichen Basis können sieben grundlegende Prinzipien des Datenschutzes definiert werden [Biz07]: Rechtmäßigkeit, Einwilligung, Zweckbindung, Erforderlichkeit und Datensparsamkeit, Transparenz und Rechte des Betroffenen, Datensicherheit sowie Kontrolle. Diese Prinzipien werden im Folgenden kurz dargestellt.

Rechtmäßigkeit: Erhebung, Verarbeitung und Nutzung personenbezogener Daten sind im Grundsatz immer verboten, Ausnahmen bedürfen einer ausdrücklichen Legitimation und sind nur zulässig, soweit dieses Gesetz oder eine andere Rechtsvorschrift dies erlaubt oder anordnet oder der Betroffene eingewilligt hat.

Einwilligung: Eine Einwilligung ist nur wirksam, wenn sie auf der freien Entscheidung des Betroffenen beruht; dabei ist dieser auf den vorgesehenen Zweck der Erhebung (Zweckbindung), Verarbeitung oder Nutzung sowie auf die Folgen der Verweigerung der Einwilligung hinzuweisen.

Zweckbindung: Der Grundsatz der Zweckbindung bedeutet, dass die verantwortliche Stelle für eine Zweckänderung eine gesonderte Berechtigung (Legitimation) benötigt, diese Berechtigung kann eine Einwilligung des Betroffenen oder aber eine gesetzliche Regelung sein. Der Betroffene soll wissen und entscheiden, zu welchen Zwecken seine Daten erhoben und verarbeitet werden. Die Zweckbindung verhindert, dass die verantwortliche Stelle nach der Erhebung die Daten zu anderen Zwecken verarbeitet, als für die sie erhoben worden sind und ohne dass dies für den Betroffenen erkennbar war.

Erforderlichkeit und Datensparsamkeit: Die Erforderlichkeit besagt, dass keine überflüssigen personenbezogenen Daten erhoben, verwendet oder genutzt werden dürfen. Die verantwortliche Stelle soll nur so viele personenbezogene Daten verarbeiten dürfen, wie es für den mit dem Betroffenen vereinbarten oder im Gesetz erlaubten Verwendungszweck notwendig ist.

Transparenz und Rechte des Betroffenen: Das Transparenzprinzip folgt dem Inhalt des informationellen Selbstbestimmungsrechts, dass der Betroffene wissen können soll, wer was über ihn weiß. Die Regeln zur Transparenz unterscheiden sich in Informationspflichten, bei denen die verantwortliche Stelle von sich aus aktiv werden muss (Unterrichtung und Benachrichtigung des Betroffenen), und dem Auskunftsanspruch, den der Betroffene selbst geltend machen muss.

Datensicherheit: Ziele der IT-Sicherheit und damit auch der Datensicherheit sind die Vertraulichkeit, Verfügbarkeit und Integrität personenbezogener Daten. Hier sind technische und organisatorische Maßnahmen zu unterscheiden.

Kontrolle: Die Bedeutung der Kontrolle der Verarbeitung personenbezogener Daten ergibt sich insbesondere aus der Unsichtbarkeit der Erhebung, Verarbeitung und Nutzung. Der Betroffene hat in der Regel keinen Zugriff auf die Datenverarbeitung bei der verantwortlichen Stelle, so dass er auf andere Kontrollinstitutionen angewiesen ist, damit sein Recht auf informationelle Selbstbestimmung gewahrt bleibt. Art. 29 der EG-Datenschutzrichtlinie spricht ausdrücklich von „unabhängigen Kontrollstellen", die die Mitgliedsstaaten einzurichten haben.

Ergänzt werden die rechtlichen Anforderungen an den Datenschutz um allgemeine und AAL-spezifische, abgeleitete Empfehlungen. Dies ist zunächst der Privacy by Design-Ansatz (PbD) [RB11a]. PbD besagt, dass der Datenschutz bereits in der Entwicklungsphase Berücksichtigung findet. Wesentliche Aspekte sind Privacy as Default und Privacy Embedded into Design. Privacy as Default besagt, dass bei technischen Systemen in ihrem Auslieferungszustand bzw. in der Standardeinstellung jedwede Verarbeitung personenbezogener Daten deaktiviert sein sollte. Diese muss erst separat aktiviert werden. Privacy Embedded into Design besagt, dass der Privatsphären-Schutz bereits zu Beginn eines Entwicklungsprozesses berücksichtigt wird und in allen Systembestandteilen integriert ist. Eine frühzeitige Berücksichtigung von PbD ist angezeigt, da dies zum einen im Entwurf der neuen EU-Datenschutzverordnung verankert ist [EC12] und zum anderen den Datenschutz derart im Entwicklungsprozess festschreibt, dass zukünftige rechtliche Entwicklungen in einer frühen Phase antizipiert werden können.

Aus den rechtlichen Anforderungen und allgemeinen Empfehlungen können nun noch AAL-spezifische Empfehlungen abgeleitet werden. Dies sind im Einzelnen:

- Operative Souveränität [RB11b]: Dem Endanwender ist, solange es der Gesundheitszustand ermöglicht, die operative Souveränität über die ihm assistierenden Systeme zu geben. Dies beinhaltet auch die Möglichkeit der Abschaltung aller Systeme.

- Kontrolle der Datenflüsse durch Endanwender: Für den Endanwender muss im Rahmen der informationellen Selbstbestimmung ersichtlich sein, welche Datenflüsse vorhanden sind und über welche Steuermöglichkeiten dieser verfügt [Dix09].

- Bedarfsorientierte Datenübertragung [MNS09]: Eine Datenübertragung sollte nur bei Bedarf, also beispielsweise im Notfall, während eines Monitorings oder bei Abruf von Servicediensten erfolgen. Dies impliziert, dass die Verarbeitung von Sensordaten in der häuslichen Umgebung vollzogen wird und nicht auf externen Systemen.

- Korrekturrechte [ULD10]: Dem Betroffenen soll das Recht zugestanden werden, vorhandene Daten einzusehen und korrigieren zu können. Dies kann entweder durch den Nutzer selbst oder durch einen vom Nutzer beauftragten Stellvertreter geschehen.

Im Projekt GAL wird der Ansatz verfolgt, dass zunächst alle rechtlichen Anforderungen und Empfehlungen zusammengeführt werden und die daraus resultierenden Anforderun-

gen in den betroffenen Softwarekomponenten umgesetzt werden [RKR+11]. Dieses Vorgehen gewährleistet, dass keine datenschutzrelevanten Aspekte ausgelassen werden. Im nächsten Abschnitt wird erläutert, welche Konzepte und Maßnahmen umgesetzt werden sollten, um einen gesetzeskonformen Datenschutz innerhalb von GAL sicherzustellen.

4 Umsetzung des Datenschutzkonzepts

In diesem Abschnitt wird die Umsetzung der datenschutzrechtlichen Anforderungen durch die pEGA und das MCS beschrieben. Um eine bessere Einordnung zu ermöglichen, ist die Struktur dieses Abschnitts an die im vorherigen Abschnitt eingeführte Gliederung nach [Biz07] und [GK11] angelehnt.

4.1 Rechtmäßigkeit und Einwilligung

Gesundheitsdaten stellen im Sinne des Gesetzgebers besonders schützenswerte Daten dar. Da keine Rechtsvorschrift für die Erhebung, Verarbeitung oder Nutzung der personenbezogenen Daten innerhalb der pEGA vorliegt, ist es erforderlich, eine Einwilligung bei dem Betroffenen einzuholen. Diese Einwilligung muss vor allem durch den Betroffenen selbst und freiwillig erfolgen. Hierbei ist darauf zu achten, dass der Benutzer in der erteilten Einwilligung ausreichend über den Zweck der Datenerhebung, -verarbeitung und -nutzung informiert wird. Der Aktennutzer ist zudem auf die Folgen der Verweigerung der Einwilligung hinzuweisen. Die Einwilligung sollte im Idealfall schriftlich erklärt werden. Es ist jedoch auch zulässig, sie elektronisch zu erteilen, wenn eine Methode verwendet wird, die ein sogenanntes „Opt-In“ Verfahren umsetzt.

Zudem muss der Text, in den der Betroffene eingewilligt hat, zusammen mit dem Datum und der Uhrzeit sowie identifizierenden Informationen abgespeichert werden. Weiterhin ist zu beachten, dass der Text so formuliert ist, dass der Betroffene nicht unter Druck gesetzt wird, also kein Zwang zur Einwilligung besteht. Da es sich bei Gesundheitsdaten im Sinne des Gesetzgebers um „besondere Daten“ handelt, muss bei der Einwilligung zudem klar zu erkennen sein, auf welche Daten sie sich genau bezieht.

Der Abruf der Gesundheitsdaten durch einen Dienstleister aus dem Gesundheitsbereich oder eine bekannte Person des Akteninhabers stellt ein „automatisiertes Abrufverfahren“ im Sinne des Gesetzes dar. Das bedeutet, dass eine externe Person, die die Daten von der pEGA von außen abruft, nach § 10(2) BDSG auch die Verantwortung für die Zulässigkeit des Abrufes Rechnung trägt. Das bedeutet insbesondere, dass dieser Dritte „technische und organisatorische Maßnahmen der Datensicherung“ schriftlich festzulegen hat. Die pEGA kann eine verschlüsselte Übertragung der Daten ermöglichen, hat aber keinen Einfluss darauf, was passiert, wenn diese Daten lokal auf dem empfangenen Rechner gespeichert werden. Hier muss eine entsprechende Erklärung der empfangenen Stelle eingeholt werden, in der schriftlich garantiert wird, dass für die empfangenen Daten die oben genannten Maßnahmen zur Datensicherung schriftlich definiert wurden.

Die speichernde Stelle (die pEGA) muss zudem „gewährleisten, dass die Übermittlung personenbezogener Daten durch geeignete Stichprobenverfahren festgestellt und überprüft werden kann“ (§ 10(4) BDSG)). Hier wird durch die pEGA ein entsprechendes Protokoll geführt, aus dem klar ersichtlich ist, wer wann auf welche Daten zugegriffen hat.

Auch wenn der Betroffene die Einwilligung für die Erhebung und Verarbeitung der Daten gegeben hat, so kann dies für andere Personen, die sich zeitweise in der Wohnung des Betroffenen, beispielsweise im Rahmen eines Besuches oder einer medizinischen oder pflegerischen Dienstleistung, aufhalten, nicht vorausgesetzt werden. Können die Daten nicht eindeutig der betroffenen und einwilligenden Person zugeordnet werden, was bei ambienten Sensoren der Fall ist, so hat das technische System geeignete Mechanismen vorzusehen, die Datenerhebung und -verarbeitung für diesen Zeitraum zu unterbinden. Das MCS ermöglicht dem Benutzer, in den Datenfluss der AAL-Plattform einzugreifen und die Datenverarbeitung zu unterbinden. Das MCS bietet dem Nutzer die Wahlfreiheit, den Modus (manuell oder automatisch nach einer gewissen Zeitspanne) für die Reaktivierung selbst zu bestimmen.

Probleme können sich ergeben, wenn die Aktivitätserkennung durch einen Servicedienstleister analog zu dem bekannten „Hausnotruf-Knopf“ vertrieben wird. Hier kann es sinnvoll und für die vom Patienten in Auftrag gegebene und bezahlte Serviceleistung notwendig sein, eine entsprechende Dokumentation oder Übertragung des Abschaltzeitpunktes an den Servicedienstleister vorzunehmen. Der Dienstleister könnte zur Erfüllung des Vertrages beispielsweise nach einer gewissen Zeitspanne beim Patienten anrufen und erfragen, ob nur vergessen wurde, das Monitoring zu aktivieren oder ob die länger andauernde Deaktivierung beabsichtigt ist. Alternativ kann er so nachweisen, dass das Monitoring durch den Nutzer selbst deaktiviert wurde und so plausibel machen, dass die Verantwortlichkeit für diese Zeit nicht bei ihm lag.

4.2 Zweckbindung, Erforderlichkeit und Datensparsamkeit

Im Falle der pEGA ist ein großes Spannungsfeld zwischen der Erhebung der personenbezogenen Daten des Betroffenen und der Nutzung dieser Daten zu seinem Wohle zu erkennen. Prinzipiell könnten verschiedenste Daten der persönlichen Lebensführung für eine medizinische Diagnose von Relevanz sein, jedoch ist die Vorratsdatenspeicherung verboten und auch die Zweckbindung ist in diesem Fall nur grob umrissen. Wenn solche, nicht für die primäre Versorgung bestimmten, Daten erhoben werden, dann sollte dabei immer das Informationsbedürfnis des Betroffenen selbst im Vordergrund stehen und keinesfalls medizinische Diagnosen anhand dieser Daten gestellt werden. Dies wird aber in jedem Fall bezüglich professioneller Dienstleister auch durch das Fernbehandlungsverbot gesichert. Die Nutzung der Daten für die Ableitung von automatisierten Einzelentscheidungen ist ebenfalls explizit durch den Gesetzgeber untersagt.

Durch das MCS kann Datenverarbeitung vorübergehend deaktiviert werden. Dies kann bei Anwesenheit weiterer Personen in der Wohnung des Betroffenen neben der fehlenden Einwilligung (siehe Abschnitt 4.1) auch bei nicht eindeutiger Zuordbarkeit der Daten angezeigt sein, da die erhobenen Daten in diesem Fall für höhere Dienste, beispiels-

weise die Aktivitätserkennung, unbrauchbar sind. Auch wenn sich diese Daten für andere Zwecke verwenden lassen, so widerspricht diese Nutzung jedoch unter Umständen der Zweckbindung.

4.3 Transparenz und Rechte des Betroffenen

Personenbezogene Daten sind nur bei dem Betroffenen selbst zu erheben. Die pEGA ermöglicht jedoch einen Import von Daten, die in einer Arztpraxis durch Dritte erhoben wurden. Die Entscheidung, ob diese Daten importiert werden sollen, liegt jedoch wieder bei dem Nutzer selbst. Die Verantwortung für Datensicherheit für die in der Arztpraxis erhobenen Daten trägt weiterhin die entsprechende Stelle. Eine Ausnahme stellt der physische Transportweg von der Praxis zum Patienten oder umgekehrt dar. Hier trägt der Patient die Verantwortung, insofern er selbst der Transporteur eines Datenträgers ist. Die pEGA des GAL-Projektes setzt hier auf eine Kombination von Standards, die einen sicheren offline Datenaustausch über einen USB-Stick oder eine CD-ROM ermöglichen.

Nach dem Import sollte für den Nutzer in jedem Fall nachvollziehbar sein, wer der Urheber der Daten ist, die ihm angezeigt werden und wann sie durch wen importiert wurden.

Der Betroffene ist über folgende Punkte zu unterrichten:

- Welche seiner Daten gespeichert wurden,
- welches die verantwortliche Stelle ist,
- die Zweckbestimmung der Verarbeitung und
- die Kategorien von Empfängern.

Im Falle der GAL-pEGA hat der Nutzer die Möglichkeit, seine gespeicherten Daten direkt im Web-Interface einzusehen. Er hat so die Möglichkeit, festzustellen, was über ihn gespeichert ist. Werden darüber hinausgehende Daten gespeichert, ist der Nutzer darüber zu informieren.

Werden einzelne Informationen innerhalb der pEGA für die Ausführung von Assistenzsystemen verwendet, so ist das dem Benutzer anzuzeigen und er ist bei der Erhebung auf den entsprechenden Zweck hinzuweisen.

Es muss kenntlich gemacht werden, welche Daten bei einem Export aus der pEGA in das resultierende Dokument einfließen. Wird ein solches Dokument als Ergebnis eines Exports auf einem USB-Stick gespeichert, sollte der Betroffene darauf hingewiesen werden, dass er selbst die Verantwortung für die Sicherung dieses Datenträgers trägt. Optimalerweise wird er auch zur Nutzung eines verschlüsselten Sticks aufgefordert. Die Kategorien von Empfängern müssen durch den Betroffenen selbst durch die physische Übergabe und im Falle eines gesicherten Datenträgers über die Eingabe eines Passworts oder das Setzen entsprechender Rechte bestimmbar sein. Zudem muss dem Betroffenen

kenntlich gemacht werden, dass er jederzeit das Recht hat, dritten Personen die Zugriffsrechte auf seine Daten wieder zu entziehen.

Damit der Benutzer sich informieren kann, welche seiner Daten wann von welchen Personen eingesehen wurden, sollte ihm das bereits erwähnte Protokoll zugänglich gemacht werden.

Eine bislang ungelöste Fragestellung ergibt sich aus der Tatsache, dass der Betroffene seine Daten selbst jederzeit ändern kann. Hier ergibt sich ein erhebliches Missbrauchspotential, da z. B. eine vom Patienten veränderte Medikation erhebliche Folgen zu seinen Ungunsten haben kann. Eine mögliche Lösungsstrategie könnte hier die erzwungene Dokumentation von Änderungen durch den Patienten an Daten sein, die klinischen Ursprungs sind. So wäre für die klinische Entscheidungsfindung zumindest sichergestellt, dass darauf hingewiesen wird, dass Änderungen an den Originaldaten durch den Patienten vorgenommen wurden. Ein Arzt könnte den Patienten darauf ansprechen, wobei dieser die Änderung dann begründen kann, aber nicht muss. Es bliebe dann der Urteilskraft des Arztes überlassen, wie die Änderungen zu bewerten sind und ob die Daten für die entsprechende Entscheidung noch als vertrauenswürdig einzuschätzen sind.

Die Statusanzeige in Abbildung 3 informiert den Betroffenen darüber, ob das Monitoring aktiviert oder deaktiviert ist. Hierdurch kann der Betroffene jederzeit nachvollziehen, ob die Datenverarbeitung ein- oder ausgeschaltet ist. Diese Anzeige verwendet zwei einfache und durch Form und Farbe eindeutige Symbole zur Ausgabe des aktuellen Status (rotes Kreuz für „deaktiviert“, grüner Haken für „aktiviert“), um die Verwechselungsgefahr zu minimieren.

4.5 Datensicherheit

Datensicherung bezeichnet im Sinne des Datenschutzgesetzes nicht das Backup der Daten, sondern deren Sicherheits- (engl. Security) Aspekte. Sie lassen sich anhand verschiedener Faktoren einteilen: Vertraulichkeit bezeichnet den Umstand, dass die Daten nur durch Befugte genutzt werden können. Integrität stellt sicher, dass die Daten nicht unbefugt geändert werden können. Verfügbarkeit stellt sicher, dass die Daten zu festgelegten Zeitpunkten im festgelegten Umfang genutzt werden können. Authentizität stellt sicher, dass die Datenherkunft gesichert ist. Um diese Faktoren zu gewährleisten, sind in der pEGA entsprechende technische und organisatorische Maßnahmen zu etablieren.

Beide Komponenten werden sich physisch auf einem Rechner im häuslichen Umfeld des älteren Menschen befinden. Es ist daher schwierig, eine Zutrittskontrolle zu gewährleisten. Sie müsste durch die Privatperson selbst installiert werden und sicherstellen, dass immer protokolliert wird, wer wann die Wohnung betreten und verlassen hat. Auch wird es schwierig, sicherzustellen, dass Unbefugte nicht in der Lage sind, die Hardware, auf der die Komponenten installiert sind, zu erreichen. Die Hardware sollte nach Möglichkeit nicht im Eingangsbereich des Wohnumfelds oder an einem stark frequentierten Ort untergebracht werden. Idealerweise befindet sie sich in einem Teil der Wohnung, der schwer zugänglich ist bzw. der nur so zugänglich ist, dass Personen, die ihn betreten, gesehen werden. Zudem sollte die Hardware in einem abgeschlossenen Schrank oder

einem ähnlich gesicherten Bereich untergebracht werden. Sollte es einem Angreifer dennoch gelingen, sich der Hardware zu bemächtigen, sollten die darauf gespeicherten Gesundheitsdaten auf Datenbankebene verschlüsselt abgelegt werden. Da die betroffene Person üblicherweise selbst die Zutrittsberechtigungen erteilt, ist diese besonders darauf hinzuweisen, dass entsprechende Vorsichtsmaßnahmen zu treffen sind.

Die Zugangskontrolle zu dem System kann auf technischem und organisatorischem Wege realisiert werden. Hier muss, wie bereits erwähnt, gewährleistet werden, wer wann auf das IT-System (die GAL-Plattform) Zugriff genommen hat. Die technische Zugangskontrolle wird in Bezug auf die pEGA durch ein entsprechendes Login mit Benutzername und Passwort realisiert.

Die Zugriffskontrolle auf das System wird mittels der erwähnten Logins und einem Rechtemanagementsystem, das in der pEGA implementiert wurde, realisiert. Auf der Betriebssystemebene sind entsprechend feingranulare Zugriffsrechte zu vergeben und zu verwenden. Auch hier spielt die erwähnte Protokollierung der Zugriffe eine wichtige Rolle.

Die Daten der pEGA sollen dem Betroffenen im Idealfall lebenslang zur Verfügung stehen. Es ist daher eine Möglichkeit vorzusehen, wie die Daten auf ein anderes IT-System migriert werden können. Für die Interoperabilität zwischen den Systemen spielt daher die Implementierung von Standards eine entscheidende Rolle. Zudem sollte sich die pEGA auch verwenden lassen, wenn andere Komponenten der GAL-Plattform nicht mehr funktionieren. Ein Absturz des Betriebssystems wird jedoch auch Auswirkungen auf die Verfügbarkeit der Daten der pEGA haben und ist nur schwer zu verhindern. Eine Weitergabekontrolle stellt sicher, dass personenbezogene Daten während der elektronischen Übertragung nicht unbefugt gelesen, kopiert oder verändert werden können. Die pEGA sollte daher mit dem Nutzer und auch bei der elektronischen Übertragung selbst Verschlüsselungsverfahren nach dem Stand der Technik einsetzen. Jeder Auszug der Daten aus der pEGA sollte auf einem gesicherten USB-Stick gespeichert werden und evtl. verwendete WLANs sollten ebenfalls gesichert sein.

4.6 Kontrolle

„Verfahren der automatisierten Verarbeitung personenbezogener Daten sind vor der Inbetriebnahme der zuständigen Aufsichtsbehörde zu melden, wenn kein Datenschutzbeauftragter bestellt ist…“. Dieses Verfahren bietet sich für Privatpersonen nicht an, da sie selbst die Entscheidung fällen, ob sie eine pEGA in Betrieb nehmen oder nicht. Werden die hier erhobenen Daten jedoch z. B. zu Forschungszwecken verwendet, ist ein Datenschutzbeauftragter zu bestellen oder einzuschalten. Hier muss eine entsprechende Meldung vorgenommen werden.

Da es sich bei Gesundheitsdaten um besondere Daten handelt, muss in einem solchen Fall vor der Erhebung zudem eine Vorabkontrolle durch einen Datenschutzbeauftragten vorgenommen werden.

4.7 AAL-spezifische Empfehlungen

Die Datenverarbeitung lässt sich durch das MCS steuern, d. h. die betroffenen Systemkomponenten können mit Hilfe dieser Komponente ein- und ausgeschaltet werden. Durch die Bestimmung des Default-Status durch den Benutzer ist es möglich, die Empfehlung Privacy as Default zu berücksichtigen, nach der die Verarbeitung von erhobenen Daten in der Standardeinstellung deaktiviert sein soll.

Durch die Möglichkeit zur manuellen Deaktivierung und Aktivierung des Monitorings hat der Betroffene die Verfügungsgewalt (operative Souveränität) über die für die Datenverarbeitung verantwortlichen Systemkomponenten. Hierdurch wird gewährleistet, dass der Betroffene für die Abschaltung dieser Systemkomponenten nicht „den Stecker ziehen“ muss und dass die einzelnen Systemkomponenten auf diese Statusänderung reagieren können.

Jeder Patient hat das uneingeschränkte Recht, unrichtige Daten, die über ihn gespeichert wurden, korrigieren zu lassen. Dies kann er im Falle der pEGA über die Oberfläche selbst in die Hand nehmen. Die Daten müssen zudem gelöscht werden, wenn sie für den Zweck der Verarbeitung nicht mehr benötigt werden. Beschließt also ein Nutzer, seine Gesundheitsdaten nicht mehr verwenden zu wollen, sollte ihm explizit die Möglichkeit angeboten werden, die über ihn gespeicherten Daten restlos zu löschen. Die pEGA verwaltet zwar Gesundheitsdaten, unterliegt aber wegen der Verantwortlichkeit des Patienten selbst nicht den gesetzlichen Aufbewahrungsfristen, wie sie bei Gesundheitsdaten in Arztpraxen vorgeschrieben werden. Das bedeutet, dass die Daten aus diesem Aspekt heraus auch tatsächlich gelöscht werden können, wenn der Nutzer dies wünscht. Eine Sperrung der Daten kann vorgenommen werden, wenn „Grund zu der Annahme besteht, dass durch die Löschung schutzwürdige Interessen des Betroffenen beeinträchtigt“ werden. Aus dieser Erwägung heraus sollte sichergestellt werden, dass der Akteninhaber nicht versehentlich eine Löschung angefordert hat.

5 Zusammenfassung

Um einerseits eine integrierte Versorgung zu ermöglichen und andererseits das Recht auf Informationelle Selbstbestimmung des Patienten zu ermöglichen, werden in GAL im Wesentlichen die die pEGA und das MCS verwendet. In der pEGA muss vor allem sichergestellt werden, dass der Nutzer ausreichend informiert ist, wenn er die Einwilligung zur Verarbeitung seiner Daten gibt. Auch bei der Form der Einwilligung muss die Konformität bezüglich datenschutzrechtlicher Anforderungen gewährleistet sein. Sollte ein Nutzer sich entscheiden, auch anderen Personen Zugriff auf seine Gesundheitsdaten zu gewähren, so sollte sichergestellt werden, dass die Person sich der möglichen Risiken gegenüber bewusst ist und sich nicht durch ein Abhängigkeitsverhältnis unter Druck gesetzt fühlt, der Verarbeitung seiner Daten zuzustimmen. Wenn immer möglich sollte zudem nur ein Personenkreis Zugriff auf die Daten des Patienten erhalten, der nach §203 StGB zur Geheimhaltung verpflichtet ist. Bislang ungelöst sind Fragen, die sich darauf beziehen, ob die Systeme sicherstellen müssen, dass Servicedienstleister bzw. Ärzte

informiert werden müssen, wenn das System abgeschaltet wird bzw. Daten klinischen Ursprungs durch den Patienten verändert werden.

Literaturverzeichnis

[Biz07] Johann Bizer. Sieben goldene Regeln des Datenschutzes, Datenschutz und Datensicherheit (DuD). 2007, Vol.31, Nr.5, S.350-356.

[Dix09] Alexander Dix. Informations- und datenschutzrechtliche Aspekte von Ambient Assisted Technologies – Was muss man beachten? Tagungsband Ambient Assisted Living 2009.

[EC12] Europäische Kommission. Proposal for a Regulation of the european parliament and of the council on the protection of individuals with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation). 25.01.2012

[GK11] Peter Gola, Christoph Klug, Grundzüge des Datenschutzrechts, Beck Juristischer Verlag, 2011

[MNS09] Fabio Massacci, Viet Hung Nguyen, Ayda Saidane. No Purpose, No Data: Goal-oriented Access Control for Ambient Assisted Living. ACM Workshop on Security and Privacy in Medical and Home-Care Systems (SPIMACS) 2009.

[PRK00] Das Europäische Parlament, der Rat und die Kommission. Charta der Grundrechte der Europäischen Union, 2000

[RB11a] Martin Rost, Kirsten Bock. Privacy By Design und die Neuen Schutzziele. Grundsätze, Ziele und Anforderungen. Datenschutz und Datensicherheit (DuD). 2011, Vol.35, Nr.1, S.30-35.

[RB11b] Martin Rost, Iris Brameshuber. Datenschutz in AAL-Systemen: Schutzziele und Anforderungen an ihre Umsetzung. Tagungsband Ambient Assisted Living 2011.

[RKR+11] Lars Rölker-Denker, Harald Künemund, Hartmut Remmers, Wilfried Thoben, Lars Wolf. Datenschutz im AAL-Kontext. Tagungsband Ambient Assisted Living 2011.

[ULD10] Unabhängiges Landeszentrum für Datenschutz Schleswig-Holstein. 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". 2010.

[War05] Warder, Frank Elektronische Gesundheitsakten, rheinware Verlag 2005