Blickpunkt Recht
„Juristische Fragen im Bereich Altersgerechter Assistenzsysteme“

Thilo Weichert, Leiter des ULD

4. AAL-Kongress

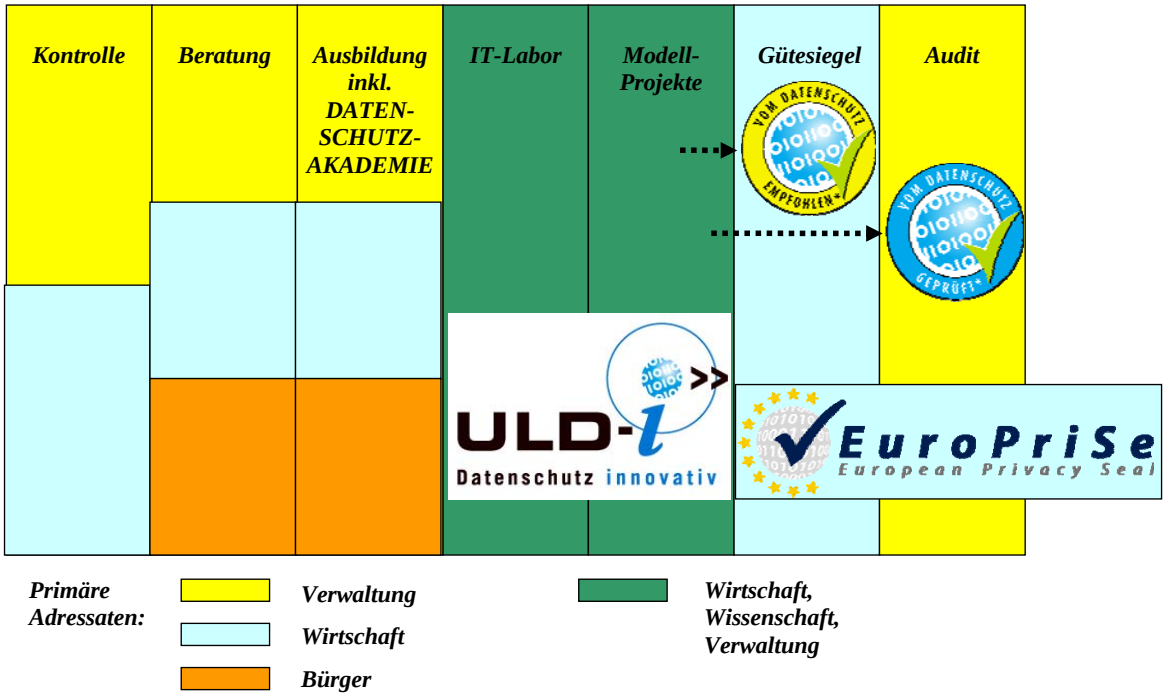
Berlin, 26.01.2011

ULD
Unabhängiges Landeszentrum für Datenschutz Schleswig-Holstein

Inhalt

- Unabhängiges Landeszentrum für Datenschutz
- Betroffene Rechtsgebiete
- Hilfsbedarfe, Rollen und Datenflüsse
- Verfassungsrechtliche Grundlagen
- Gesetzliche Grundlagen
- Einwilligung
- Betroffenenrechte und Verantwortlichkeiten
- Technisch-organisatorische Maßnahmen – Schutzziele
- Medizinische Besonderheiten
- Sonstige Rechtsgebiete
- Forderungen und Schlussfolgerungen

Unabhängiges Landeszentrum für Datenschutz



Vorstudie im Auftrag von VDI/VDE-IT

- Feststellung des verfassungsrechtlichen und gesetzlichen Rahmens von AAL-Anwendungen
- Feststellung der rechtlichen Fragestellungen und der rechtlichen Antwortmöglichkeiten
- Detektieren der offenen Fragen

Grundlage für Detailstudien

- Zielsetzung:

Rechtssicherheit für Betreiber und Anbieter

Vertrauen und Rechtssicherheit für Nutzende

Rechtsgebiete

- Datenschutzrecht (BDSG, TMG, TKG)
  Einwilligung - AAL-Nutzungsvertrag
  Transparenz, Zweckbindung, Betroffenenrechte
  Datensicherheit
- Ärztliches Berufsrecht
- Haftungsrecht, Vertragsrecht
- Sozialversicherungsrecht (SGB V, SGB XII)
- Strafverfolgungsrecht (StPO)
- Versicherungsrecht (Verbraucherrecht)

Hilfsbedarfe

- Alter
- Demenz, geistige Behinderung
- Körperliche Behinderung
- Sonstige Pflegebedürftigkeit, z.B. Krankheit, Rehabilitation
- Unterstützung im Alltag

- Tägliche Verrichtungen, Komfort
- Kommunikationserleichterung
- Verbesserung der Informationslage f. Betroffene u. Helfer
- Notfallhilfe (vor Ort, automatisches Fernwirken)

Rollen beim AAL

- Betroffener als Patient, Klient, Kunde, Nutzer, Mensch
- Privater Dritter (Nachbar, Vermieter, Familienangehöriger)
- IT-Infrastruktur-Anbieter (Acces, Content, Service)
- Medizinische und sonstige Hilfsanbieter (Arzt, Krankenhaus, Pflegedienst...)
- Mitarbeitende von IT- und Hilfsanbieter
- Öffentliche Verwaltung (110, 112, Soziales, Medizin, Datenschutz)
- Forschende
- Interessengruppen
- Öffentlichkeit

Datenflüsse

(von innen nach außen)

- Datenerhebung in Wohnung, am Körper
- Verfügung durch Betroffenen
- Verfügung durch Freund/Eltern/Familie
- Externe individuelle Dienstleistung
- Offenes Notfallmanagement und tägliche Begleitung
- Einbeziehung von Pflegeeinrichtungen/Krankenkassen u.Ä.
- Sonstige Bedarfsträger: Statistik, Kostenträger (Krankenkassen, Versicherungen), Sicherheitsbehörden, Forschung, IT-Anbieter

Verfassungsrechtliche Grundlagen I

- Art. 2 I GG: Allgemeine Handlungsfreiheit
- Art. 2 II 1 GG: Jeder hat das Recht auf Leben und körperliche Unversehrtheit
- Art. 3 III 2 GG: Niemand darf wegen seiner Behinderung benachteiligt werden
- Art. 5 GG: Informations-, Meinungs- und Pressefreiheit
- Art. 6 GG: Schutz von Ehe und Familie
- Art. 10 GG: Telekommunikationsgeheimnis
- Art. 12 GG: Berufsfreiheit (Vertraulichkeit bei Berufsausübung, Patienten- und Sozialgeheimnis)
- Art. 13 GG: Unverletzlichkeit der Wohnung

Verfassungsrechtliche Grundlagen II

Allgemeines Persönlichkeitsrecht nach Art. 2 I iVm 1 I GG (Menschenwürde, Autonomie)

- Grundrecht auf informationelle Selbstbestimmung
- Schutz der Privatsphäre, insbes. Kernbereich persönlicher Lebensgestaltung, right to be let alone
- Grundrecht auf Gewährleistung der Vertraulichkeit und Integrität eigengenutzter informationstechnischer Systeme
- Verbot von Persönlichkeitsprofil, Vorratsdatenverarbeitung, Rundumüberwachung
- Datensparsamkeit, Transparenz, Wahlfreiheit

Analog: Europäische Grundrechtecharta (insbes. Art. 8)

Gesetzliche Grundlagen

- Ärztliche Berufsordnung, § 203 StGB, MedizinprodukteG
  EU-Datenschutzrichtlinie, ePrivacy-Directive
  Bundesdatenschutzgesetz (BDSG), LDSG, SGB, SpezialR
  Telemediengesetz (TMG), TelekommunikationsG (TKG)
- Einwilligung § 4a BDSG (incl. informed consent) od.
- gesetzliche Grundlage (§§ 28 I Nr. 1, 3 IX, 28 VI-IX BDSG):
  Schutz lebenswichtiger Interessen, Gesundheitsvorsorge, medizinische Diagnostik, Gesundheitsversorgung, Behandlung, Verwaltung von Gesundheitsdiensten
- Verbot automatisierter Entscheidungen § 6a BDSG

Einwilligung I

Jede Einwilligung muss **freiwillig**, **bestimmt** und **informiert** erfolgen

- Freiwillig = frei von (innerem und äußerem) Zwang:
  - z.B. fraglich im Bereich der öffentlichen Leistungserbringung, im Krankenversicherungsrecht und in Abhängigkeitsverhältnissen, da bei Nichteinwilligung ggf. die Leistung nicht bewilligt wird oder die Befürchtung besteht, nicht die optimale Leistung zu erhalten (Behandlungsverhältnis, Pflegeverhältnis)
  - Folgen der Nichtteilnahme? (Koppelungsverbot)
  - Technikzwang?
  - Widerruflichkeit

Einwilligung II

- Bestimmt = erkennbar, was mit den personenbezogenen Daten geschieht
  - Problem bei komplexen, schnell variablen und außerhalb des Herrschaftsbereichs liegenden Systemen
  - Unbewusste, unbemerkte Erhebung der Daten?
  - Einflussmöglichkeiten (z.B. bei Besuch)?
  - Einsichtnahme in das System?
- Informiert = Information über die Daten, Stellen und Zwecke und Folgen einer Verweigerung der Einwilligung
  - Nutzergruppe + Verständlichkeit
  - Technikzwang?
  - Komplexität der Anwendung
  - „laufende“ Informiertheit

Einwilligung III

Ziele:

- kein Alleinlassen mit der Technik: Datenflüsse und ihre Steuerbarkeit sind den Nutzern transparent zu machen (Bringschuld!)
- Keine „Bevormundung“ oder „Entmündigung“ der Nutzer Höchstmaß an Selbstbestimmung und Wahlmöglichkeit der Betroffenen nötig
- Durch die Einwilligung muss tatsächlich Einfluss auf den Umgang mit den eigenen Daten ausgeübt werden können

Einwilligung IV

Lösungsansätze - Klärungsbedarfe

- Zeitliche Begrenzung der Einwilligung
- Abgestufte Einwilligungen
  - Ausschlussmöglichkeit hinsichtlich verschiedener Datenverarbeitungszwecke (Modulare Angebote z.B. bzgl. Sicherheit, Gesundheit, Soziales), Empfänger, Umfang und Art der Datenerhebung
  - Möglichkeit des zeitliches Aussetzens der Anwendung
  - Delegation/Patenschaft/Treuhänderschaft?
- Standardisierung

  Transparenz, Datenlöschung, Zweckbindung, Wahlmöglichkeiten, Berichtspflichten gegenüber Aufsichtsbehörden, technische Standards

ULD www.datenschutzzentrum.de

Bestimmungsmacht der Betroffenen I

Betroffenenrechte

- § 4 III Information über Stelle, Zweck und Empfänger
- § 34 BDSG Auskunft, Einsicht
- § 33 BDSG Benachrichtigung
- § 42a BDSG Informationspflicht bei Zwischenfällen
- § 35 I, III-V BDSG Berichtigung, Sperrung, Widerspruch
- § 35 II BDSG Löschung (u.a. bei Nichtnutzung, auf Wunsch, bei Tod)
- § 7 BDSG, §§ 823 ff. BGB Schadensersatzanspruch
- § 6 BDSG Unabdingbarkeit der Betroffenenrechte
- § 38 BDSG Anrufung Datenschutzkontrolle
- Anrufung Ärztekammer, allgemeiner Rechtsschutz

Bestimmungsmacht der Betroffenen II

Lösungsansätze – Klärungsbedarfe

Kontrollmöglichkeiten durch den Betroffenen selbst (Systemkontrolle, Anzeigen, Optionen, Dokumentation)

Interne ergänzende Kontrollen (bDSB)

Externe Kontrollen (Datenschutzbehörden)

Verantwortlichkeiten

- § 3 VII BDSG: Verantwortliche Stelle ist jede Person oder Stelle, die personenbezogene Daten für sich selbst erhebt, verarbeitet oder nutzt oder dies durch andere im Auftrag vornehmen lässt

Lösungsansätze – Klärungsbedarfe

Tatsächliche Einflussmöglichkeiten

- Nutzer/Betroffene
- Hersteller
- Betreiber
- Sog. Paten (Freund/Arzt/Krankenhaus) auf gesetzlicher, vertraglicher od. gewillkürter Grundlage?

Schutzziele

- Verfügbarkeit Maßnahme: Redundanz
- Integrität Maßnahme: Hash-Wert-Vergleiche
- Vertraulichkeit M.: Verschlüsselung, Abschottung, Rollentrennung
- Transparenz M.: Dokumentation, Protokollierung, Unterrichtung, Auskunft
- Nichtverkettbarkeit M.: Rollen- und Strukturkonzept
- Intervenierbarkeit M.: Einrichtung eines Single-Point-of Contact, Interventionsmanagement, Wahloptionen, Treuhänderverfahren

AAL-Problemkonstellationen (nach Rost)

- *Verfügbarkeit / Vertraulichkeit / Integrität*: Wem gehören die Daten sowie die technische Infrastruktur? Wer bekommt in welcher Form wie lange auf welche Systeme, Applikationen, Daten Zugriff? Wie lange werden welche Daten (roh, aggregiert, anonymisiert?) wo zu welchem Zweck (Generierung von Referenzwerten für eine „normale Lebensführung“) wie lange unter welchen Bedingungen gespeichert? Wie wird die Qualität der Daten gesichert?
- *Transparenz*: Mit welchen Instrumenten können Betreiber und Betroffene die laufenden Daten, Komponenten, Systeme überprüfen?
- *Intervenierbarkeit*: Mit welchen Instrumenten können Betroffene und Betreiber in die laufenden Systeme eingreifen, Trigger konfigurieren, Daten korrigieren, löschen, Prozesse bzw. Systeme stoppen?
- *Verkettbarkeit*: Mit welchen Prozessen lässt sich seitens der Betreiber, der Betroffenen und der Aufsichtsinstanzen prüfen, dass die AAL-DV jeweils zweckkonform stattfindet?
- Wie lässt sich phasenweise Unbeobachtbarkeit durch den Betroffenen herstellen (Sexualität)?
- Interaktion mit unbeteiligten Dritten (diese haben keine Mögl. zur Einwilligung)
- Gestaltung des gesundheitlichen Graubereichs des gesellschaftlich akzeptierten Drogenkonsums (ungesundes Essen, Bewegungsarmut, riskante Freizeitgest.)?
- Abfluss von Daten an Versicherung, Forschungsinstitute, Sicherheitsbehörden.

Rechtlich-technische Anforderungen

- Umgang mit pseudonymen Sensor- und Prozessdaten
- Sicherung der Betroffenenkontrolle
- Sicherung der Zweckbindung
- Sicherung der Transparenz

Lösungsansätze – Klärungsbedarfe
Aggregierung, Löschungspflichten, Abschottung
Verhinderung von Profilbildung
Entwicklung von Standardlösungen/Protection Profiles
Zertifizierung von AAL-Lösungen

Staatliche Infrastrukturverantwortung

- Gewährleistung der informationellen, medizinischen und sonstigen Selbstbestimmung
- Gewährleistung der Integrität und Vertraulichkeit informationstechnischer System

Lösungsansätze – Klärungsbedarfe
Festlegung von Einwilligungsumfang und -verfahren
Einführung von Treuhänder- und Patenlösungen
Verfahren zur Umsetzung der Betroffenenrechte
Begrenzung der Profilbildung
Förderung und Etablierung von Codes of Conduct

Berufliche Schweigepflicht (Patientengeheimnis)

Rechtliche Grundlage: Standesrecht, § 203 StGB

Gilt für Ärzte, Kliniken, Berufspsychologen und andere Heilberufe sowie Mitarbeiter

> Keine Aufzeichnung von Verbindungsdaten

- bei jeder Art von elektronischer Kommunikation: Keine Rückschlüsse auf die Identität der Kontaktpersonen (Patienten).
- Grund: Nur die Berufsgeheimnisträger selbst sind berechtigt, solche Daten zu speichern. Es darf also keine automatische Speicherung von E-Mail-Adressen der Patienten in Systemen geben, auf die von anderen als den Ärzten und sonstigen Schweigepflichtigen zugegriffen werden kann.
- Wo sich eine solche Speicherung nicht vermeiden lässt, gilt: Es muss eine ausdrücklich Einwilligung bzw. Entbindung von der Schweigepflicht stattfinden.

> Grds. keine Einschaltung externer Dritter (Dienstleister) ohne Einwilligung der Betroffenen einschalten, soweit personenbezogene Kenntnisnahme nicht ausgeschlossen (z.B. durch Verschlüsselung der Daten)

Medizinische Dokumentationspflichten

- Im Rahmen des Behandlungszusammenhangs in Ausübung des Berufs gemachten Feststellungen und getroffenen Maßnahmen
- Vertragliche Nebenpflicht aus Behandlungsvertrag
- Einblickrecht des Patienten
- Evtl. Beweislastumkehr zugunsten des Patienten
- Bei digitalen Dokumenten Sicherung von Unverfälschtheit und Authentizität notwendig

Lösungsansätze – Klärungsbedarfe

- Rechtliche Absicherung der Einschaltung externer Dienstleister

Haftung

- Arbeitsteilung und Komplexität der AAL-Systeme
- U.U. hohes Schadenspotenzial

Lösungsansätze – Klärungsbedarfe
Klärung der Verantwortlichkeiten
Präzise Pflichtenbeschreibung und Dokumentation
Allgemeine Einführung verschuldensunabhängiger Haftung

Sozialversicherungsrecht

- Besondere Einsparmöglichkeiten
- Besondere Leistungen und Zusatzkosten

Lösungsansätze – Klärungsbedarfe
Schaffung technikspezifischer Vergütungsregelungen

Stellvertretung/Delegation

- Sicherung der Verbindlichkeit von Festlegungen
- Delegationsbedarf
- Kontrollfähigkeit der Entscheidungsprozesse

Lösungsansätze – Klärungsbedarfe
Festlegung eines Delegationsverfahrens

Zugriffsrechte Dritter

- Möglichkeit der Datenbeschlagnahme
- Faktischer od. vertraglicher Zwang zur Vorlage von AAL-Daten an Versicherungen

Lösungsansätze – Klärungsbedarfe
Gesetzliche Beschränkung der Zugriffsmöglichkeit bzw. von Zugriffsrechten

Schlussfolgerungen

- AAL kann Informationsbasis erhöhen, Selbständigkeit wahren, Kommunikation verbessern, technisch unterstützen, schnelle Hilfe erleichtern, Kosten einsparen
- Bedarf an Standardisierungen (Schutzprofile), Zertifizierung, Verhaltensregeln und Gesetzen
- Einführung von AAL modular und sukzessiv
- Einbindung aller Interessengruppen (Betroffene, Hilfeleister, IT, Datenschutz, Kostenträger)

- Technikhilfe kann menschliche Zuwendung nicht ersetzen, sondern nur ergänzen

Blickpunkt Recht „Juristische Fragen im Bereich Altersgerechter Assistenzsysteme“

Dr. Thilo Weichert
Unabhängiges Landeszentrum für Datenschutz Schleswig-Holstein (ULD)
Independent Center for Privacy Protection Schleswig-Holstein (ICPP)
Holstenstr. 98, D- 24103 Kiel
mail@datenschutzzentrum.de
https://www.datenschutzzentrum.de