SimoBIT

Gefördert durch:

Bundesministerium
für Wirtschaft
und Technologie

aufgrund eines Beschlusses
des Deutschen Bundestages

Leitfaden

Ergebnisse des SimoBIT-Arbeitsforums

Rechts- und Haftungsfragen bei mobilen Geschäftsanwendungen

Autoren

Annette Hillebrand, WIK-Consult
Susanne Birke-Arnold, etz Stuttgart
Christiane Mayer, etz Stuttgart
Wolfgang Neifer, WIBU-Systems AG
Markus Keubke, Rechtsanwalt, Rostock
Sirin Torun, SerNet GmbH
Welf Schröter, Forum Soziale Technikgestaltung

Bad Honnef, November 2010

www.simobit.de

Inhaltsverzeichnis

Abbildungsverzeichnis **II**

Vorwort **III**

1 Welche Herausforderungen stellen Entwicklung und Einführung mobiler Geschäftsanwendungen an KMU und Verwaltung? Lösungsansätze aus den SimoBIT-Projekten **1**

2 Elektronische Signatur **4**

2.1 Elektronische Signatur im SimoBIT-Förderprojekt MAREMBA 8

2.1.1 Allgemeines 8

2.1.2 Einsatz in MAREMBA 8

2.1.3 Lösung in MAREMBA 13

2.2 Elektronische Signatur im SimoBIT-Förderprojekt VitaBIT 14

2.2.1 Ausgangslage 14

2.2.2 Ziele des SimoBIT-Förderprojekts VitaBIT 14

3 Haftungsfragen **19**

3.1 Produkthaftung bei mobilen Geschäftsanwendungen 20

3.2 Haftungsfragen in der Gesundheitswirtschaft: Das Beispiel des SimoBIT-Förderprojekts Med-on-@ix 23

3.3 Erfahrungen aus dem SimoBIT-Förderprojekt MobisPro 28

3.4 Erfahrungen aus dem SimoBIT-Förderprojekt simoKIM 30

4 Datenschutz **33**

4.1 Anforderungen des Bundesdatenschutzgesetzes in Bezug auf mobile Geschäftsanwendungen – BDSG-Novelle 2009 33

4.1.1 Strengere Anforderungen an die Auftragsdatenverarbeitung 33

4.1.2 Auftragsdatenverarbeitung - Definition und Abgrenzung 33

4.1.3 Was jetzt beachtet werden muss 34

4.1.4 Kontroll- und Dokumentationspflichten 34

4.1.5 Maßnahmen für die Praxis 35

4.1.6 Altes im neuen Gewand 36

4.1.7 Allgemeiner Handlungsbedarf 36

4.2 Datenschutz in der Telemedizin: Das Beispiel des SimoBIT-Förderprojekts Med-on-@ix 37

5 Mitbestimmung bei der Einführung mobiler Geschäftsanwendungen **40**

ZUSAMMENFASSUNG: Zentrale Rechts- und Haftungsfragen bei der Einführung mobiler Geschäftsanwendungen - Die Herausforderungen im Förderschwerpunkt SimoBIT **43**

Weiterführende Literatur und Hinweise **47**

SimoBIT-Förderprojekte im Überblick **49**

Abbildungsverzeichnis

Abbildung 1-1:	Die 12 SimoBIT-Förderprojekte	2
Abbildung 2-1:	Vertragspartner bei der Vergabe im SimoBIT-Förderprojekt MAREMBA	8
Abbildung 2-2:	Vertragspartner bei der Durchführung im SimoBIT-Förderprojekt MAREMBA	9
Abbildung 2-3:	Vertragspartner bei der Durchführung im SimoBIT-Förderprojekt MAREMBA	12
Abbildung 2-4:	Smartphone mit Sicherheitskomponente zur Anwendung im ambulanten Pflegedienst - Micro SD Card im SimoBIT-Förderprojekt VitaBIT	15
Abbildung 2-5:	VitaBIT: Plattform für sichere Kommunikation und den sicheren Informationsaustausch zwischen allen Beteiligten im Pflegeprozess	17
Abbildung 2-6:	Ablauf “Erfassen von Daten und Signatur”	17
Abbildung 3-1:	SimoBIT-Förderprojekt Med-on-@ix: Mobile Informationslösungen im deutschen Rettungsdienst	24
Abbildung 3-2:	Datenhaltung im SimoBIT-Förderprojekt simoKIM	32
Abbildung 5-1:	Datenschutz und Mitbestimmung	41

Vorwort

Mobile Geschäftsanwendungen entwickeln sich zu einer Schlüsselapplikation in Unternehmen und öffentlichen Verwaltungen. Mit ihrer Hilfe lassen sich auf allen Ebenen betrieblicher und öffentlicher Wertschöpfungsaktivitäten Prozesse vereinfachen, flexibilisieren und effizienter gestalten. Zwar dominieren heute noch eher einfache Anwendungen wie Sprachtelefonie, SMS und E-Mail die mobile Geschäftskommunikation, aber die Entwicklungen und Lösungen der zwölf SimoBIT-Projekte zeigen, dass durch den ubiquitären und jederzeitigen Zugriff beispielsweise auf Patienteninformationen oder auf Geo- und Planungsdaten, die Qualität der ambulanten Pflege, die Effizienz landwirtschaftlicher Prozesse oder die Effizienz unternehmerischer Entscheidungen deutlich erhöht werden können.

Es bestehen somit hohe Erfolgsaussichten, dass sich durch mobile Geschäftsanwendungen über alle Branchen hinweg sowohl erhebliche Kosten- und Zeitersparnisse als auch beachtliche Produktivitäts- und Qualitätsgewinne bei der Reorganisation von Wertschöpfungs- und Fachprozessen realisieren lassen. Durch die Optimierung des Personaleinsatzes, Einsparungen in der Logistik und die Verbesserung der Datenqualität beim Kunden vor Ort wird nicht nur die Wettbewerbsfähigkeit von Unternehmen, sondern auch die Effizienz vieler Verwaltungsorganisationen nachhaltig gesteigert.

Angesichts der enormen volkswirtschaftlichen Bedeutung von mobilen Geschäftsanwendungen hat das Bundesministerium für Wirtschaft und Technologie (BMWi) 2006 die Förderinitiative SimoBIT ins Leben gerufen. SimoBIT steht für „Sichere Anwendungen der mobilen Informationstechnik zur Wertschöpfungssteigerung in Mittelstand und Verwaltung“. Die Zielsetzung von SimoBIT besteht darin, durch eine nahtlose Integration von IT-Sicherheit in mobile Technologien und Anwendungen die Implementierung von mobilen Anwendungen in bestehende betriebliche und verwaltungsorganisatorische Strukturen zu erleichtern und zu beschleunigen.

Um eine möglichst effiziente Umsetzung der Förderung zu sichern und einen breiten Transfer der Ergebnisse und Lösungen in den Markt zu gewährleisten und dadurch eine Möglichkeit zur erfolgreichen Nachahmung zu eröffnen, wurde im Frühjahr 2009 das SimoBIT-Arbeitsforum Rechts- und Haftungsfragen ins Leben gerufen, bestehend aus Fachleuten der einzelnen SimoBIT-Förderprojekte sowie weiterer externer Experten. Die Ergebnisse dieses Arbeitsforums werden mit dem vorliegenden Leitfaden dokumentiert. Er basiert auf den konkreten Erfahrungen der Projekte und der SimoBIT-Begleitforschung sowie den Ausarbeitungen und Diskussionen im Rahmen von Arbeitstreffen und Workshops.

Die Themenstellung dieses Arbeitsforums war besonders breit. Sie reicht von der Frage nach den Erfahrungen beim Einsatz elektronischer Signaturen, den Anforderungen des Bundesdatenschutzgesetzes (BDSG) in Bezug auf die Geschäftstätigkeit der Entwickler und Anbieter innovativer mobiler Geschäftsanwendungen bis hin zu konkreteren Frage-

stellungen, wie z. B. welche Daten auf welche Weise genutzt werden dürfen, wenn Dienstleister Daten aus unterschiedlichen Quellen miteinander verschneiden oder was genau bei Datenverlust oder Datenveränderung geschieht. Wer muss haften, wenn Daten verloren gehen? Gibt es gesonderte Haftungsproblematiken in mobilen Anwendungsbereichen wie etwa dem Gesundheitswesen? Wie ist das informationelle Selbstbestimmungsrecht der Beschäftigten in einer mobilen Arbeitswelt zu berücksichtigen?

Es liegt im Wesen der Rechtsentwicklung, dass viele dieser Fragen in der Regel nur generisch beantwortet werden können und am Ende einer konkreten Überprüfung durch gerichtliche Entscheidungen unterfallen. Insofern hat der vorliegende Leitfaden insbesondere die Aufgabe, interessierte Anbieter und Anwender für die mit der Einführung von mobilen Geschäftsanwendungen verbundenen Fragen nach den rechtlichen Rahmenbedingungen sowie den möglichen Rechtsfolgen zu sensibilisieren.

Die Verantwortung für die Inhalte des Leitfadens liegt bei der Patin des Arbeitsforums sowie bei den weiteren Autoren. Ihnen sei an dieser Stelle herzlich gedankt für ihr großes Engagement.

Dr. Franz Büllingen
Leiter der SimoBIT-Begleitforschung

1 Welche Herausforderungen stellen Entwicklung und Einführung mobiler Geschäftsanwendungen an KMU und Verwaltung? Lösungsansätze aus den SimoBIT-Projekten

Sichere mobile Geschäftsanwendungen – immer, überall und für jede Organisation: diese Entwicklung bedeutet neue Chancen, zu mehr Wertschöpfung und zu branchenübergreifenden Produktivitäts- und Qualitätsgewinnen, die durch sichere mobile Anwendungen der Informations- und Kommunikationstechnologien (IKT) in kleinen und mittleren Unternehmen (KMU) sowie öffentlichen Verwaltungen entstehen.

SimoBIT ist ein Förderschwerpunkt des Bundesministeriums für Wirtschaft und Technologie (BMWi) zur *sicheren Anwendung der mobilen Informationstechnik (IT) zur Wertschöpfungssteigerung in Mittelstand und Verwaltung.* Gefördert werden zwölf ausgewählte Forschungs- und Entwicklungsprojekte zur Entwicklung von mobilen Lösungen in den Bereichen Maschinenbau, Handwerk bzw. kleine und mittelständische Unternehmen, Gesundheitswirtschaft und der öffentlichen Verwaltung. Ziel ist es, die Entfaltung des Potenzials mobiler Multimedia-Dienste voranzutreiben, um ihre Potenziale zur Produktivitäts- und Qualitätssteigerungen sowie Kosten- und Zeiteinsparungen auszuschöpfen. Bestehende Prozess- und Wertschöpfungsketten sollen optimiert und reorganisiert beziehungsweise neu erschlossen werden. Einen besonders hohen Stellenwert haben im Rahmen der Förderprojekte Konzepte zur Gewährleistung von IT-Sicherheit.

Die SimoBIT-Leuchtturmprojekte machen deutlich, dass IT-Sicherheit die Basis für die Ausschöpfung der hohen Einsparpotenziale ist. Denn nur wenn Vertraulichkeit, Integrität und hohe Zuverlässigkeit gegeben sind, werden die neuen mobilen IKT-Systeme eingesetzt. Datensicherheit und Datenschutz sind damit eine maßgebliche Voraussetzung für die schnelle Verbreitung von mobilen IT-Geschäftsanwendungen.

Während der Laufzeit des SimoBIT-Projektes wurden zu den Rechts- und Haftungsfragen von der SimoBIT-Begleitforschung zwei Workshops organisiert zu den Themen:

- Elektronische Signatur
- Haftungsfragen bei mobilen Geschäftsanwendungen

Vorträge zum Download unter www.simobit.de

Die Ergebnisse der SimoBIT-Förderprojekte machen deutlich, dass IT-Sicherheit immer mehrseitig ist und neben technischen und organisatorischen Aspekten immer auch Rechts- und Haftungsfragen zu adressieren sind.

Obwohl die zwölf SimoBIT-Förderprojekte in ganz verschiedenen Branchen – Gesundheitswirtschaft, Maschinenbau, Öffentliche Verwaltung, Handwerk und KMU – umgesetzt wurden, lassen sich in Bezug auf Rechts- und Haftungsfragen Gemeinsamkeiten feststellen, deren Diskussion auch für kleine und mittlere Unternehmen nicht nur aus der jeweiligen Branche wertvolle Hinweise bietet.

Abbildung 1-1: Die 12 SimoBIT-Förderprojekte

Gesundheits-wirtschaft	Maschinen-bau	Öffentliche Verwaltung	Handwerk und kl. Unternehmen
▸ Med-on-@ix ▸ VitaBIT ▸ OPAL Health	▸ Mobile Ser-vicewelten ▸ SiWear ▸ R2B	▸ Mobis Pro ▸ simoKIM ▸ Mobility@ forest	▸ MAREMBA ▸ ModiFrame ▸ M3V

Quelle: SimoBIT

Mobile Geschäftsprozesse und die diesem Phänomen zugrunde liegenden Rechts- und Haftungsfragen finden jedoch bisher in der öffentlichen Diskussion wenig Beachtung. In der Überzeugung, dass sich der Trend Mobilität und Mobiles Arbeiten in Ausprägungen wie

- Ressourcen on Demand (z. B. Cloud Computing, Web-Anwendungen, Online-Datenbanken („Verschneiden von Informationen"), Thin Clients),
- Individualisierung (z. B. SOA - Service-Oriented Architecture),
- Veränderung der Lebens- und Arbeitswelten (z. B. Personalisierung, Location based Services, „Hypervernetzte"),
- und die damit verbundenen Anforderungen an Datenschutz und IT-Sicherheit

fortsetzt und in Zukunft noch verstärkt, will der vorliegende Leitfaden dazu beitragen, dass sich Unternehmen mit Rechts- und Haftungsfragen auseinandersetzen und deren Herausforderungen für die Mobilisierung ihrer Geschäftsprozesse erkennen.

Der vorliegende SimoBIT-Leitfaden behandelt Fragen wie z. B.:

- Welche Erfahrungen mit dem Einsatz elektronischer Signaturen liegen vor? Welche Einsatzmöglichkeiten bestehen im Bereich qualifizierte vs. elektronische Signatur?
- Welche Anforderungen stellt das Bundesdatenschutzgesetz (BDSG) in Bezug auf die Geschäftstätigkeit der Entwickler und Anbieter von innovativen mobilen Geschäftsanwendungen?
- Welche Daten darf man wie nutzen, wenn Dienstleister Daten von unterschiedlichen Stellen miteinander verschneiden?

- Was passiert bei Datenverlust, -veränderung u.ä. und den daraus resultierenden Folgen? Wer muss haften, wenn Daten verloren gehen? Was ist im Rahmen der „üblichen“ Haftpflichtversicherung abgedeckt, was nicht?
- Manche Projekte setzen in ihren Lösungen auf bestehende Datenquellen. Gibt es eine eindeutige Aussage zur Haftung bei fehlerhaften oder veralteten Daten und sich daraus ergebenden Fehlentscheidungen?
- Welche besondere Haftungsproblematik besteht im Bereich Gesundheitswesen und mobile Geschäftsanwendungen?
- Was verändert sich durch mobile Geschäftsanwendungen in der Arbeitswelt?
- Wie ist das informationelle Selbstbestimmungsrecht der Beschäftigten in einer mobilen Arbeitswelt zu berücksichtigen?
- Benötigt man z. B. eine Betriebs- bzw. Dienstvereinbarungen, wenn mobile Endgeräte eingesetzt werden?

Dieser Leitfaden basiert auf den Erkenntnissen der zwölf SimoBIT-Förderprojekte während der letzten vier Jahre in ihren jeweiligen Innovationsentwicklungen sowie auf Vorträgen und anderen Beiträgen von Experten während der SimoBIT-Workshops im Rahmen des SimoBIT-Arbeitsforums Rechts- und Haftungsfragen. Betreut wurde das Arbeitsforum von Annette Hillebrand, WIK-Consult, SimoBIT-Begleitforschung.

Der Leitfaden richtet sich an Entwickler und Anwender von mobilen Geschäftsanwendungen. Er adressiert ebenso KMU wie die öffentliche Verwaltung. Der Fokus liegt dabei auf Fragen im Zusammenhang mit der Authentifizierung, Integrität und Autorisierung unter Verwendung elektronischer Signaturen, auf datenschutzrechtlichen Aspekten, Haftungsfragen sowie Fragen der Mitbestimmung bei der Implementierung mobiler Geschäftsprozesse. Im Vordergrund steht dabei, zentrale rechtliche Aspekte herauszustellen und ihre praktische technisch-organisatorische Umsetzung im jeweiligen Förderprojekt zu erläutern.

Der vorliegende Leitfaden will für die Problematik sensibilisieren und Hinweise zur Beantwortung geben. Eine individuelle Rechtsberatung für Entwickler und Anwender mobiler Geschäftsanwendungen kann und will der Leitfaden nicht ersetzen.

2 Elektronische Signatur

Die Integrität von Daten und die Authentifizierung des Absenders ist eine wichtige Voraussetzung für die Abwicklung verbindlicher Informations- und Kommunikationsprozesse. Die eigenhändige Unterschrift übernimmt die Funktion der Nachweisbarkeit und Nichtabstreitbarkeit in der „Papierwelt“. Diese Unterschrift ist über Jahrhunderte zu einem integrierten Bestandteil von Kommunikation geworden. Bei der Implementierung mobiler Geschäftsprozesse stellt sich die Frage, wie diese Funktion in der „virtuellen Welt“ nachgebildet werden kann.

Digitale Signaturen sind kein Äquivalent zu einer eigenhändigen Unterschrift per se. Dazu werden sie vielmehr erst, wenn sie gesellschaftlich und rechtlich in demselben Bedeutungskontext stehen. Ihre Einsatzgebiete sind vielfältig.

Für bestimmte Bereiche stellt der Gesetzgeber spezifische Anforderungen an digitale Signaturen. In Deutschland erfüllen nur **qualifizierte elektronische Signaturen** gemäß § 2 Nr. 3 Signaturgesetz (SigG) die Anforderungen an die elektronische Form gemäß § 126a BGB, die die gesetzlich vorgeschriebene Schriftform ersetzen kann.

In Fällen, in denen die Schriftform und damit eine qualifizierte elektronische Signatur nicht vorgeschrieben ist, ist eine so genannte **fortgeschrittene elektronische Signatur** gemäß § 2 Nr. 2 SigG ausreichend.

Der Gesetzgeber hat dadurch die Option geschaffen, eine Vielfalt von technischen Lösungen realisierbar zu machen, die Kommunikations- und Geschäftsbeziehungen absichern können. Entwickler und Anwender sind dadurch in die Lage versetzt, unter Kosten-Nutzen-Abwägungen die für sie beste Lösung für ihre Mobile Business-Anwendung auszuwählen.

Eine neue Möglichkeit steht seit Ende 2010 durch den neuen Personalausweis im Scheckkartenformat zur Verfügung. Die Online-Ausweisfunktion basiert auf dem Prinzip des gegenseitigen Ausweisens, wonach beide Seiten auf die angegebene Identität ihres Gegenübers vertrauen können: Mit einem staatlich ausgestellten Berechtigungszertifikat ist es für Dienstleister im Internet technisch möglich, auf Ausweisdaten zuzugreifen. Im Berechtigungszertifikat ist zusätzlich hinterlegt, welche Datenkategorien (z.B. Name, Adresse, Geburtsjahr) abgefragt werden können.

*Ab November 2010 wird der **neue Personalausweis** den bisherigen Personalausweis ablösen.*

***Ausweisen im Internet:** Der neue Personalausweis ist mit der Funktion des elektronischen Identitätsnachweises zum Online-Ausweisen ausgerüstet. Damit können Prozesse wie z. B. Log-in oder Alters- und Wohnortbestätigung wirtschaftlicher und schneller realisiert werden. Nur berechtigte Anbieter von Dienstleistungen dürfen die Daten des Ausweises abfragen. Der Ausweisinhaber selbst behält die Kontrolle darüber, welche seiner persönlichen Daten an den Anbieter übermittelt werden.*

***Elektronische Signatur:** Die Ausweisinhaber können ein Zertifikat für die qualifizierte elektronische Signatur auf ihren Personalausweis – von einem Zertifikat-Anbieter Ihrer Wahl – laden. Damit sollen auch Dienste, die eine eigenhändige Unterschrift erfordern, medienbruchfrei, sicher und preiswert auf dem elektronischen Wege in Anspruch genommen werden.*

www.bmwi.bund.de

Es bleibt noch abzuwarten, inwieweit diese bald in der gesamten Bevölkerung ab 16 Jahren vorhandene elektronische Funktionen des Identifizierens und des digitalen Unterschreibens künftig in Anwendungen des mobilen E-Government, aber auch beim mobilen Online-Shopping, Online-Banking oder beim Online-Kauf von Tickets integriert werden und inwieweit diese Option von Dienstleitungsanbietern und Nutzern angenommen wird.

Zertifikatsbasierte Systeme stellen insbesondere für KMU und Handwerk Technologien zur Verfügung, die mobile IT-Sicherheit für diese Unternehmen gewährleisten. Die SimoBIT-Projekte haben unterschiedliche Wege gefunden, um zertifikatsbasierte Lösungen zur Erhöhung der IT-Sicherheit und zur Schaffung von mehr Rechtssicherheit zu integrieren. Nicht in jedem Fall ist eine eigenhändige Unterschrift bzw. eine qualifizierte elektronische Signatur erforderlich.[1] Darüber hinaus zeigen die Erfahrungen aus den Projekten, dass mehrere, parallel eingesetzte unterschiedliche Verfahren zum Identitätsnachweis den Bedienkomfort für die Benutzer einer Mobile Business-Anwendung erhöhen.

Das Angebot, Identifizierungslösung plus qualifizierte elektronische Signatur auf einer Karte zu vereinen, trägt der Tatsache Rechnung, dass heute bei ca. 80 Prozent der potenziellen Signaturanwendungen eine Identifizierung ausreichend ist. Die Erfordernis, ein Äquivalent zur händischen Unterschrift zu nutzen, besteht nur bei einem Fünftel der Anwendungen.

Bei der Entwicklung von Lösungen für das digitale Unterschreiben übernehmen die SimoBIT-Projektverbünde eine wichtige Vorreiterfunktion. Diese Anforderung stellt sich schon bald für alle Unternehmen. Ab 2010 sollen EU-weit alle öffentlichen Aufträge nur noch elektronisch ausgeschrieben werden.

Vorträge des SimoBIT-Workshops „Elektronische Signatur“

Neue technische Lösungen bei elektronischer Signatur

Experten-Workshop zu Authentifizierungslösungen

Download unter *www.simobit.de*

Experten aus Politik, Forschung und Industrie diskutierten am 2. Oktober 2010 am Elektro Technologie Zentrum (etz) in Stuttgart auf Einladung von SimoBIT die Möglichkeiten und Potenziale der elektronischen Signatur für mobile Anwendungen in Wirtschaft und öffentlicher Verwaltung.

Vier externe Experten stellten die aktuellen rechtlichen und technischen Entwicklungen auf dem Gebiet des elektronischen Unterschreibens vor und erläuterten ihr Vorgehen bei der organisatorischen Implementierung von Signaturanwendungen. Abschließend präsentierten zwei SimoBIT-Förderprojekte den Stand ihrer Authentifizierungslösungen.

1 Vgl. dazu auch den Leitfaden des SimoBIT-Arbeitsforums IT-Sicherheit, insbes. den Beitrag von Decker, M.; Günther, J.; Kunoth, R. (2010): Mobile IT-Sicherheit in Handwerk und KMU: Digitale Zertifikate für sichere mobile Anwendungen, Bad Honnef, www.simobit.de

Elektronischer Personalausweis ab 2010

„Der elektronische Personalausweis und die elektronische Signatur – Stand und Ausblick“, Andreas Reisen, Referatsleiter Pass- und Ausweiswesen, Bundesministerium des Innern

Ab November 2010 wird der elektronische Personalausweis im Scheckkartenformat den bisherigen Personalausweis ablösen. Erstmals wird ein hoheitliches Ausweisdokument mit der Möglichkeit des elektronischen Identitätsnachweises kombiniert. Damit werden die Bürgerinnen und Bürger zukünftig auch in der elektronischen Welt über eine sichere Identität verfügen. Nicht zu verwechseln ist diese neue Funktion mit der qualifizierten elektronischen Signatur. Aber auch hier hilft das neue Ausweisdokument. Die Ausweisinhaber können zusätzlich ein Zertifikat für die qualifizierte elektronische Signatur auf ihren Personalausweis laden. Der elektronische Personalausweis wird die Sicherheit und den Komfort von E-Business und E-Government durch die beiden neuen Funktionen für alle deutlich erhöhen.

Kritische Masse: „Henne-Ei“-Problem

„IT-sicherheitsrelevante Erfahrungen in der Anwendung der Elektronischen Signatur“ - Uwe Bendisch, Leiter des Fraunhofer Competence Center PKI, berichtete über die Herausforderungen an die Benutzerfreundlichkeit.

Bei der Einführung einer Signaturlösung für die rund 15.000 Mitarbeiter bei Fraunhofer handelt es sich um eine hardware-basierte PKI-Lösung mit fortgeschrittener Signatur. Jeder Mitarbeiter erhält eine Multifunktionskarte mit Foto und Namen, die er für Anwendungen wie z. B. Personalangelegenheiten (Urlaub, Zeiterfassung u. ä.) sowie für Sicherheitsanwendungen verwenden kann. Ziele sind u.a. die „Elektronifizierung“ von Geschäftsprozessen sowie eine starke Authentifizierung für das Mitarbeiter-Portal. Als externer Vertrauensanker dient ein selbst-signiertes Zertifikat des akkreditierten Zertifizierungsdienste-Anbieters T-Systems / Telesec; dadurch sind Zertifikate auch von Außenstehenden überprüfbar.

Das „Henne-Ei“-Problem der Verbreitung elektronischer Signaturkarten beim Nutzer kann in einer nach außen abgegrenzten Anwendungsumgebung leicht durch Nutzungsvorschriften gelöst werden. Hohe Anforderungen an die Usability und an die Kosteneffizienz bleiben jedoch auch bestehen, wenn die Anwendung für Mitarbeiter verpflichtend ist. Da die einzelnen Institute der Organisation die jeweiligen Kosten selbst tragen müssen, wurde der Nutzen einer kritischen Prüfung unterworfen. Der Rollout war bisher sehr erfolgreich.

Akzeptanz

Jochen Knaab, Leiter Produktmanagement, S-Trust, legte in einer Gegenüberstellung der qualifizierten und fortgeschrittenen elektronischen Signatur sowie in einem Ausblick zum Thema „Softwarezertifikatslösungen“ den aktuellen Stand und die künftige Entwicklung in diesem Bereich dar.

Die technische Lösung des Deutschen Sparkassenverlages S-Trust wurde in dem Beitrag vorgestellt. Prinzipiell sind heute etwa 45 Mio. Bank-Chipkarten für die elektronische Signatur einsetzbar. Zurzeit mangelt es aber noch an Anwendungen.

Die zögerliche Nutzung der Bank-Karten für elektronische Signaturen zeigt, dass in der Vergangenheit zwar die technischen Möglichkeiten beim Kunden vorhanden waren, mangels konkreter Massenanwendungen für alle jedoch der breite Einsatz einer digitalen Unterschrift unterblieb.

Die Ursache sehen Experten nicht zuletzt in der mangelnden Akzeptanz beim Kunden. Alle Verträge sind „seit Jahrhunderten“ händisch ausgefertigt, sie sind schriftlich und griffig. Die neuen elektronischen Lösungen greifen in Gewohnheiten der Menschen ein und werden nur zurückhaltend angenommen – eine Tatsache, die Anbieter abwarten lässt, bevor sie in eine elektronische Unterschriftslösung investieren. Wie zögerlich selbst viele Bankkunden Neuerungen gegenüberstehen, belegt etwa die Tatsache, dass nur 20% aller Sparkassenkarten tatsächlich am POS – Point of Sales in Gebrauch sind.

Die „Anforderungen und technische Lösungen bei elektronischem Rechnungsversand und digitaler Signatur“ stellte Frank Schulz, Vertriebsleiter, eviatec Systems AG, vor.

Die Existenz von Akzeptanzhürden im Zusammenhang mit technischen Lösungen beim elektronischen Rechnungsversand und bei der digitalen Signatur ist nicht von der Hand zu weisen. Kernfrage ist für viele Anbieter, wie die Kunden auf die elektronische Rechnung reagieren. Manche Anbieter haben Bedenken, Nutzungshürden aufzubauen, die sich letztlich in einem Auftragsrückgang niederschlagen könnten. Trotz nachweisbarer Kosteneinsparungen auf beiden Seiten und funktionierender technischer Lösungen ist daher die Bereitschaft, neue Wege zu gehen nicht immer vorhanden.

Lösungen zur elektronischen Unterschrift bei SimoBIT vorgestellt

Die SimoBIT-Förderprojekte zeigen, so Christiane Mayer, etz Stuttgart, Projektleiterin MAREMBA, dass insbesondere kleine und mittlere Unternehmen sowie Verwaltungen vom Einsatz innovativer Technologien und neuer IT-Sicherheitskonzepte profitieren. Handwerksunternehmen geraten durch die Umstellung auf eine elektronische Auftragsvergabe zunehmend unter Handlungsdruck und benötigen Unterstützung bei der Umsetzung von technischen Lösungen. Ziel des Projekts ist die Entwicklung eines prozessübergreifenden Ressourcenmanagementsystems für die gemeinsame Bauauftragsabwicklung von Handwerkernetzwerken, das auch mobil nutzbar ist. Im Pilotbetrieb wird die fortgeschrittene elektronische Signatur im Modul Vergabe und die einfache elektronische Unterschrift im Modul Durchführung und im Modul Service erfolgreich eingesetzt.

Die Anforderungen an die Sicherheit der mobilen Anwendungen und die damit verbundenen Herausforderungen für das Unterschreiben in einer digitalen Umgebung bei ambulanten Pflegediensten lassen sich im Projekt VitaBIT anschaulich demonstrieren, stellte Wolfgang Neifer, Business Development, WIBU-SYSTEMS, Konsortialführer VitaBIT, heraus. VitaBIT entwickelt eine offene Plattform für sichere Anwendungen mobiler Informationsdienste in der Pflegelogistik. Ein Vorteil von VitaBIT ist, dass die Krankenpfleger vor Ort sämtliche Daten des Betreuten während des Pflegeablaufs eingeben und in einem zentralen Rechenzentrum ablegen, auf das nur autorisierte Personen Zugriff haben. Mittels eines Dokustifts erfasste Pflege-Daten werden nach dem Upload in einer zentralen Datenbank elektronisch signiert und erhalten einen Zeitstempel.

2.1 Elektronische Signatur im SimoBIT-Förderprojekt MAREMBA

Susanne Birke-Arnold, Christiane Mayer, etz Stuttgart, SimoBIT-Förderprojekt MAREMBA

2.1.1 Allgemeines

Die Entwicklung der Informations- und Kommunikationstechnik eröffnet neue Möglichkeiten des Informationsaustausches und der wirtschaftlichen Betätigung. Warenbestellungen, Zahlungsanweisungen an Banken, Anträge oder Einsprüche bei Behörden, die Übermittlung sensitiver Daten im medizinischen Bereich und eine Vielzahl weiterer Kommunikationsbeziehungen sowohl in formfreien als auch in formgebundenen öffentlich-rechtlichen Bereichen, die in der Vergangenheit über Papier abgewickelt wurden, erfolgen bereits zu einem großen Teil auf elektronischem Wege.

Da sich die Dokumentationserstellung, Kommunikation und Archivierung auf der Basis digitaler Daten etabliert hat und expandiert, ergibt sich der dringende Bedarf nach einer digitalen Lösung, die einerseits den Anforderungen einer offenen Kommunikation (in der sich die Teilnehmer nicht kennen müssen) gerecht wird, bei der andererseits zuverlässig auf den Urheber geschlossen werden kann und die Daten vor unbemerkter Veränderung geschützt sind. Diese Forderungen erfüllt die **qualifizierte elektronische Signatur** (QES).

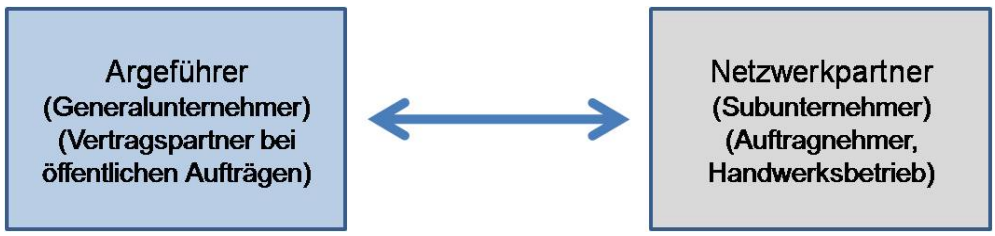
2.1.2 Einsatz in MAREMBA

In den nachfolgenden Prozessen ist die Verwendung der digitalen Signatur zwingend vorgegeben. Die einzelnen Phasen können ohne entsprechende Signatur nicht abgeschlossen werden.

Phase 1 Vergabe

Vertragspartner bei der Vergabe

Abbildung 2-1: Vertragspartner bei der Vergabe im SimoBIT-Förderprojekt MAREMBA



Quelle: MAREMBA

Eine **qualifizierte elektronische Signatur** wird auf Basis eines qualifizierten Zertifikates mittels einer sicheren Signaturerstellungseinheit erstellt. Bei dieser höchsten Sicherheitsstufe der elektronischen Signatur wird die Signatur ihrem Urheber über ein qualifiziertes Zertifikat zugeordnet.

Eine qualifizierte elektronische Signatur ist immer dann erforderlich, wenn die gesetzlich geforderte eigenhändige Unterschrift mit der elektronischen Unterschrift ersetzt werden kann und so geleistet werden soll.

Die **qualifizierte elektronische Signatur** ist in Deutschland durch das Signaturgesetz der eigenhändigen Unterschrift rechtlich gleichgestellt. Die technischen Anforderungen sind gesetzlich geregelt und unterstehen der Kontrolle durch die Bundesnetzagentur - BNetzA.

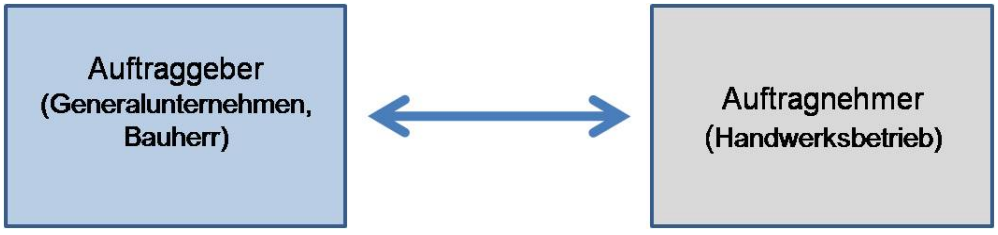
Im Bereich der E-Vergabe hat sich neben der **qualifizierten elektronischen Signatur** noch eine weitere elektronische Signatur durchgesetzt, die **fortgeschrittene elektronische Signatur**.

Durch die Vergaberechtsreform 2006 ist die fortgeschrittene elektronische Signatur ebenfalls für die elektronische Angebotsabgabe im öffentlichen Bereich zugelassen. Die **fortgeschrittene elektronische Signatur** wird mit elektronischen Mitteln erstellt und sichert die Echtheit des Dokuments und dessen Herkunft. Änderungen an unterzeichneten Daten müssen erkennbar sein. Die tatsächliche Sicherheit einer fortgeschrittenen elektronischen Signatur ist jedoch von dem eingesetzten Signaturverfahren, den verwendeten Software- und Hardwarekomponenten und der Sorgfalt der Anwender bei der Signaturerstellung abhängig.

Phase 2 Durchführung

Vertragspartner bei der Durchführung

Abbildung 2-2: Vertragspartner bei der Durchführung im SimoBIT-Förderprojekt MAREMBA



Quelle: MAREMBA

Jedoch entstehen in jeder Phase, die ein Bauwerk von der ersten Planung bis zur Fertigstellung durchläuft, bei allen Fachbereichen Informationen, die aktuell für den Bauablauf verfügbar sein müssen und deren Rechtsgültigkeit sichergestellt sein muss. Daher ist eine Vielzahl von signierten Dokumenten als Nachweis für erbrachte Leistungen erforderlich, insbesondere unter Einbeziehung der VOB/B (**Vertragsordnung für Bauleistungen**). Für den handwerklichen Unternehmer, der den Löwenanteil seines Umsatzes mit Bauleistungen erbringt, wird die Vereinbarung der VOB/B immer die bessere Vertragskonstellation darstellen. Dazu sind aber Kenntnisse über die VOB/B und deren Anwendung notwendiges Grundwissen.

Aufmaß

Das Aufmaß ist die einseitige oder gemeinsame Feststellung der erbrachten Leistungen als Abrechnungsgrundlage. Gemäß den Vorgaben der VOB/B sollte die Aufmaßerstellung gemeinsam durch die Vertragsparteien erbracht werden. Darüber ist ein Protokoll zu erstellen und mit den Unterschriften der beiden Vertragsparteien zu versehen. Die darin dokumentierten Massen sind dann die für beide Seiten verbindliche Rechnungsgrundlage.

Abnahme

Nach Fertigstellung der Arbeiten gilt die **Abnahme** als wesentlichste Handlung zur Vertragserfüllung. Die wesentlichen Merkmale bestehen in dem zu erstellenden Werk (Erfolg) des AN, d. h., er muss die versprochene, vertraglich definierte Leistung hergestellt haben und diese bei der Abnahme dem Auftraggeber (AG) übergeben oder zugängig machen. Diese **Abnahme** bedeutet rein rechtlich die Entgegennahme - verbunden mit der Anerkennung des Werkes - durch den AG als in der Hauptsache vertragsgemäß. Durch die erfolgte **Abnahme** wird der Vertrag bezüglich des Leistungsinhalts abgeschlossen.

Die Abnahme bedeutet im Einzelnen:

- **Umkehr der Beweislast**

Bis zur Abnahme hat der AN nachzuweisen, dass seine installierte Leistung mangelfrei ist, mit der erfolgten Abnahme hat der AG nachzuweisen, dass ein Mangel besteht (hier vor allen Dingen maßgeblich bei einer Mängelrüge während der Gewährleistungsfristen).

- **Gefahrübergang**

Der Schutz seiner installierten Leistung vor Diebstahl, Beschädigung etc. ist Pflicht des AN und gemäß der VOB/C DIN 18 299/18 015/18 382 unentgeltliche Nebenleistung. Mit erfolgter Abnahme muss der AG dafür Sorge tragen, dass sein Eigentum nicht beschädigt wird.

Zur weiteren Gefahrenteilung dient die Teilabnahme, die nur für in sich abgeschlossene Bereiche gefordert werden kann.

- **Beginn der Gewährleistung**

Ab dem Zeitpunkt der Abnahme beginnt die Gewährleistung, deren Ende im förmlichen Abnahmeprotokoll formuliert wird. Der Tag der Abnahme ist der erste Gewährleistungstag.

- **Ausschluss von Vorbehalten**

Da die Abnahme die faktische Beendigung der Werkleistung darstellt, müssen weitere Forderungen vor oder in dieser Beendigung vorbehalten werden. Diese sind in der Regel die verwirkte Vertragsstrafe oder weitere Schadensersatzansprüche des AG, die der AG als Gegenrechnung zur Schlussrechnung geltend machen will. Das kann nur erfolgen, wenn diese Forderungen im Abnahmeprotokoll definiert sind. Im nachfolgend abgedruckten Abnahmeprotokoll fehlt dieses, in der Regel bei anderen Abnahmeformularen vorhandene, Ankreuzkästchen. Soweit der AG sich die entsprechenden Rechte nicht ordnungsgemäß vorbehalten hat, verliert er bei einer Abnahme trotz Kenntnis vorhandener Mängel die Gewährleistungsansprüche (§ 640 Abs. 2 BGB).

- **Ende der Vorleistungspflicht des AN / Fälligkeit der Vergütung**

Da dem AN erst mit der Abnahme ein Zahlungsanspruch zusteht, muss er seine Leistung mit Material und Personal bis zur Abnahme (Lösung: Abschlagszahlung nach VOB/B § 16 Nr.1, vertraglich vereinbarte Vorauszahlung) vorfinanzieren.

Laut den gesetzlichen Vorgaben des BGBs steht dem Handwerker die vereinbarte Vergütung erst dann zu, wenn der AG die Werkleistung abgenommen hat. Nach diesen Vorgaben kann der AN, wenn er dem AG nach erfolgreicher Abnahme die Rechnung übergibt, seine Vergütung sofort verlangen. Im VOB/B- Vertrag wird die Vergütung erst nach spätestens zwei Monaten fällig.

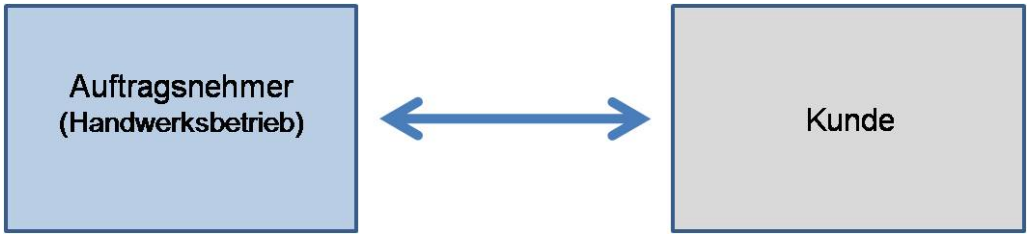
In den meisten Fällen, bei denen der AN auf sein Geld wartet, mangelt es an der **Abnahme**. Damit besteht aber das Problem, dass die Forderungen nicht gerichtlich geltend gemacht werden können, da die Vergütung ohne Nachweis der Abnahme nicht fällig ist.

Zur Steigerung der Effizienz des Mahnwesens und des Inkassos ist es maßgeblich von Bedeutung, die Abnahme durchgeführt und **schriftlich** niedergelegt zu haben.

Phase 3 Service

Vertragspartner bei Service

Abbildung 2-3: Vertragspartner bei der Durchführung im SimoBIT-Förderprojekt MAREMBA



Quelle: MAREMBA

Finden Arbeiten statt, bei denen kein schriftlicher Werkvertrag zugrunde liegt, ist meistens der Nachweis, dass ein Vertrag besteht und die daraus entstandene Vergütung strittig.

Im Allgemeinen ruft der Kunde beim Handwerker an, schildert sein Problem und bittet um Abhilfe. Wenn telefonisch bereits die Vergütung geklärt ist, kommt zu diesem Zeitpunkt ein Vertrag fernmündlich zustande. Der Nachweis, dass ein Vertrag mit diesem Kunden besteht, muss vom AN erbracht werden.

Um solche Arbeiten rechtssicher anschließend auch vergütet zu bekommen, ist es sinnvoll vor der Ausführung den Kunden zur schriftlichen Auftragserteilung zu bewegen.

Hierbei müssen die Verrechnungssätze und Fahrkosten auf dem Formular enthalten sein. Zudem können bei diesem neuen Vertragsschluss vertraglich die eigenen allgemeinen Geschäftsbedingungen mit vereinbart werden.

Anders verhält es sich bei der Durchführung von vertraglich vereinbarten Wartungsleistungen. In diesem Fall liegt ein nach BGB geregelter Dienstvertrag zugrunde.

In beiden Fällen hat der Kunde nach Ausführung der Arbeiten durch seine Unterschrift die geleistete Arbeit anzuerkennen und bei erfolgreich durchgeführten Arbeiten die Abnahme zu erteilen.

2.1.3 Lösung in MAREMBA

Qualifizierte elektronische Signatur

Um eine elektronische Unterschrift zu erstellen, werden drei Komponenten benötigt:

- eine Signaturkarte (mit digitalem Zertifikat),
- ein Kartenlesegerät,
- eine entsprechende Software.

Das Signaturgesetz stellt auch die Anforderungen an Hard- und Software auf, die bei der Erstellung einer qualifizierten elektronischen Signatur Verwendung finden müssen, um eine rechtskonforme Signatur zu erzeugen. Rechtsgültige Signaturen können nur unter Verwendung solcher Produkte erzeugt werden, die von der BNetzA bestätigt sind.

Die Beschaffungskosten hierfür betragen ca. € 170,00 – 250,00 je nach Lieferumfang (Soft- und Hardware)

Fortgeschrittene elektronische Signatur

Zur Beschaffung muss ein entsprechendes Antragsformular, welches über das Internet bzw. die Sparkassen erhältlich ist, ausgefüllt werden. Dieses muss dann mit einer Kopie des Personalausweises an S-Trust gesendet werden.

Nach abgeschlossener Zertifikatsbeantragung erhält der Antragsteller eine Benachrichtigungs-E-Mail, die darüber informiert, dass das S-TRUST-Personenzertifikat zum Download bereitsteht.

Die Beschaffungskosten hierfür betragen ca. € 70,00.

Umsetzung

Um die Handhabung und den finanziellen Aufwand für eine digitale Signatur im Hinblick auf die Netzwerkpartner so gering wie möglich zu halten, wird bei den unterschiedlichen Phasen die **fortgeschrittene elektronische Signatur** eingesetzt. Jedoch ist die Plattform so gestaltet, dass jederzeit auch die **qualifizierte elektronische Signatur** eingesetzt werden kann.

Erfahrungen haben auch gezeigt, dass der praktische Umgang mit der fortgeschrittenen elektronischen Signatur für die Netzwerkpartner weniger aufwendig erscheint. Dies erhöht die Bereitschaft zur Nutzung.

Die Plattform ist so gestaltet, dass die Unterschrift jederzeit sowohl an stationären Endgeräten als auch über ein mobiles Endgerät erfolgen kann.

2.2 Elektronische Signatur im SimoBIT-Förderprojekt VitaBIT

Wolfgang Neifer, WIBU-Systems AG, SimoBIT-Förderprojekt VitaBIT

2.2.1 Ausgangslage

Im Sinne einer möglichst menschenwürdigen Betreuung und wegen der hohen Kosten der stationären Pflege sollten die Menschen so lange wie möglich in ihrer eigenen Wohnung behandelt werden können. Aufgrund der steigenden Zahl der Pflegefälle sind die Pflegedienste mittlerweile stark überlastet. Die Dokumentation der Pflegeleistungen erfolgt meist zeitaufwendig ausschließlich per Hand, aufgrund dessen sich oftmals Fehler unter Zeitdruck einschleichen. Die Kommunikation mit Ärzten und Krankenhäusern ist ebenso verbesserungswürdig wie die Bereitstellung verwertbarer Daten. Zeitersparnis zu erzielen, um mehr Zeit für fachgerechte Betreuung zu haben und öfter mal ein persönliches Wort mit dem Betreuten wechseln zu können, wäre sicher ein wünschenswerter Zustand.

Das im Juli 2007 gestartete SimoBIT-Förderprojekt VitaBIT beschäftigt sich mit der zentralen Frage, wie ambulante Pflege bereits heute effizienter, qualitativ hochwertiger und damit kostensparender gestaltet werden kann.

2.2.2 Ziele des SimoBIT-Förderprojekts VitaBIT

Ziel ist es, über die Realisierung mobiler und plattformübergreifender Dienste in der ambulanten Pflege die Mobilität der Pflegemitarbeiter zu erhöhen, Routinetätigkeiten und Bürokratie mittels IT-gestützter Services abzubauen, die Arbeitsprozesse zu flexibilisieren und durch eine orts- und zeitnahe Bereitstellung von Dienstleistungen und kontextsensitivem Wissen, die Pflegequalität deutlich zu erhöhen.

Innovation

Die Neuentwicklung besteht in einer offenen, mobilen und effizient vernetzten Plattform, an die beliebig viele Dienste angeschlossen werden können. Dazu zählen im Bereich der Pflege die Dokumentation, Telemedizin, Kommunikation und Sicherheitselemente. Künftig soll es möglich sein, über die Anbindung von Sensoren und mobilen Endgeräten, Vitaldaten des Patienten in Echtzeit zu erfassen und direkt in einer digitalen Pflegeakte zu hinterlegen. Dort sind die medizinischen Daten permanent archiviert und können jederzeit eingesehen beziehungsweise aktualisiert werden. Realisiert wird auch die Verknüpfung zu Arztpraxen und Krankenhäusern. Auf diese Weise können Pflege- und medizinisches Personal den Gesundheitszustand des Patienten ständig überwachen und im Notfall wesentlich schneller reagieren. Der Einsatz eines digitalen Stiftes soll überdies die genaue Dokumentation der erbrachten Leistungen garantieren - Zeiter-

fassung und Leistungsnachweis erfolgen heute mitunter recht willkürlich und unpräzise. Die geplante Synchronisation der IT-Systeme in der Zentrale des Pflegedienstes mit den mobilen Endgeräten der Mitarbeiter direkt am Einsatzort wird zum einen verwaltungstechnische Prozesse, wie die Leistungs- und Dienstplanung oder das Abrechnungswesen, vereinfachen. Andererseits wird der Pflegedienstmitarbeiter auch von Erleichterungen in der täglichen Praxis profitieren, wenn er auf seinem mobilen Endgerät über detailgetreue Geoinformationen verfügt. Damit lassen sich etwa Tourenplanung und Navigation wesentlich effizienter gestalten. Als mobiles Endgerät eignet sich sehr gut das Mobiltelefon, da es ohnehin mitgeführt wird, ein zusätzliches Gerät obsolet macht und einfach zu bedienen ist.

Sicherheitsaspekte

In Gesundheits- und Pflegefragen geht es um besonders sensible Daten, die entsprechend geschützt werden müssen. Hier müssen Vertraulichkeit, Integrität und Authentizität unbedingt gewährleistet sein. Deshalb kommt die weit verbreitete SD-Karte (SD Card) zum Einsatz. In der kleinsten Bauform ist dies auch eine Micro SD Card, die heute in sehr vielen Mobiltelefonen gebräuchlich ist. Das besondere an der Karte ist der integrierte CodeMeter Sicherheitschip, der den Zugriff auf die Patientendaten im System exakt festlegt und steuert. Zudem müssen im Pflegevertrag dahingehend Anpassungen vorgenommen werden, dass der Betreute dem Einsatz der neuen Möglichkeiten der mobilen Lösung zustimmt.

Abbildung 2-4: Smartphone mit Sicherheitskomponente zur Anwendung im ambulanten Pflegedienst - Micro SD Card im SimoBIT-Förderprojekt VitaBIT

Quelle: WIBU-Systems AG

Mobile Anwendung für Pflegekräfte

Über das Mobiltelefon hat die Pflegefachkraft die Möglichkeit den Tourenplan sowie sämtliche Daten des zu pflegenden Patienten abzurufen. Mit einem digitalen Stift der DokuStift GmbH dokumentiert die Pflegekraft während der Arbeit wie gewohnt die durchgeführten Pflegemaßnahmen. Am Ende des Tages werden alle Daten des DokuStifts in die zentrale VitaBIT-Datenbank übertragen und der elektronischen Akte zugeordnet.

Der Einsatz drahtloser Messgeräte mit einer Schnittstelle zu der oben beschriebenen mobilen Lösung ermöglicht es, dass die Vitalwerte digital erfasst und damit auch ausgewertet werden können. Mit einer entsprechenden Logik ist es dann möglich, große Abweichungen in den erfassten Vitalwerten zu identifizieren und z. B. dem betreuenden Arzt automatisch eine Benachrichtigung zukommen zu lassen.

Zentrale Koordination

Die Pflegedienstzentrale wird durch den Client am Verwaltungsarbeitsplatz bei der Planung und Koordination der Mitarbeiter sowie der Kommunikation mit anderen Einrichtungen wie z.B. Krankenhäusern, Ärzten, Mahlzeitenservice, Angehörigen, etc. unterstützt. Mit der offenen Plattform werden die gesamten Patienteninformationen zentral gesammelt und allen Beteiligten ortsunabhängig und unter Berücksichtigung hoher Datensicherheit bereitgestellt.

Der Zugang zu persönlichen oder gesundheitsbezogenen Daten wird dabei je nach Anwender beschränkt. Eine spezielle Sicherheitskomponente für die Autorisierung des Zuganges zu sensitiven Pflege- und Patientendaten wird in jedem Terminal eingesetzt. Um eine optimale Erweiterbarkeit und Wartung des Systems auch nach individuellen Erweiterungen und Anpassungen gewährleisten zu können, basiert VitaBIT auf einer Plugin-Architektur. Die Plugins können über Standard Webservice-Schnittstellen integriert werden. VitaBIT stellt Schnittstellen für die Pflegeplanungssoftware zur Verfügung, so dass der Pflegedienst weiterhin die gewohnte Umgebung verwenden kann.

Kommunikation mit Dritten im Pflegenetzwerk

Der dritte Client bietet die Möglichkeit des Zugriffs auf die gemeinsame Datenbasis durch verschiedene weitere Benutzergruppen, die an der Pflege der Patienten unmittelbar beteiligt sind. Hier sind insbesondere die Ärzte und Krankenhäuser, die die jeweiligen Patienten betreuen, aber auch die Angehörigen der Patienten sowie Notrufzentralen zu nennen.

Abbildung 2-5: VitaBIT: Plattform für sichere Kommunikation und den sicheren Informationsaustausch zwischen allen Beteiligten im Pflegeprozess

Quelle: VitaBIT

Relevanz Elektronische Signatur

Im Anwendungsfall „Pflegeakte verwalten“ ist die Integration des Sicherheitsmechanismus „Digitale Signatur“ mit Zeitstempel vorgesehen. Der Eintrag von Patientendaten in die Pflegeakte (z. B. Vitaldaten, Zuckerwerte) erfolgt dann mittels Authentifizierungs- und Verschlüsselungsverfahren.

Abbildung 2-6: Ablauf “Erfassen von Daten und Signatur”

Erfassen (Beispiel Dokustift)
Zwischenspeichern, Zuordnen der „analogen“ Daten im Dokustift

Zugriff auf die VitaBIT-Plattform (Login)
Passworteingabe und Öffnen des UP-Loaders

Übertragung der erfassten Daten auf das VitaBIT-System
Übertragen der Daten von der VitaBIT-Plattform an den Dokustift-Service

Integration in VitaBIT-Zentrale (Zentrale Datenbank mit Patientendaten)
Rückübertragung an VitaBIT nach erfolgter Umwandlung in Formular-Daten (XML, sichere Übertragung über das VitaBITGateway)

Upload quittieren, wenn erfolgreich
Präsentation der erfassten Dokustift-Daten, Quittieren mit Anwendung Elektronischer Signatur und Zeitstempel

Quelle: VitaBIT

Zusammenfassung: Welche Vorteile besitzt die elektronische Signatur derzeit bei mobilen Geschäftsanwendungen?

- Mobile Endgeräte bieten schon heute hohen Komfort für sichere Signaturanwendungen. Im Prinzip ist der Nutzer mittels dieser Anwendungen jederzeit weltweit handlungsfähig.
- In Zukunft wird die Identifikationsfunktion des neuen Personalausweises (nPA) die Handlungsoptionen auch bei mobilen Geschäftsanwendungen noch ausweiten. Dasselbe gilt z.B. für die Entwicklung von mobilen biometrischen Lösungen wie etwa Fingerprint statt PIN-Eingabe.
- Security Token (wie z.B. die SIM-Card oder auch die im SimoBIT-Projekt VitaBIT verwendete MicroSD-Card) bilden die Voraussetzung für die Integration von Sicherheit in mobile Endgeräte für Signaturanwendungen. Annähernd 80% der heute angebotenen SmartPhones könnten so signierfähig gemacht werden.
- Mittels neu entwickelter Betriebssysteme für mobile Endgeräte werden die technischen Voraussetzungen für Sicherheitszonen geschaffen, die eine gesicherte Eingabe der PIN über die mobile, integrierte Tastatur ermöglichen. Moderne Smart Phones besitzen darüber hinaus die erforderliche Bildschirmgröße, um die zu signierenden Dokumentenseiten bequem lesbar darzustellen.
- Für Transaktionen aller Art wie z.B. Kaufgeschäfte bieten mobile Signaturanwendungen sowohl in technischer als auch rechtlicher Hinsicht zurzeit komfortable und sichere Lösungen für die fortgeschrittene elektronische Signatur.

3 Haftungsfragen

Das Produkthaftungsgesetz (Gesetz über die Haftung für fehlerhafte Produkte – ProdHaftG) vom 15. Dezember 1989 (BGBl. I S. 2198) regelt in Deutschland die Haftung eines Herstellers bei fehlerhaften Produkten. Darunter sind alle beweglichen Sachen, auch wenn sie einen Teil einer anderen beweglichen Sache oder einer unbeweglichen Sache sind sowie Elektrizität zu verstehen.

Produkthaftungsgesetz § 1 Abs. 1, Satz 1

Wird durch den Fehler eines Produktes jemand getötet, sein Körper oder seine Gesundheit verletzt oder eine Sache beschädigt, so ist der Hersteller des Produkts verpflichtet, dem Geschädigten den daraus entstehenden Schaden zu ersetzen.

Für jeden Hersteller ist es wichtig, darüber informiert zu sein, inwieweit er für Fehler seiner Produkte haftbar gemacht werden kann. Im Produkthaftungsgesetz (ProdHaftG) ist geregelt, wann und wer für Folgeschäden an Personen oder Sachen einstehen muss, die ein fehlerhaftes Produkt verursacht hat.

Haften muss z. B. auch ein Hersteller von mobilen Geschäftsanwendungen, wenn auf ihn die folgenden Merkmale zutreffen:[2]

- Hersteller des Endprodukts

Voraussetzung für eine Haftbarkeit des Herstellers des Endprodukts ist, dass es sich um eine gewerbsmäßige Herstellung handelt, die eigenverantwortlich und selbständig betrieben wird.

- Hersteller des Teilprodukts

Der Hersteller eines Teilprodukts kann genauso für den gesamten entstandenen Schaden haftbar gemacht werden, wie der Endprodukthersteller. Seine Haftung setzt dabei voraus, dass das von ihm hergestellte Teilprodukt fehlerhaft war.

- Quasihersteller

Als „Quasihersteller“ werden solche Hersteller bezeichnet, die ein Produkt nicht selbst herstellen, sondern lediglich von anderen Herstellern produzierte Produkte unter Anbringung des eigenen Namens, Warenzeichens oder einer eigenen Marke in die Öffentlichkeit bringen. Häufig kommt dies bei Hausmarken von z. B. Einzelhändlern vor.

- Händler

Generell können auch Händler haftbar gemacht werden. Allerdings sieht das ProdHaftG vor, dass ein Händler haftungsfrei wird, wenn er den Vorlieferanten innerhalb einer einmonatigen Frist nennen kann. Eine lückenlose Dokumentation der Vertriebskette ist somit für Händler ein Muss.

---

2 Vgl. IHK Stuttgart (2008): Produkthaftung nach dem ProdHaftG, Industrie- und Handelskammer Region Stuttgart, http://www.stuttgart.ihk24.de/produktmarken/recht_und_fair_play/recht/Produkthaftung.

Hersteller im Sinne des ProdHaftG sollten entsprechend ihrem Haftungsrisiko für ausreichenden Versicherungsschutz sorgen. Häufig empfiehlt es sich, eine Produkthaftpflichtversicherung ergänzend zur normalen Betriebshaftpflichtversicherung abzuschließen, da die Betriebshaftpflichtversicherung nicht alle Schäden erfasst.

3.1 Produkthaftung bei mobilen Geschäftsanwendungen

Markus Keubke, Rechtsanwalt, Rostock

Über die Hälfte aller Personenschäden in Verbindung mit technischen Geräten entsteht durch Fehlbedienung der Geräte und nur in wenigen Fällen durch tatsächliche Gerätefehler (Laufs/Kern, 4. Aufl., § 54 Rn 4[3]). Der Haftung aus diesen Gerätefehlern kann der Hersteller jedoch zu einem überwiegenden Teil vorbeugen. Im Folgenden soll dargestellt werden, wie diese Haftung aussieht und was von ihr erfasst wird.

Grundsätzlich kann auf zwei Arten gehaftet werden. Zum einen infolge der so genannten Verschuldenshaftung, also der Haftung aufgrund persönlich vorwerfbaren Verhaltens und zum anderen infolge der Gefährdungshaftung. Dabei wird für Schäden gehaftet, die aufgrund der Schaffung einer besonderen Gefahrenquelle entstanden sind. Ein schuldhaftes Verhalten wie bei der Verschuldenshaftung ist nicht erforderlich. Die Haftung erfolgt allein durch eine gesetzliche Regelung. Das Produkthaftungsgesetz (ProHaftG) ist eine solche Regelung.

Bezüglich der Verschuldenshaftung findet sich die wichtigste Regelung in § 823 BGB. Diese Norm beinhaltet in ihrem zweiten Absatz eine Haftung bei Verletzung eines Schutzgesetzes. Schutzgesetze im Sinne dieser Norm sind neben dem ProdHaftG das Medizinproduktegesetz (MPG), das Geräte- und Produktsicherheitsgesetz (GPSG) und die Medizinprodukte-Betreiberverordnung (MPBetreibV). Diese Regelungen geben auch Personen gegenüber dem Hersteller einen Anspruch auf Schadensersatz und Schmerzensgeld, die in keiner vertraglichen Beziehung zum Hersteller stehen, sondern das jeweilige Gerät anwenden, bzw. durch die Anwendung an ihnen einen Schaden erlitten.

Schauen wir uns diese Regelungen im Einzelnen an und beginnen mit dem ProdHaftG:

Dort bestimmt § 1 Abs. 1 Satz 1: *"Wird durch den Fehler eines Produktes jemand getötet, sein Körper oder seine Gesundheit verletzt oder eine Sache beschädigt, so ist der Hersteller des Produkts verpflichtet, dem Geschädigten den daraus entstehenden Schaden zu ersetzen."*

Entsprechend dieses Satzes lassen sich die Voraussetzungen einer Haftung entnehmen. Es bedarf dazu eines Produktfehlers, der für eine Rechtsgutverletzung (Schaden) ursächlich (Kausalität) ist. Verantwortlich für den Produktfehler ist der Hersteller. Umfasst vom Schutz des Gesetzes sind Vertragspartner, Produktbenutzer und Dritte.

3 Adolf Laufs, Bernd-Rüdiger Kern, Handbuch des Arztrechts, 4. Auflage 2010, C. H. Beck, München.

In § 2 des ProdHaftG wird bestimmt, was ein Produkt im Sinn des Gesetzes ist. Danach ist grundsätzlich jede bewegliche Sache ein Produkt. Ein Problem stellen dabei die Abgrenzungen zu Dienstleistungen und intellektuelle Leistungen, wie Software, dar. Zur Lösung des Problems wird auf die Verkörperung der Information zurückgegriffen. Die Software stellt demnach dann ein Produkt dar, wenn diese auf einem Datenträger gespeichert ist und der Warencharakter überwiegt. Wird die Software online übertragen, besteht die Produkteigenschaft solange, wie die Informationen beim Provider gespeichert sind und der Nutzer eine identische Kopie der Software erhält. Erfolgt die Nutzung der Daten ohne Überspielen, handelt es sich um eine Dienstleistung.

§ 3 regelt den Fehlerbegriff. Sowohl im Kauf- als auch im Werkvertragsrecht wird auf die Sollbeschaffenheit, d.h. auf die vereinbarte Beschaffenheit der jeweiligen Sache abgestellt. Im Produkthaftungsrecht wird jedoch ein objektiver Fehlerbegriff zugrunde gelegt, der sich an den Sicherheitserwartungen des Produktes sowie an der von der Allgemeinheit erwarteten Produktsicherheit orientiert. Dabei werden mehrere Fehlertypen unterschieden:

- Fabrikationsfehler: das Produkt genügt den eigenen Anforderungen des Herstellers nicht;
- Konstruktionsfehler: durch ein anderes technisch mögliches Produktdesign hätte die Rechtsgutverletzung vermieden werden können;
- Instruktionsfehler: der Verwender wurde unzureichend über die Art und Weise der Anwendung aufgeklärt oder die Gebrauchsanleitung war fehlerhaft;
- Produktbeobachtungsfehler: es wurden keine ausreichenden Vorkehrungen für Rückmeldungen über Anwendungsprobleme getroffen, explizite Regelungen dazu finden sich im GPSG und der Medizinproduktesicherheitsplanverordnung;
- Haftung für Wirkungslosigkeit: es wurde eine Wirkung versprochen, die mit dem Produkt nicht erreicht werden kann, der Fehler liegt dann in der Wirkungslosigkeit, z.B. Software, die einen Virenschutz verspricht, aber dazu nicht tauglich ist.

Hersteller im Sinn des ProdHaftG ist jeder, in dessen Organisationsbereich eine bewegliche Sache (oder Software) entstanden ist. Hersteller ist auch derjenige, der ein abgrenzbares Teil des Endproduktes fabriziert sowie der, der ein Produkt nur mit seinem Label kennzeichnet. Dem Hersteller gleichgestellt sind Importeure und Lieferanten (§ 4 Abs. 2 und 3).

Weiterhin enthält das Gesetz verschiedene Haftungsbegrenzungen und -ausschlüsse (§ 1 Abs. 2 und 3, §§ 6, 10, 11) sowie Regelungen zur Verjährung. Letztere endet drei Jahre nach Kenntnis des Schadens, dem Fehler und der Person des Ersatzpflichtigen spätestens aber nach zehn Jahren seit dem Inverkehrbringen des Produktes.

Abschließend eine kurze Darstellung, wie der Hersteller nach den oben bereits genannten Schutzgesetzen haften kann. § 4 MPG verbietet das in Inverkehrbringen von Medi-

zinprodukten, die die dort normierten Voraussetzungen nicht erfüllen. Diese ähneln denen des ProdHaftG, sind aber im Unterschied zum ProdHaftG zum einen auch strafbewehrt und können sogar wettbewerbsrechtliche Folgen haben und zum anderen reicht hier der begründete Verdacht aus, dass das Gerät diese in § 4 MPG benannten Schäden, insbesondere Gesundheitsschäden bei Patienten und Anwendern, verursachen kann.

Die Regelungen der §§ 5 und 6 MPBetreibV füllen den aus § 3 ProdHaftG bekannten Instruktionsfehler mit Leben aus und bestimmten im Detail, welche Pflichten dem Hersteller diesbezüglich obliegen.

Im GSPG finden sich schließlich für alle Produkte Bestimmungen zur Vermeidung von Instruktions- und Produktbeobachtungsfehlern. Das GSPG ist jedoch im Verhältnis zu anderen Gesetzen zur Produkthaftung subsidiär, d.h. erst wenn der Schutz durch eine andere Regelung nicht erreicht werden kann, können die Bestimmungen des GSPG angewendet werden.

Zusammenfassende Hinweise

1. *Gibt es einen Unterschied in Bezug auf Haftungsfragen bei mobilen Anwendungen im Gegensatz zu herkömmlichen Internet-Anwendungen?*
   In den Rechtsfolgen gibt es bei mobilen Anwendungen keinen Unterschied zu "stationären" Internet-Anwendungen. Wenn der Anwendungszweck aber maßgeblich von der Möglichkeit des mobilen Einsatzes bestimmt wird, so sollte, um Haftungsfragen zu vermeiden, vorher sichergestellt werden, dass durch die technischen Besonderheiten der mobilen Anwendung keine Störungen bei der Anwendung auftreten.

2. *Wofür muss ich als mobiler IT-Dienstleister haften, wenn ich verschiedene Informationen von verschiedenen (öffentlichen) Stellen neu zusammenstelle (verschneide), um sie dann Dritten mobil zur Verfügung zu stellen? (Kunde ist z.B. dann eine Stadtverwaltung, eine Feuerwehr).*
   Wenn der Dienstleister fremde Informationen nicht nur Dritten ungeprüft zur Verfügung stellt, sondern derart bearbeitet, dass verschiedenen Informationen verschnitten werden und gegebenenfalls anwendungsbezogen aufbereitet werden, so haftet der Dienstleister für die Verwendungsfähigkeit der Informationen, d.h. ob diese korrekt und aktuell sind. Von dieser Haftung kann sich jedoch individualvertraglich gelöst werden.

3. *Was ist im Rahmen der „üblichen“ Betriebs-, Produkt- oder Umwelt-Haftpflicht-Versicherungsprogramme abgedeckt, was nicht?*
   Diese Frage kann nicht pauschal beantwortet werden, da der Versicherungsumfang von der Art des Haftpflichtvertrages abhängt.

4. Manche SimoBIT-Projekte setzen in ihren mobilen Lösungen auf bestehende Datenquellen. Gibt es eine Aussage zur Haftung bei fehlerhaften oder veralteten Daten und sich daraus ergebenden Fehlentscheidungen?

Es empfiehlt sich, auf die bestehenden Datenquellen und deren möglichen unzureichenden (also veralteten oder unvollständigen) Zustand deutlich erkennbar hinzuweisen, bzw. den Kunden vor Vertragsschluss darüber zu informieren. Wenn eine solche Information unterbleibt, haftet der Anbieter für die fehlerhaften Datenquellen und möglicherweise auch für die sich daraus ergebenden Fehlentscheidungen.

3.2 Haftungsfragen in der Gesundheitswirtschaft: Das Beispiel des SimoBIT-Förderprojekts Med-on-@ix

In Aachen wird ein System zur präklinischen Notfallversorgung erprobt, bei dem das Rettungsdienstpersonal vor Ort durch eine Telenotarztzentrale unterstützt wird.[4]

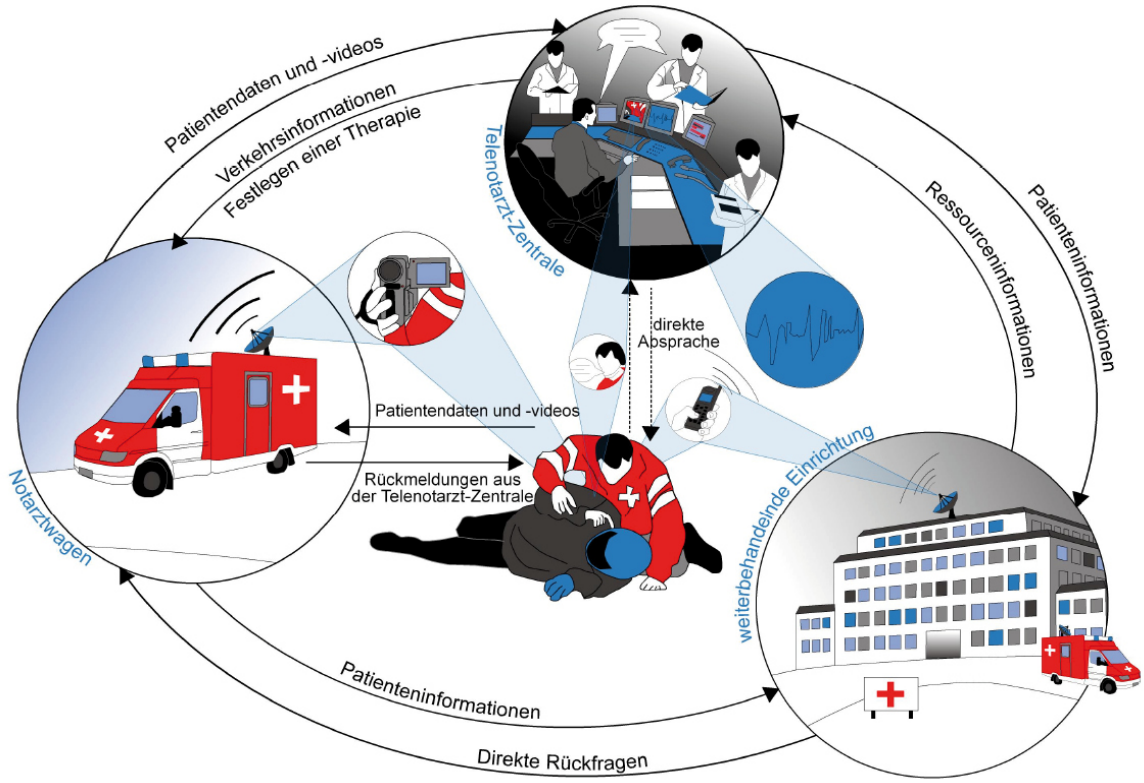
Einerseits steigt in unserer alternden Gesellschaft die Anzahl von Notarzteinsätzen kontinuierlich an. Andererseits nimmt der Mangel an Notärzten so weit zu, dass in manchen Landkreisen die flächendeckende Versorgung bereits gefährdet ist. In Anbetracht der Funktionalitäten, die zum Beispiel ein privat genutztes Smartphone bietet, muss zudem die derzeit überwiegend im deutschen Rettungsdienst verwendete Informations- und Telekommunikationsstruktur (Analogfunk) als rückständig beziehungsweise nicht mehr zeitgemäß bezeichnet werden.

Vor diesem Hintergrund wurde in Aachen ein innovatives telemedizinisches Unterstützungssystem für die präklinische Notfallversorgung entwickelt. Dieses ermöglicht dem ärztlichen oder nichtärztlichen Rettungsdienstpersonal vor Ort jederzeit den Kontakt zu einem erfahrenen Notfallmediziner per Telekonsultation. Zwei Rechtsgutachten, die zu Projektbeginn in Auftrag gegeben wurden, bestätigen, dass der Einsatz von Telemedizin im Rettungsdienst grundsätzlich rechtmäßig ist.

Kernelement des Projekts „Med-on-@ix“ bildet die Telenotarztzentrale, ein mit erfahrenen Notfallmedizinern besetztes Kompetenzzentrum. Der Telenotarzt erhält durch speziell konzipierte mobil- und medizintechnische Lösungen sämtliche Vitaldaten in Echtzeit, hochauflösende Bilder, etwa von Arztbriefen und Medikamentenlisten sowie Videostreams vom Einsatzort beziehungsweise aus dem Rettungswagen. Außerdem stehen ihm eine Software zur leitliniengerechten Patientenbehandlung sowie der Online-Zugriff zu anderen sinnvollen Unterstützungsmöglichkeiten (wie Rote Liste, Giftnotrufzentralen) zur Verfügung. Hierdurch kann der Telenotarzt die Rettungskräfte am Einsatzort optimal unterstützen.

4 Vgl. dazu Naß, E., Renno, C., Rörtgen, D. und Skorning, M. (2010). Forschungsprojekt Med-on@ix: Telemedizin im Rettungswesen. Deutsches Ärzteblatt 107, no. 14. Herrn Dr. Max Skorning sei an dieser Stelle für seine unterstützenden Hinweise sowie das Zurverfügungstellen der Rechtsgutachten gedankt.

Abbildung 3-1: SimoBIT-Förderprojekt Med-on-@ix: Mobile Informationslösungen im deutschen Rettungsdienst



Quelle: Med-on-@ix

Durch Implementierung des Systems lassen sich die in der Praxis vielfach beklagten Schnittstellenprobleme zwischen präklinischer und stationärer Versorgung minimieren. So werden dem später angefahrenen Krankenhaus bereits vorab umfassende und systematisierte patientenbezogene Informationen durch den Telenotarzt elektronisch übermittelt. Hierdurch lässt sich ein durchgängiger Informationsfluss entlang der Rettungskette zum Wohle des Notfallpatienten gewährleisten. Gleichzeitig unterstützen das elektronische Dokumentationssystem beziehungsweise die darüber generierte Datenmenge und -qualität eine verbesserte Einsatzevaluierung und ein umfassenderes Qualitätsmanagement.

Vor allem in Gebieten mit geringer Notarztdichte vermag Med-on-@ix zur Aufrechterhaltung einer funktionierenden flächendeckenden Versorgung beizutragen. Trotz der vielfältigen Potenziale hinsichtlich der Organisation einer effizienteren und effektiveren präklinischen Versorgungsstruktur bleibt eine schnelle Umsetzung in den Regelrettungsdienst aufgrund gesundheitssystemimmanenter Hürden fraglich. Wahrscheinlicher ist eine schrittweise regionale Einführung des telemedizinischen Unterstützungssystems.

Im Rahmen des Projekts Med-on-@ix wurden zwei Rechtsgutachten eingeholt, in denen umfangreich alle wesentlichen juristischen Fragestellungen und Problematiken beantwortet wurden. Die Gutachter sind Prof. Dr. iur. Christian Katzenmeier (Institut für Medizinrecht, Universität zu Köln) und Prof. Dr. Karsten Fehn (Fachanwalt für Medizinrecht, Fachhochschule Köln).

Die Begutachtung des Vorhabens Med-on-@ix erfolgte unter anderem zu folgenden Themen:

- Datenschutz
- Grundsätze der persönlichen Leistungserbringung
- Fernbehandlungsverbot
- Haftungsfragen / strafrechtliche Verantwortlichkeiten
- Telemedizinische Delegation ärztlicher Maßnahmen

Einige Auszüge zu wesentlichen Erkenntnissen, die durch die Rechtsgutachten in Bezug auf Haftungsfragen gewonnen wurden:

- In der Evaluationsphase herrscht für das Personal vor Ort besondere Rechtssicherheit: Es ist immer ein Notarzt anwesend, wenn das System eingesetzt wird und dieser ist immer der medizinisch Verantwortliche.
- Mehr Rechtssicherheit für Rettungsassistenten in sog. „Notkompetenzsituationen“, da primär ärztliche Maßnahmen auch telemedizinisch delegiert werden können.
- Ist ein Notarzt vor Ort anwesend, dann hat dieser in der Regel nach wie vor die Letztentscheidungs-Kompetenz.
- Notarzt vor Ort und Telenotarzt können sich strafbar machen, wenn sie offensichtliche Fehler des jeweils anderen Arztes nicht erkennen.
- Im Schadenfall haftet der Telenotarzt gesamtschuldnerisch neben dem Notarzt vor Ort.
- Die strafrechtliche Verantwortung des Telenotarztes ist verschärft, wenn lediglich nichtärztliches Personal vor Ort ist.
- Das nichtärztliche Personal vor Ort kann sich strafbar machen, wenn eine richtige Therapieempfehlung des Telenotarztes schuldhaft missachtet und eine andere Maßnahme ergriffen wird.

Aus dem Rechtsgutachten im Rahmen des Projekts Med-on-@ix: „Ergänzendes Rechtsgutachten zu strafrechtlichen Fragen und Rechtsfragen der sog. Notkompetenz im Zusammenhang mit der Etablierung eines telemedizinischen Notarzt-Systems im öffentlichen Rettungsdienst“ Prof. Dr. iur. Karsten Fehn, Köln:

„Als Gesamtergebnis ist mithin festzustellen:

Die Etablierung eines Telenotarzt-Systems, wie es das Projekt „Med-on-@ix“ zum Ziel hat, ist aus strafrechtlicher Sicht nicht zu beanstanden. Es ist jedoch zur Vermeidung einer Strafbarkeit wegen Geheimnisverrats gemäß § 203 Abs. 1 Nr. 1 bzw. Abs. 2 Nr. 1 StGB sicherzustellen, dass vor der Beteiligung des Telenotarztes an der Behandlung des Notfallpatienten dessen diesbezügliche Einwilligung herbeigeführt oder — soweit dies nicht möglich ist — dessen mutmaßliche Einwilligung festgestellt wird.

Bei einem Fehlverhalten, insbesondere bei fahrlässigem Handeln, können für alle Beteiligten Strafbarkeitsrisiken auftreten. So kann sich der Telenotarzt zunächst wegen fahrlässiger Tötung gemäß § 222 StGB bzw. wegen fahrlässiger Körperverletzung gemäß § 229 StGB strafbar machen, wenn er an einen vor Ort anwesenden Notarzt oder Rettungsassistenten eine fehlerhafte Therapieempfehlung bzw. -anweisung gibt. Ebenso kann es zur Strafbarkeit des Telenotarztes führen, wenn er eine fehlerhafte Behandlung des Notfallpatienten durch einen vor Ort anwesenden Notarzt nicht erkennt und nicht korrigierend eingreift. Dies kann indes nur bei evidenten Fehlern des vor Ort agierenden Notarztes gelten. Eine Überwachungspflicht trifft den Telenotarzt gegenüber dem vor Ort anwesenden Notarzt wegen des Vertrauensgrundsatzes nicht.

„Aus den vorstehenden Ausführungen lassen sich folgende Empfehlungen zur Minimierung eines strafrechtlichen Risikos ableiten:

Zunächst ist das Funktionieren der Technik durch umfangreiche Erprobung sicherzustellen, um so technisch bedingte Fehler und Schäden an den Rechtsgütern „Leben“ und „Gesundheit“ des Patienten auszuschließen.

Weiterhin sollte während der Testphase des Projektes wie es auch beabsichtigt ist — stets ein Notarzt zur Einsatzstelle mit alarmiert werden, der bei technischen, taktischen oder fachlichen Problemen umgehend eingreifen kann. Hierdurch wird ein dahingehender Fahrlässigkeitsvorwurf vermieden, dass ein in der Erprobung befindliches System zu Lasten des Patienten ohne Absicherung getestet worden sei. Bei Versuchen gelten — wie im technisch-apparativen Bereich — erhöhte Sorgfaltsanforderungen. Auf die organisatorischen Voraussetzungen wurde bereits hingewiesen.

Vor Beginn eines Praxistests sollte das gesamte an der Erprobung beteiligte Rettungsdienstpersonal (Telenotärzte, Notärzte, Rettungsassistenten und Leitstellenmitarbeiter) umfassend technisch, taktisch und rechtlich in der Handhabung des Systems geschult werden. Inhalt dieser Schulungen sollten für die beteiligten Rettungsassistenten v.a. erweiterte Versorgungsmaßnahmen (Notkompetenzmaßnahmen) sein, darüber hinaus Informationen darüber, was der Telenotarzt leisten kann und was nicht. Ferner sollte das

Rettungsdienstpersonal insbesondere über die Bedeutung der Einwilligung des Patienten in die Einschaltung des Telenotarztes geschult werden. Außerdem muss die sichere Handhabung der Technik durch Schulungsmaßnahmen gewährleistet sein. Beim späteren „Echtbetrieb“ sollten solche Schulungen regelmäßig durchgeführt und wiederholt werden.

Darüber hinaus ist anzuraten, vor Beginn des Praxistests praktische Übungen an dem System durchzuführen. Auch solche sollten beim späteren Praxisbetrieb Bestandteil der regelmäßigen Fortbildung sein.

Während der Praxistests sollte außerdem ein effektives Qualitätsmanagementsystem etabliert und möglichst eine unabhängige (externe) Studie über die Sicherheit und den Patientennutzen in Auftrag gegeben werden.

Es sollte ferner für die Rettungsdienstmitarbeiter vor Ort (Rettungsassistenten und Notärzte) ein verbindlicher Indikationskatalog erstellt werden, der vorgibt, wann der Telenotarzt einzuschalten ist. Darüber hinaus sollte es für Rettungsassistenten, Telenotärzte und Leitstelle einen Indikationskatalog geben (sofern nicht bereits vorhanden), aus dem sich ergibt, in welchen Fällen ein Notarzt zur Einsatzstelle zu alarmieren ist. Des Weiteren sollte das Verhältnis des Telenotarztes zu den Rettungsdienstmitarbeitern an der Einsatzstelle und zur Leitstelle durch Dienstanweisung klar geregelt werden. In der Dienstanweisung sollte ebenfalls geregelt sein, dass es über die vorgenannten Indikationskataloge den Rettungsassistenten bei eigenständiger Einsatzabwicklung vor Ort freisteht, in weiteren Fällen den Telenotarzt einzuschalten und/oder einen Notarzt zur Einsatzstelle nachzualarmieren, wenn sie dies für erforderlich halten. Auch ein Notarzt vor Ort muss über einen Indikationskatalog hinausgehend frei sein, den Telenotarzt zu kontaktieren. Eine solche Dienstanweisung muss konform gehen mit evtl. mit dem Träger eines Kompetenzzentrums zu schließenden Verträgen. Aus diesen müssen sich die Rechtsverhältnisse zu allen Beteiligten sowie die Befugnisse und Verantwortungsbereiche klar entnehmen lassen.

Zudem sollte eine Standardaufklärung und ein Standarddokumentationsmodul für die Information und Einwilligung des Patienten in die Einschaltung des Telenotarztes entwickelt werden.

Darüber hinaus scheint es überlegenswert, zumindest während der Testphase vorsorglich für die Telenotärzte eine Strafrechtsschutzversicherung abzuschließen, da diese sich in einem neuen rechtlichen Umfeld bewegen. Für die übrigen Rettungsdienstmitarbeiter scheint dies nicht unbedingt erforderlich, da diese — wie dieses Gutachten gezeigt hat — letztlich kaum mehr strafrechtliche Risiken tragen als bei den bisherigen Einsätze ohne die Existenz eines Telenotarztes.

Schließlich sollte die Etablierung des Telenotarzt-Systems durch Öffentlichkeitsarbeit begleitet werden, um potenzielle Patienten im Vorfeld zu informieren und dadurch Vorbehalte und schließlich die Beschwerde- und Anzeigebereitschaft zu minimieren.“

3.3 Erfahrungen aus dem SimoBIT-Förderprojekt MobisPro

MobisPro - Mobiles Informationssystem zur Prozessoptimierung in Feuerwehren und öffentlichen Verwaltungen[5]

Ausgangslage

Rücken heute Feuerwehrleute im Schadensfall aus, sind sie hinsichtlich wichtiger Informationen über den Einsatzort, wie z. B. die Lage der Gasleitungen oder der Hydranten, auf einen laminierten Einseiter angewiesen. Das Problem ist, dass papiergebundene Dokumentationen beispielsweise von Gewerbeimmobilien trotz einer reichhaltigen Bebilderung nicht mobil verfügbar sind. Bei Industriegebäuden kommt noch erschwerend hinzu, dass häufig Nutzungsänderungen vorgenommen werden und die Unterlagen nicht mehr auf dem aktuellen Stand sind. Untersucht und geprüft werden Gebäude nur alle fünf Jahre. Diese Veränderungen können verheerend sein - man denke sich nur den Fall, dass aus einem Stahllager ein Papierlager geworden ist. Die im Durchschnitt zu verzeichnenden fünf bis sieben Minuten Anfahrt verstreichen ungenutzt, ohne dass die Fachleute eine Auswertung von Basisdaten vornehmen könnten, die die Brandbekämpfung direkt vor Ort beschleunigen würde. Dabei ist zu bedenken, dass sich alle zweieinhalb Minuten ohne Eingreifen der Feuerwehr der Schaden am betreffenden Objekt verdoppelt.

Projektziel

Mit einer neuen Lösung, die auf die mannigfachen Vorteile mobiler Geräte zurückgreift, sollen vorbeugender Brandschutz und die Brandbekämpfung in Zukunft wesentlich schneller und effizienter gestaltet werden. Den Feuerwehrleuten sollen bereits auf dem Weg zum Einsatzort potenzielle Gefahrenquellen, Hydrantenstandorte, Leitungspläne, Luftbilder oder Pläne über die kürzeste Anfahrt zur Verfügung stehen, um wertvolle Minuten zu gewinnen, die Menschenleben retten und den finanziellen Schaden geringer halten können.

Innovation

Integraler Bestandteil zur Erreichung dieses Zieles ist das System Mobis Pro, das die Mitarbeiter der rund 25.000 Feuerwehren in Deutschland bei der Datenaufnahme vor Ort unterstützten kann, und so den mobilen Informationsaustausch mit der jeweiligen Dienststelle ermöglicht. Grundlage ist ein Behördenübergreifendes Informationssystem, in dem sehr unterschiedliche Daten aus verschiedenen Datenbanken der Gebäudeverwaltung, des Planungsamtes, des Bauordnungsamtes, der Vermessungsämter, der Energie- und Versorgungsunternehmen, der Verkehrsbetriebe und den unterschiedlichen Fachabteilungen der Feuerwehren zusammengeführt werden und an einer zentra-

5 Frau Martina Kaster, Vomatec, SimoBIT-Förderprojekt MobisPro vielen Dank für die Unterstützung bei der Erstellung dieses Kapitels.

len Stelle zum Abruf bereit stehen. Aufgrund der ortsunabhängigen Verfügbarkeit und der hohen Qualität der Daten können künftig Entscheidungsprozesse der Feuerwehrführungskräfte unterstützt werden. Darüber hinaus bietet sich ein weites Anwendungsfeld für Mobis Pro im Bereich des Vorbeugenden Brandschutzes. Insbesondere bei der Durchführung der Brandschau können mobil zur Verfügung gestellte Daten die Bearbeitungsqualität und auch die Schnelligkeit steigern. Die Verwendung mobiler Datenanwendungen bietet darüber hinaus auch die Möglichkeit, Änderungen an Gebäudestrukturen oder Nutzungen schnell zu erfassen und allen anderen Beteiligten (vom Bauordungsamt bis zum Feuerwehrmann im Brandfall) schnell und sicher bereitzustellen.

Rechts- und Haftungsfragen

Besondere Berücksichtigung erfordern im Projekt MobisPro rechtliche Aspekte. Dabei geht es vor allem um datenschutzrechtliche Fragen. Zum einen muss der vertrauliche Umgang mit Personendaten gewährleistet sein, zum anderen ist aber auch die eindeutige Festlegung der Verantwortlichkeiten beim Schreibzugriff unabdingbar.

Es geht um rechtliche Aspekte wie

- Datenschutz (Umgang mit Personendaten),
- Datensicherheit (Rechte bei Schreibzugriff),
- Haftung (Datenaktualität).

Technisch wird diesen Anforderungen entsprochen durch:

- Vereinheitlichung und Standardisierung des Zugriffs auf heterogene Daten durch ihre semantische Verknüpfung,
- Realisierung einer aktiven, situations- und rollenangepassten Informationsverteilung,
- Gewährleistung von Ausfallsicherheit, Vertraulichkeit, Authentizität und Integrität der Datenkommunikation.

3.4 Erfahrungen aus dem SimoBIT-Förderprojekt simoKIM

simoKIM: Datenkonsolidierung und mobile Anbindung für das moderne kommunale Infrastruktur-Management[6]

Ausgangslage

Betrieb und Unterhaltung der Infrastruktur gehören sowohl in der öffentlichen Wahrnehmung durch den Bürger (Baustellen), als auch in der Planung und Durchführung durch den Hoheitsträger zu den Dauerbrenner-Themen. Sie gestalten sich deshalb so schwierig, weil viele unterschiedliche Organisationen mit spezifischen Aufgabengebieten wie beispielsweise Tiefbauunternehmen, Stadtwerke, Telekommunikationsbetriebe, die Polizei oder Stadtplanungsämter in den Prozess involviert sind. Es liegt in der Natur der Sache, dass jeder Beteiligte auf völlig unterschiedliche Datenbanken mit abweichenden Strukturen zugreift. Nehmen wir eine einfache Straße: Diese ist durchschnittlich in sieben Datenbanken verzeichnet! Dazu zählen die Datenbanken für Liegenschaften, Geoinformationen, spezielle Straßendatenbanken, solche für Kanäle, für die Stadtmöblierung und Fahrbahnmarkierung sowie für die Beschilderung. Eine heterogenere Systemlandschaft ist kaum vorstellbar und erschwert die tägliche Arbeit an und auf der Straße enorm, da auch kaum Verknüpfungen existieren.

Projektziel

Die Aktivitäten im Projekt simoKIM sind darauf ausgerichtet, die Effektivität und Effizienz beim Management kommunaler Straßeninfrastrukturen zu verbessern und dabei auch die Kosten zu minimieren, die in erster Linie den Steuerzahler belasten. Es ist zu wünschen, dass beispielsweise ein Straßenbegeher bei seinen Touren die Arbeit für andere Bedarfsträger gleich mit übernehmen kann.

Innovation

Im Projekt simoKIM wird ein integratives Kommunales Infrastrukturmanagement (KIM) konzipiert und beispielhaft realisiert. Hierbei kommt es zu einer einheitlichen Vernetzung von Daten aller Beteiligten, die kontextabhängig und mobil bereitgestellt werden. SimoKIM stellt Dienste und Funktionen für eine gesicherte, zentrale Steuerung und den mobilen Zugriff auf Daten bereit. Erstmalig wird dem Anwender eine einheitliche Informationslogistik im kommunalen Infrastrukturmanagement bereitgestellt.

Dazu entwickelt das Konsortium ein Systemmodell, auf dessen Grundlage Produkte für das kommunale Infrastrukturmanagement angeboten werden können. Kernelement des simoKIM-Systemmodells stellt eine Workflow-Laufzeitumgebung dar, mit dessen Hilfe es möglich wird, die bestehenden KIM Prozesse zu modellieren und innerhalb einer Laufzeitumgebung zur Ausführung zu bringen. Durch die aktuelle und gesicherte Bereitstellung aller relevanten Informationen im laufenden Workflow ist es möglich, die in

---

6 Herrn Rolf Mosemann, regioIT Aachen, SimoBIT-Förderprojekt simoKIM vielen Dank für die Unterstützung bei der Erstellung dieses Kapitels.

den verschiedenen Organisationen vorhandenen Datensätze systematisch zu vernetzen und kontextabhängig für den mobilen Zugriff aufzubereiten. Eine erste Evaluierung des Systemmodells wird durch das Konsortium im Rahmen der Entwicklung eines Demonstrators durchgeführt.

Auf diese Weise wird das reibungslose Zusammenspiel aller Akteure wie Ämter, Kommunalbetriebe oder Energieversorger auf der einen sowie den Einsatzteams direkt vor Ort auf der anderen Seite sichergestellt. Die Abschaffung von heute noch gängigen Medienbrüchen sowie der Abgleich und Austausch wirklich relevanter Daten in Echtzeit führt zu einer Harmonisierung und Homogenisierung einzelner Arbeitsabläufe, die somit wesentlich schneller durchgeführt werden können. Um diese Verschlankung der Geschäftsprozesse realisieren zu können, sollen nicht nur innovative Mobil- und Sicherheitstechnologien eingesetzt, sondern vor allem eine zukunftsweisende und übertragbare Systemarchitektur entwickelt und umgesetzt werden. Im Rahmen von simoKIM ist der Begriff Mobiltechnologien weit gefasst: Hierzu gehören alle IT-Technologien, die mobile Anwender unterstützen und mit relevanten Informationen versehen können. Kommunen nutzen in der Zukunft einen innovativen Dienst, ohne in Hard- und Software, Lizenzen oder zusätzliches Personal investieren zu müssen. Mit simoKIM werden primär die Prozesse in der öffentlichen Verwaltung optimiert, es werden aber auch neue Dienstleistungen beziehungsweise Front-Office-Angebote für die Wirtschaft und die Bürger ermöglicht, da erstmals Daten aus unterschiedlichen Quellen integrativ mit standardisierten Vorgehensweisen zusammengeführt werden.

Rechts- und Haftungsfragen

Ziel ist, allen Beteiligten am richtigen Ort, in der richtigen Situation bzw. dem richtigen Kontext entsprechend der jeweiligen Rolle, in der sich die handelnde Person befindet, alle relevanten Daten und Informationen mobil und sicher zur Verfügung zu stellen.

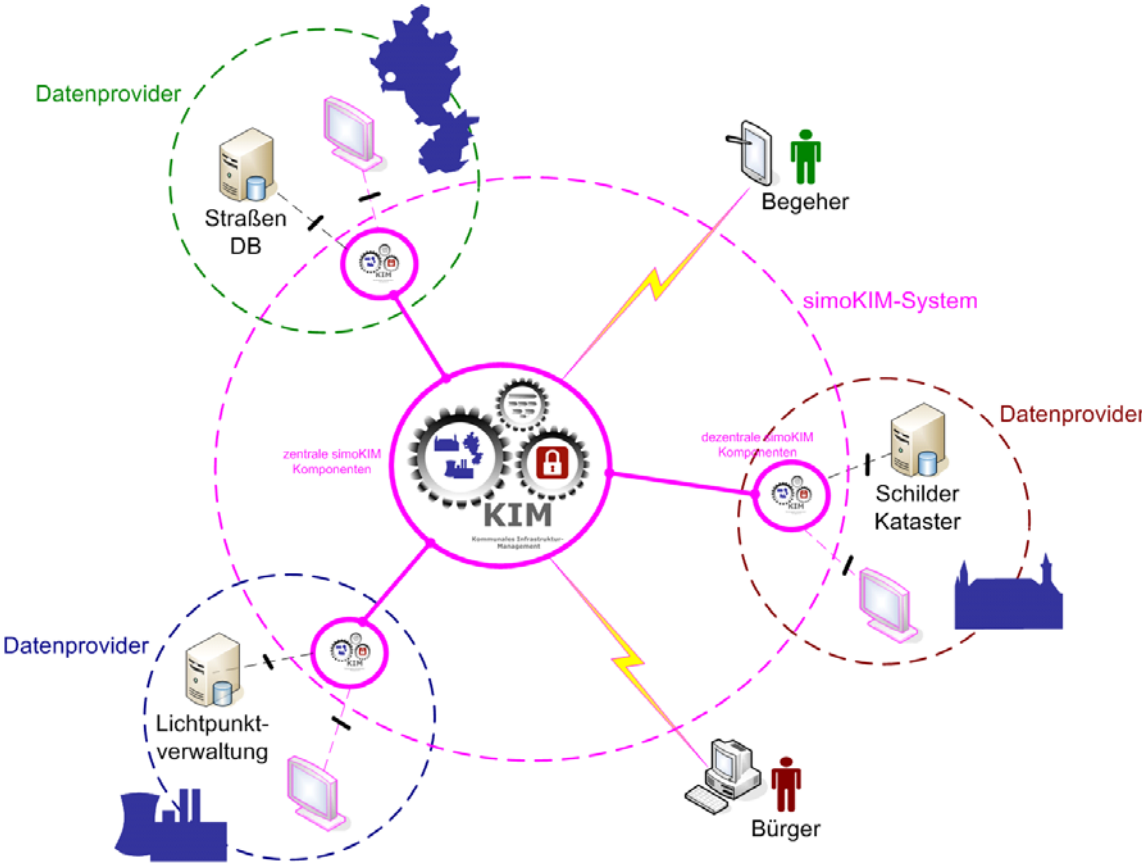
Die in diesem Zusammenhang relevanten rechtlichen Problemstellungen umfassen beispielsweise:

- Daten- und Informationsprovider wollen sichergehen, dass innerhalb der Verarbeitung im simoKIM ihre Daten Unberechtigten nicht offen gelegt werden.
- Anwender, die Infrastrukturdaten mittels simoKIM nutzen, wollen sichergehen, dass diese „echt“ und „aktuell“ sind und ihre Herkunft nachvollziehbar ist.
- Der simoKIM Betreiber muss *allen* Sicherheitsrichtlinien gerecht werden.

Dies bedeutet im Einzelnen, dass Datenschutz- und Sicherheitsrichtlinien strikt einzuhalten sind und das Haftungsregelungen geklärt sein müssen während gleichzeitig das Ziel verwirklicht wird, die Daten allen Beteiligten zugänglich zu machen, einen einheitlichen Zugriff über eine Schnittstelle zu realisieren, den mobilen Zugriff auf Daten zu gewährleisten sowie verschiedene Datensätze aus verschiedenen Quellen miteinander zu verschneiden.

Die im SimoBIT-Förderprojekt simoKIM realisierte Lösung sieht dazu vor, dass die Daten bei den Partnern (Kommune, TK-Diensleister, Energieunternehmen etc.) verbleiben und dieser für die Datenvalidität haftet. Der Betreiber von simoKIM übernimmt die Rolle eines Intermediärs.

Abbildung 3-2: Datenhaltung im SimoBIT-Förderprojekt simoKIM



Quelle: simoKIM

Sicherheitstechnische Umsetzung

Beim Zugriff und der Verarbeitung der Daten muss zu jedem Zeitpunkt die Absicherung der Daten gegenüber Missbrauch erfolgen, da beispielsweise ein Telekommunikationsunternehmen kein Interesse daran hat, dass der Wettbewerb erfährt, welche Leitungen in welcher Bandbreite an welchem Ort liegen. Hierzu ist es notwendig, dass schon innerhalb der Workflow-Modellierung Sicherheitsfunktionalitäten wie z. B. Signaturerstellung und Verschlüsselung bereitgestellt werden. Dies hat den Vorteil, dass innerhalb der Prozesse kontrolliert und auditiert werden kann, inwieweit eine Absicherung wirkungsvoll erfolgt ist und nicht die Infrastruktur in aufwendiger Art und Weise abgesichert werden muss.

4 Datenschutz

Datenschutz ist auch im Bereich von Mobile Business-Anwendungen ein hochaktuelles, kontrovers diskutiertes Thema. Die Erfassung und Verarbeitung persönlicher Daten durch Mobile Business-Dienstleister für private Nutzer oder geschäftliche Anwender oder auch der Umgang mit personenbezogenen (geographischen) Informationen über Arbeitnehmer, die im Rahmen ihrer Beschäftigung mobile Systeme nutzen, bedeuten neue Herausforderungen für den Datenschutz. Nicht zuletzt werfen Trends wie SaaS – Software as a Service oder Cloud Computing auch Fragen zur Gewährleistung der Datensicherheit und des damit verbundenen Schutzes persönlicher Daten in komplexen technischen Systemen auf.

Das geltende Datenschutzrecht wird zurzeit in vielen Gremien behandelt und zahlreiche Positionspapiere und Internet-Diskussionsforen befassen sich mit der Suche nach den Antworten auf die drängenden Fragen, die immer neue (mobile) Web-Anwendungen aufwerfen. Auftragsdatenverarbeitung, Kundendatenschutz und Arbeitnehmerdatenschutz sind zufriedenstellend für alle Seiten zu regeln, damit mobile Anwendungen erfolgreich sein können.

4.1 Anforderungen des Bundesdatenschutzgesetzes in Bezug auf mobile Geschäftsanwendungen – BDSG-Novelle 2009

Sirin Torun, Juristin und Senior Consultant Certs and Audits, SerNet GmbH

4.1.1 Strengere Anforderungen an die Auftragsdatenverarbeitung

Als Reaktion auf die zahlreichen Datenskandale sind im September 2009 umfangreiche Neuerungen im Bundesdatenschutzgesetz (BDSG) in Kraft getreten. So wurde u. a. die Stellung des betrieblichen Datenschutzbeauftragten gestärkt, der Umgang mit personenbezogenen Daten zu Werbezwecken reformiert, eine Generalklausel zum Arbeitnehmerdatenschutz formuliert, eine Reihe neuer Ordnungswidrigkeitstatbestände eingeführt sowie gleichzeitig der Bußgeldrahmen erhöht.

Auch die Regelungen zur Auftragsdatenverarbeitung nach § 11 BDSG sind durch die BDSG-Novelle konkretisiert worden.

4.1.2 Auftragsdatenverarbeitung - Definition und Abgrenzung

Die Auftragsdatenverarbeitung bezeichnet die Erhebung, Verarbeitung oder Nutzung personenbezogener Daten eines externen Dienstleisters im Auftrag, ohne dass ein Erlaubnistatbestand für eine Datenübermittlung gegeben sein muss. Im praktischen Alltag wird die Auftragsdatenverarbeitung oftmals auch als „Outsourcing“ bezeichnet.

Im Falle einer Auftragsdatenverarbeitung besteht ein Abhängigkeitsverhältnis, in welchem der Auftragnehmer auf Weisung des Auftraggebers die Datenverarbeitung vornimmt. Bei Ausführung des Auftrages hat der Auftragnehmer keinerlei Entscheidungsbefugnis. Die inhaltliche und datenschutzrechtliche Verantwortung für die Aufgabenerfüllung verbleibt beim Auftraggeber.

Die Auftragsdatenverarbeitung privilegiert den Auftraggeber, der die Daten im Rahmen der gesetzlichen Befugnisse auch ohne Einwilligung des Betroffenen weitergeben darf.

Wird hingegen der Geschäftsprozess durch einen Auftragnehmer in voller Eigenverantwortung und ohne Einflussnahme des Auftraggebers ausgeführt, handelt es sich um eine sog. Funktionsübertragung. Der Auftragnehmer ist in diesem Fall als Dritter zu betrachten und ist damit nicht Teil der verantwortlichen Stelle, so dass der Privilegierungseffekt nicht eintritt. Die datenschutzrechtliche Zulässigkeit der Funktionsübertragung ist nach §§ 28 und 4 BDSG zu beurteilen.

4.1.3 Was jetzt beachtet werden muss

Das Gesetz stellt nun eindeutig in § 11 Abs.1 S.1 BDSG klar, dass der Auftraggeber seine externen Dienstleister sorgfältig im Hinblick auf die von ihm getroffenen technischen und organisatorischen Maßnahmen zur Datensicherheit auszusuchen hat. Für die Beurteilung ist es notwendig, die vorhandene technische Ausstattung zu überprüfen. Dies bedeutet konkret die Kontrolle von Zutritt, Zugang, Zugriff, Weitergabe, Eingabe, Auftrag und Verfügbarkeit sowie die Einhaltung des Trennungsgebots.

Darüber hinaus ist mit der Novellierung für die Auftragsdatenverarbeitungsverträge nun ausdrücklich die Schriftform gesetzlich vorgeschrieben. Zudem enthält die neue Fassung des § 11 Abs.2 S.1 in einem 10-Punkte Katalog detaillierte Vorgaben, die als Mindestanforderung in einer Vereinbarung zur Auftragsdatenverarbeitung zwingend festgelegt sein müssen. So werden nun explizite vertragliche Regelungen zu Berichtigung, Sperrung und Löschung von Daten, Mitteilungspflichten des Auftragnehmers im Sinne des neuen § 42a BDSG, Kontrollrechten des Auftraggebers, Klauseln über die Einschaltung von Subunternehmern etc. gefordert.

4.1.4 Kontroll- und Dokumentationspflichten

Der Auftraggeber war bereits vor der Gesetzesänderung verpflichtet, die technischen und organisatorischen Maßnahmen beim Auftragnehmer zu kontrollieren. Seit dem 1. September 2009 sind die Unternehmen durch die zeitlichen Vorgaben und Dokumentationsverpflichtungen nun stärker in der Pflicht, ihre Auftragsdatenverarbeiter zu auditieren. Nach § 11 Abs. 2 S.4 muss die Erstkontrolle künftig vor Beginn der Datenverarbeitung erfolgen. Die Folgekontrollen sind regelmäßig in festgelegten Prüfintervallen oder anlassbezogen zu wiederholen. Das Ergebnis ist als Nachweis zu dokumentieren.

Der Gesetzgeber hat keine näheren Angaben über Art und Umfangs der Kontrolle bzw. Dokumentation gemacht. Gestützt auf die Gesetzesbegründung kann jedoch davon ausgegangen werden, dass eine persönliche Kontrolle oder eine Vor-Ort-Kontrolle nicht erforderlich sind. Je nach Sachlage kann im Einzelfall eine Selbstauskunft des Auftragnehmers oder ein Sachverständigentestat bzw. -zertifikat (interne Revision, Datenschutzbeauftragte des Auftragnehmers, externe Prüfer, ISO 27001 Zertifikat) ausreichend sein.

Um einen sachgerechten Nachweis zu erbringen, sollte die Dokumentation zur Prüfung der Auftragsdatenverarbeitung u. a. Angaben zu den Beteiligten und zur durchgeführten Kontrolle, zum Umfang der Kontrolle, Erfassung von vertraglichen, gesetzlichen oder sonstigen Abweichungen, ggf. Beseitigungsmaßnahmen enthalten.

Mit den neuen Vorgaben zur Auftragsdatenverarbeitung wurde ebenfalls der Bußgeldkatalog entsprechend erweitert, so dass die nicht richtige, nicht vollständige oder die nicht in der vorgeschriebenen Weise erfolgte Erteilung eines Auftrages nach § 43 Abs.1 Nr.2b BDSG mit einem Bußgeld bis zu 50.000 Euro geahndet werden kann.

Ein Bußgeld droht dem Auftraggeber aber auch dann, wenn er entgegen § 11 Abs.2 S.4 BDSG vor Beginn der Datenverarbeitung seiner Kontrollpflicht gegenüber dem Auftragnehmer nicht nachkommt.

4.1.5 Maßnahmen für die Praxis

Für die Umsetzung der Neuerungen ist es empfehlenswert, in einem ersten Schritt jeden gesetzesrelevanten Abschnitt in einem Geschäftsprozess zu definieren und Verantwortliche zu benennen.

Bei Neuverträgen hat die Novellierung bereits Auswirkungen auf den vorvertraglichen Bereich, so dass die Anpassungen schon bei der Vertragsanbahnung anzusetzen sind. In diesem Zusammenhang hat sich die Erstellung einer Checkliste entsprechend der Anlage zu § 9 BDSG bewährt, welche die unternehmens- und auftragsspezifischen technischen und organisatorischen Anforderungen des Auftraggebers widerspiegelt. Zudem sollten bestehende Vertragsmuster auf ihre Konformität mit dem neuen § 11 BDSG überprüft und ggf. angepasst werden. Für Altverträge stellt sich die Rechtsfrage, ob sie durch die neuen Regelungen unwirksam sind. Da das Gesetz keine Übergangsregelungen vorsieht, müssten auch diese Verträge seit dem September 2009 den neuen Vorgaben entsprechen. Dies könnte jedoch mit dem Schutz des Vertrauens in die Beständigkeit und Nachhaltigkeit von Gesetzen kollidieren. Da die Aufsichtsbehörden jedoch überwiegend die Auffassung vertreten, dass der neue § 11 BDSG auch auf Altverträge Anwendung findet, empfiehlt es sich zwecks Vermeidung von Bußgeldern, die Altverträge zu überprüfen und ggf. durch Zusatzvereinbarungen an die neue Rechtslage anzupassen.

Des Weiteren sollte in den Unternehmen ein Kontroll- und Dokumentationsverfahren implementiert werden. Hierbei ist zu beachten, dass Detailregelungen zu Prüfintervallen und Auditrechten nicht nur auf vertraglicher Ebene festgelegt werden, sondern darüber hinaus auch in internen Organisationsanweisungen für die betroffenen Mitarbeiter des Auftraggebers Berücksichtigung finden.

4.1.6 Altes im neuen Gewand

Entgegen des Anscheins ist für die betroffenen Unternehmen mit der Novellierung nicht ein erhöhter Arbeitsaufwand verbunden. Da in der aktuellen Fassung des § 11 BDSG im Wesentlichen das präzisiert wurde, was sich bereits vor der Gesetzesänderung aus der abstrakt formulierten Rechtsnorm ergab, dürfte der Anpassungsbedarf nicht erheblich höher ausfallen als vor der Novelle.

Die Neuerungen sorgen mit ihren klaren Anforderungen an die Auftragsdatenverarbeitung daher in erster Linie für mehr Rechtssicherheit.

4.1.7 Allgemeiner Handlungsbedarf

Um datenschutzrechtliche Verstöße zu vermeiden, sollten neben der Auftragsdatenverarbeitung u. a. folgende Aspekte beachtet werden:

- Gesetzeskonforme Datenerhebung und Datenverarbeitung,
- Verpflichtung auf das Datengeheimnis gemäß § 5 BDSG,
- Bestellung eines Datenschutzbeauftragten, § 4 f BDSG,
- Beachtung des Arbeitnehmerdatenschutz gemäß § 32 BDSG,
- Notfallplan für Datenpannen, um Meldepflicht nach § 42a BDSG erfüllen zu können,
- Regelung der privaten Nutzung von Internet und E-Mail,
- Kundendatenschutz beachten, Kundendatenbanken strukturieren, Trennung Altdaten- und Neudatenbeständen,
- Hinweis auf das Widerspruchsrecht bei Werbung, § 28 IV BDSG,
- Einhaltung von Aufbewahrung- und Löschfristen.

4.2 Datenschutz in der Telemedizin: Das Beispiel des SimoBIT-Förderprojekts Med-on-@ix

Das SimoBIT-Förderprojekt Med-on-@ix ist eines der zurzeit umfangreichsten Forschungsprojekte im deutschen Rettungsdienst und erforscht den Einsatz von aktueller Telekommunikationstechnik in der Notfallrettung.[7] Zentrales Vorhaben innerhalb des Projekts ist die Schaffung einer Telenotarzt-Zentrale, die mit hochqualifizierten Notärzten, den sogenannten Tele-Notärzten, besetzt ist. Von der Einsatzstelle und aus dem Rettungswagen werden Daten, Messwerte und Live-Videos direkt an die Telenotarzt-Zentrale übertragen. Der Notarzt in der Telenotarzt-Zentrale beurteilt die Lage und die Werte. Bei Bedarf holt er zusätzliche Informationen, z.B. bei der Vergiftungszentrale oder in Datenbanken, ein und unterstützt das Rettungsteam vor Ort schließlich beim Einsatzablauf und bei der Behandlung des Patienten. Die Konzepte sind somit an einheitlichen Qualitätsmaßstäben und medizinischen Leitlinien orientiert.

Auf diese Weise ist einerseits eine notärztliche Versorgung am Einsatzort noch vor Eintreffen des Notarztes möglich, zum Beispiel in ländlichen, schwer erreichbaren Gebieten. Andererseits können – in Fällen, in denen die manuellen Fähigkeiten des Notarztes vor Ort nicht notwendig sind – gut ausgebildete Rettungsassistenten die Patienten unter Anweisung des Telenotarztes bestmöglich behandeln. Der Notarzt selbst kann an der Einsatzstelle durch einen erfahrenen Telenotarzt nicht nur bei der Behandlung des Patienten, sondern darüber hinaus einsatztaktisch effizient unterstützt werden.

Das Forschungsprojekt Med-on-@ix könnte somit in Zukunft eine hochqualifizierte notärztliche Hilfe jederzeit zugänglich machen, die Qualität der Patientenversorgung im Rettungsdienst verbessern und die Rettungsdienst-Einsätze effizienter gestalten.

Der Datenschutz kann beim Einsatz von Telemedizin im Rettungsdienst insbesondere durch den Einsatz von Anonymisierungs- oder Pseudonymisierungsverfahren gewahrt werden.

Im SimoBIT-Förderprojekt Med-on-@ix werden die Zugriffsrechte des Systems rollenbasiert nach dem Need-to-Know-Prinzip vergeben. So hat der Administrator keinen Zugriff auf die Patientendaten und der Telenotarzt nur Zugriff auf die Daten des aktuell behandelten Notfallpatienten. Hochsensible Daten wie Videos der Patienten werden 48 Stunden aufbewahrt, bevor sie unwiederbringlich gelöscht werden. Auf der einen Seite wird so die Auswertung von kritischen Fällen erlaubt. Auf der anderen Seite wird dadurch vermieden, dass diese schlecht anonymisierbaren, schwer elektronisch auswertbaren Daten in falsche Hände geraten und öffentlich gemacht werden.

Insgesamt kommt im Rechtsgutachten in Bezug auf datenschutzrechtliche Fragen zum Ausdruck, dass der Einsatz eines telemedizinischen Systems in der Notfallrettung wie bei Med-on-@ix grundsätzlich gesetzeskonform möglich ist, wenn bestimmte Rahmenbedingungen beachtet werden:

7 Siehe http://www.medonaix.de

- Es besteht eine Aufklärungspflicht für den Einsatz der Telekonsultation im Rettungsdienst, an welche dieselben Maßstäbe anzusetzen sind, die auch für andere medizinische Maßnahmen gelten.
- Es sind hohe Anforderungen zu stellen an die zugrunde liegenden Technologien und organisatorischen Abläufe.
- Es sind bei der Verarbeitung von Patientendaten die verfassungsrechtlichen Grundsätze der Zweckbindung, Erforderlichkeit und Verhältnismäßigkeit sowie das Recht des Patienten auf informationelle Selbstbestimmung zu beachten.

aus dem Rechtsgutachten im Rahmen des Projekts Med-on-@ix „Rechtsfragen des Einsatzes der Telemedizin im Rettungsdienst, Prof. Dr. iur. Christian Katzenmeier, Dr. iur. Stefania Schrag-Slavu, L.L.M., Institut für Medizinrecht, Universität zu Köln:

„Der schnelle, umfassende und zuverlässige Austausch von Patientendaten zwischen Leistungserbringern untereinander sowie zwischen Leistungsträgern kann zur Verbesserung der Qualität und Effizienz der Gesundheitsversorgung führen. Der immer umfangreicher werdende Informationstransfer im Gesundheitswesen droht jedoch, das informationelle Selbstbestimmungsrecht des Patienten zu beeinträchtigen. Dieses Spannungsverhältnis zwischen den Interessen des Einzelnen und der Gesellschaft aufzulösen, gehört zu den schwierigsten Aufgaben bei der Weiterentwicklung des Gesundheitssystems. Bei immer komplexer werdenden telemedizinischen Verfahren müssen daher die rechtlichen Voraussetzungen und Anforderungen bei der Erhebung, Verarbeitung und Nutzung personenbezogener Patientendaten mit besonderem Nachdruck beachtet werden. Hierbei sind die verfassungsrechtlichen Grundsätze der Erforderlichkeit, Zweckbindung und Verhältnismäßigkeit sowie das Recht auf informationelle Selbstbestimmung zu beachten, unabhängig davon, auf welche Weise die Datenverarbeitung geschieht. Beim Einsatz moderner Informations- und Kommunikationstechnologien ist insbesondere die Einhaltung der Zweck- und Aufbewahrungsbestimmungen durch technische Maßnahmen zu gewährleisten.

Auch die betroffenen Rechte gemäß den Datenschutzvorschriften – z.B. die Patientenansprüche auf Akteneinsicht oder die Rechte auf Auskunft, Berichtigung und Löschung der Einträge – müssen zu jeder Zeit gewahrt werden. Der Arzt darf Dritten private Informationen über den Patienten in der Regel nur dann mitteilen, wenn der Patient zugestimmt hat. Andere Erlaubnisvorschriften greifen lediglich in wenigen Ausnahmefällen und rechtfertigen nicht zwingend den Einsatz der Telemedizin.

Festzuhalten bleibt, dass ein wirksamer Datenschutz die selbstverständliche Basis aller telemedizinischen Anwendungen sein muss. Der Datenschutz ist nur dann wirksam, „wenn er die Technik, die die elektronische Datenverarbeitung hervorgebracht hat, dazu einsetzt, um die Gefahren dieser Technik wieder einzugrenzen. Es bedarf aller An-

strengungen zur technischen Innovation, um die wechselseitige Abschottung der Informationssysteme mit den Zielen des Persönlichkeits- und Geheimnisschutzes auszubauen und zu sichern“.* Obwohl dem Bundesdatenschutzgesetz ein Schutzgedanke zu Grunde liegt, der auf den ersten Blick der Telemedizin hinderlich erscheint,** nämlich die „Datenvermeidung und Datensparsamkeit“ (§ 3a BDSG), stehen die geltenden Bestimmungen dem Einsatz telemedizischer Anwendungen im Rettungsdienst nicht entgegen. Die erwähnten Ausnahmen des Datenverarbeitungsverbotes ermöglichen einen angemessenen Schutz des Patienten, ohne der fortschrittlichen Telemedizin grundsätzlich ein Hindernis zu sein. Der Sicherung der Patientenrechte kann daher auch beim Einsatz telemedizinischer Anwendungen im Rettungsdienst nachgekommen werden. Auch indem dem Telemediziner bereits bei stillschweigender Einwilligung des Patienten personenbezogene Daten übermittelt werden können, droht keine Aushöhlung des Datenschutzes, da vorher stets sowohl der Grundsatz der Datenvermeidung und Datensparsamkeit als auch das Erforderlichkeitskriterium beachtet werden müssen.“

* *Berg*, MedR 2004, 411, 414.
** So liegt es bereits im Wesen der Telemedizin, dass im Vergleich zu einem üblichen Arzt-Patienten Verhältnis eine erhöhte Datenübertragung erforderlich ist, *Berg*, MedR 2004, 411, 413. Siehe auch *Dierks/Nitz/Grau*, Gesundheitstelematik und Recht, S. 134, die „die bestehenden Rechtsunsicherheiten im Datenschutz“ als „Hemmschuh in der Entwicklung telematischer Anwendungen“ bezeichnen.

5 Mitbestimmung bei der Einführung mobiler Geschäftsanwendungen

Welf Schröter, Forum Soziale Technikgestaltung, SimoBIT-Förderprojekt MAREMBA

Die Anwendungen, Nutzungen und Ausbreitungen der diversen Formen der Mobilität (personale Mobilität, nicht-personale Mobilität und autonome mobile Maschinenwelten) bringen erhebliche Auswirkungen und Folgen für die Arbeitswelt[8] und die Verfasstheit von Geschäftsabläufen mit sich. Um diese Folgen in gesellschaftlich akzeptable Bahnen lenken zu können, bedarf es aktiver Gestaltungsimpulse. Voraussetzung der Gestaltungen sind unter anderem Vorabschätzungen der durch die Technik auslösbaren Wirkungen. Eine Schlüsselwirkung ist in der Veränderung der Organisation der Arbeit zu erkennen.

Einer der zentralen Erfolgsfaktoren für die Einführung und erfolgreiche Umsetzung mobiler Geschäfts- und Arbeitsformen ist der zufriedenstellende Aushandlungs- und Vereinbarungsprozess zwischen Arbeitgeber und Beschäftigtenvertretung. Dabei lautet ein Kernsatz: Der Wandel und die Umorganisation eines stationären Arbeitsplatzes hin zu einem teilmobilen, mobilen oder virtuell-mobilen Arbeitsplatz stellen grundsätzlich einen mitbestimmungspflichtigen Vorgang dar. Dies gilt für die Privatwirtschaft ebenso wie für den Öffentlichen Dienst.

Bei der Einführung mobiler Arbeitsplätze bzw. mobiler Telearbeitsplätze (juristisch sind mobile Arbeitsformen mobile Telearbeitsplätze) streben Betriebsräte und Personalräte in der Regel die Gleichstellung des betrieblichen und außerbetrieblichen Arbeitsplatzes über eine Betriebs- bzw. Dienstvereinbarung an. Das mobil Verfügbarmachen von Arbeit bzw. Geschäftsvorgängen sollte – um einen aushandlungsorientierten Prozess einzuleiten – möglichst frühzeitig im Dialog mit dem Betriebsrat bzw. Personalrat erfolgen. Dies erspart Fehlinvestitionen, Zeitverluste und Motivationsverluste.

Zum Mitbestimmungsbereich gehören zudem Arbeits- und Gesundheitsschutz, Ergonomie und zu gewissen Teilen das Zeitmanagement. Zu den „Knackpunkten“ eines motivations-geladenen, nachhaltigen und erfolgreichen Einführungsprozesses gehört die „gute“ Behandlung der Faktoren „Erreichbarkeit“ und „Verfügbarkeit“. Die Einführung mobiler, teilmobiler oder virtuell-mobiler Arbeitsweisen sollte durch die kooperative Erarbeitung einer Dienst- bzw. Betriebsvereinbarung geregelt und flankiert werden. Dazu gehören dringlichst auch Spielregeln für Weiterbildung und elektronische Lernumgebungen.

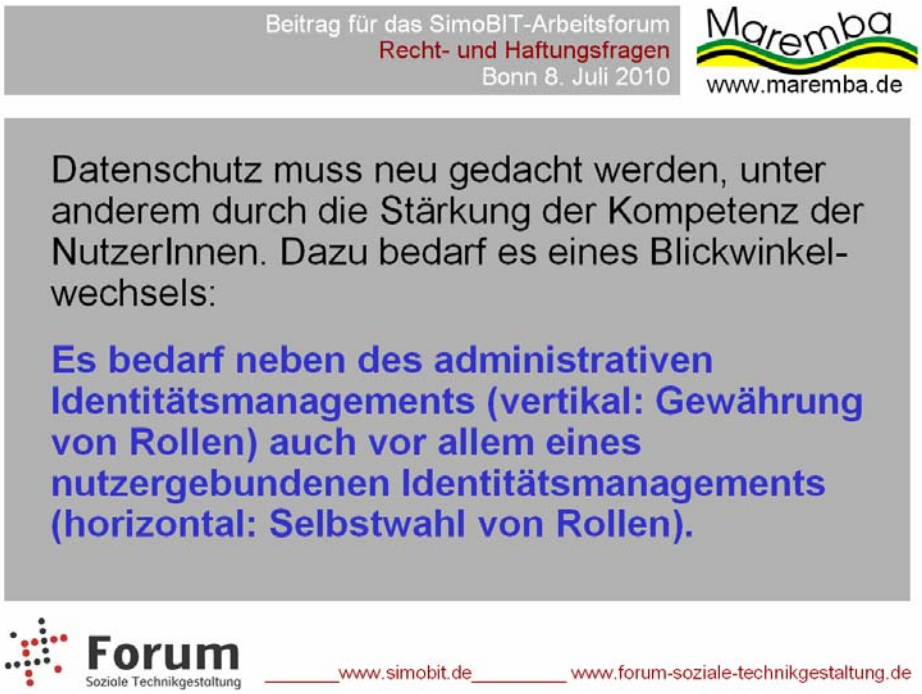
Der Abschluss einer Betriebs- bzw. Dienstvereinbarung hat den Vorteil, dass sie beide Partner – Arbeitgeber wie Arbeitnehmer – mit rechtlichen Sanktionsmöglichkeiten ausstattet. Ein Beispiel: Eine Unternehmensleitung will topdown ein elektronisches Lern-

8 Vgl. hierzu auch: Handlungsempfehlungen des SimoBIT-Arbeitsforums „Akzeptanz – Soziale Gestaltung mobiler Arbeitswelten“: Diese Liste von Handlungsempfehlungen wendet sich vor allem an Entscheidungsgremien und entscheidende Personen in Betrieben, Arbeitswelt und Verwaltungen sowie bei den Sozialpartnern und deren Verbänden.

system für die Beschäftigten im Betrieb einführen und es zugleich für alle als verpflichtend erklären. Einzelne Mitarbeiter verweigern das erzwungene Lernen. Die Geschäftsleitung greift zur Abmahnung. Der Betroffene klagt – und gewinnt. Die herrschende Rechtsmeinung besagt, dass ein Arbeitgeber in solchen Fällen keine Sanktionen verhängen kann, wenn es dafür nicht eine Betriebsvereinbarung gibt.

Aus der Perspektive der Beschäftigten sowie der Betriebs- und Personalräte sollte ein wesentlicher Baustein einer Betriebs- bzw. Dienstvereinbarung die Sicherstellung und Stärkung des informationellen Selbstbestimmungsrechts des Individuums sein. Um diese Bemühungen zu unterstützen, haben sich die Datenschützer von Bund und Ländern in ihrer „Charta für den Datenschutz“ mehrheitlich für ein verankertes Recht auf Anonymisierung und ein verankertes Recht auf Pseudonymisierung ausgesprochen. Diese sollen umfassend im Bereich des Konsums und der Privathaushalte gelten sowie in gewissen Bereichen in der Welt der Beschäftigten. Datenschutz muss so betrachtet neu gedacht werden, unter anderem durch die Stärkung der Kompetenz der Nutzer und Nutzerinnen. Dazu bedarf es eines Blickwinkel-Wechsels: Es bedarf neben des administrativen Identitätsmanagements (vertikal: Gewährung von Rollen) auch vor allem eines nutzergebundenen Identitätsmanagements (horizontal: Selbstwahl von Rollen).

Abbildung 5-1: Datenschutz und Mitbestimmung



Quelle: Forum Soziale Technikgestaltung

Ein solches Handeln erfordert eine Erweiterung der Qualifizierungsanstrengungen: Die Nutzerin bzw. der Nutzer muss die Fähigkeit erwerben, sich selbst in der virtuellen Welt schützen zu können. Das Recht auf informationelle Selbstbestimmung erfordert auch die eigenverantwortliche Pflege dieses Teil der Employability.

Jedes SimoBIT-Projekt sollte auf dem Weg in die produktive Anwendung einen verständlichen handlungsorientierten Datenschutz-„Beipackzettel“ mitbringen.

Dieser „Beipackzettel“ sollte vor allem der Orientierung der Sozialpartner dienen, um Implementierungskontroversen leichter lösen zu können.

ZUSAMMENFASSUNG: Zentrale Rechts- und Haftungsfragen bei der Einführung mobiler Geschäftsanwendungen - Die Herausforderungen im Förderschwerpunkt SimoBIT

Elektronische Signatur

- Mobile Endgeräte bieten schon heute hohen Komfort für sichere Signaturanwendungen. Im Prinzip ist der Nutzer mittels dieser Anwendungen jederzeit weltweit handlungsfähig.
- Zertifikatsbasierte Systeme stellen insbesondere für KMU und Handwerk Technologien zur Verfügung, die mobile IT-Sicherheit für diese Unternehmen gewährleisten. Die SimoBIT-Projekte haben **unterschiedliche Wege gefunden, um zertifikatsbasierte Lösungen zur Erhöhung der IT-Sicherheit und zur Schaffung von mehr Rechtssicherheit** zu integrieren. Nicht in jedem Fall ist eine eigenhändige Unterschrift bzw. eine qualifizierte elektronische Signatur erforderlich. Darüber hinaus zeigen die Erfahrungen aus den Projekten, dass mehrere, parallel eingesetzte unterschiedliche Verfahren zum Identitätsnachweis den **Bedienkomfort** für die Benutzer einer Mobile Business-Anwendung erhöhen.
- Bei der Entwicklung von Lösungen für das digitale Unterschreiben übernehmen die SimoBIT-Projektverbünde eine wichtige **Vorreiterfunktion**. Diese Anforderung stellt sich schon bald für alle Unternehmen. Ab 2010 sollen EU-weit alle öffentlichen Aufträge nur noch elektronisch ausgeschrieben werden.

Haftung

- Über die Hälfte aller Personenschäden in Verbindung mit technischen Geräten entsteht durch Fehlbedienung der Geräte und nur in wenigen Fällen durch tatsächliche Gerätefehler. Der **Haftung** aus diesen Gerätefehlern kann der Hersteller jedoch zu einem überwiegenden Teil **vorbeugen**.
- Grundsätzlich kann auf zwei Arten gehaftet werden. Zum einen infolge der so genannten **Verschuldenshaftung**, also der Haftung aufgrund persönlich vorwerfbaren Verhaltens und zum anderen infolge der **Gefährdungshaftung**. Dabei wird für Schäden gehaftet, die aufgrund der Schaffung einer besonderen Gefahrenquelle entstanden sind. Ein schuldhaftes Verhalten wie bei der Verschuldenshaftung ist nicht erforderlich. Die Haftung erfolgt allein durch eine gesetzliche Regelung. Das Produkthaftungsgesetz (ProHaftG) ist eine solche Regelung; daneben auch das Medizinproduktegesetz (MPG), das Geräte- und Produktsicherheitsgesetz (GPSG) und die Medizinprodukte-Betreiberverordnung (MPBetreibV).

- Diese Regelungen geben auch Personen gegenüber dem Hersteller einen Anspruch auf Schadensersatz und Schmerzensgeld, **die in keiner vertraglichen Beziehung zum Hersteller stehen,** sondern das jeweilige Gerät anwenden, bzw. durch die Anwendung an ihnen einen Schaden erlitten.
- In Bezug auf Haftungsfragen gibt es in den Rechtsfolgen bei mobilen Anwendungen keinen Unterschied zu herkömmlichen „stationären" Internet-Anwendungen.
- Die Etablierung eines **Telenotarzt-Systems**, wie es das Projekt „Med-on-@ix" zum Ziel hat, ist **aus strafrechtlicher Sicht nicht zu beanstanden**. Es ist jedoch zur Vermeidung einer Strafbarkeit wegen Geheimnisverrats gemäß § 203 Abs. 1 Nr. 1 bzw. Abs. 2 Nr. 1 StGB sicherzustellen, dass vor der Beteiligung des Telenotarztes an der Behandlung des Notfallpatienten dessen diesbezügliche **Einwilligung** herbeigeführt oder — soweit dies nicht möglich ist — dessen mutmaßliche Einwilligung festgestellt wird.

Datenschutz

- Die **Auftragsdatenverarbeitung** bezeichnet die Erhebung, Verarbeitung oder Nutzung personenbezogener Daten eines externen Dienstleisters im Auftrag, ohne dass ein Erlaubnistatbestand für eine Datenübermittlung gegeben sein muss. Im praktischen Alltag wird die Auftragsdatenverarbeitung oftmals auch als „Outsourcing" bezeichnet. Die inhaltliche und datenschutzrechtliche Verantwortung für die Aufgabenerfüllung verbleibt dabei beim Auftraggeber.
- Der Auftraggeber hat seine externen Dienstleister **sorgfältig im Hinblick auf die von ihm getroffenen technischen und organisatorischen Maßnahmen zur Datensicherheit auszusuchen**. Darüber hinaus ist mit der Novellierung für die Auftragsdatenverarbeitungsverträge nun ausdrücklich die **Schriftform** gesetzlich vorgeschrieben. Zudem enthält die neue Fassung des BDSG in einem 10-Punkte Katalog detaillierte Vorgaben, die als **Mindestanforderung** in einer Vereinbarung zur Auftragsdatenverarbeitung zwingend festgelegt sein müssen.
- Entgegen des Anscheins ist für die betroffenen Unternehmen mit der Novellierung **nicht ein erhöhter Arbeitsaufwand** verbunden. Die Neuerungen sorgen mit ihren klaren Anforderungen an die Auftragsdatenverarbeitung vielmehr in erster Linie für mehr Rechtssicherheit.
- Um datenschutzrechtliche Verstöße zu vermeiden, sollten des weiteren **folgende Datenschutzaspekte** beachtet werden:
    - **Gesetzeskonforme** Datenerhebung und Datenverarbeitung,
    - Verpflichtung auf das **Datengeheimnis**,

  - Bestellung eines **Datenschutzbeauftragten**,
  - Beachtung des **Arbeitnehmerdatenschutz**,
  - **Notfallplan** für Datenpannen, um Meldepflicht erfüllen zu können,
  - **Regelung der privaten Nutzung** von Internet und E-Mail,
  - **Kundendatenschutz** beachten, Kundendatenbanken strukturieren, Trennung Altdaten- und Neudatenbeständen,
  - Hinweis auf das **Widerspruchsrecht** bei Werbung,
  - Einhaltung von **Aufbewahrungs- und Löschfristen**.

- Der Datenschutz kann beim Einsatz von Telemedizin im Rettungsdienst insbesondere durch den Einsatz von **Anonymisierungs- oder Pseudonymisierungsverfahren** gewahrt werden.
- Im SimoBIT-Förderprojekt Med-on-@ix werden die **Zugriffsrechte** des Systems **rollenbasiert** nach dem Need-to-Know-Prinzip vergeben. So hat der Administrator keinen Zugriff auf die Patientendaten und der Telenotarzt nur Zugriff auf die Daten des aktuell behandelten Notfallpatienten. Hochsensible Daten wie Videos der Patienten werden 48 Stunden aufbewahrt, bevor sie unwiederbringlich **gelöscht** werden. Auf der einen Seite wird so die Auswertung von kritischen Fällen erlaubt. Auf der anderen Seite wird dadurch vermieden, dass diese schlecht anonymisierbaren, schwer elektronisch auswertbaren Daten in falsche Hände geraten und öffentlich gemacht werden.
- Insgesamt kommt im Rechtsgutachten zum SimoBIT-Förderprojekt Med-on-@ix in Bezug auf datenschutzrechtliche Fragen zum Ausdruck, dass der Einsatz eines **telemedizinischen Systems in der Notfallrettung wie bei Med-on-@ix grundsätzlich gesetzeskonform möglich** ist, wenn bestimmte Rahmenbedingungen beachtet werden:
  - Es besteht eine **Aufklärungspflicht** für den Einsatz der Telekonsultation im Rettungsdienst, an welche dieselben Maßstäbe anzusetzen sind, die auch für andere medizinische Maßnahmen gelten.
  - Es sind hohe **Anforderungen** an die zugrunde liegenden **Technologien und organisatorischen Abläufe** zu stellen.
  - Es sind bei der Verarbeitung von Patientendaten die verfassungsrechtlichen Grundsätze der **Zweckbindung, Erforderlichkeit und Verhältnismäßigkeit** sowie das Recht des Patienten auf **informationelle Selbstbestimmung** zu beachten.

Mitbestimmung

Wenn mobile Geschäftsanwendungen in einem Betrieb umgesetzt werden sollen, entstehen neue Herausforderungen für die Mitarbeiter sowie den Betriebs- bzw. Personalrat. Zum einen können Teile der Mitarbeiterschaft die veränderten Anforderungen als problematisch und tendenziell als Bedrohung für ihre Position oder ihren Arbeitsplatz begreifen. Zum anderen kann eine Gruppe von technikaffinen, qualifizierten Mitarbeitern entstehen, die eine mobile und damit auch häufig flexible Arbeitsumgebung schätzen. Gegenüber dieser Gruppe verlieren althergebrachte Regelungen zur Leistungskontrolle und Kontrolle der Arbeitszeit an Bedeutung und möglicherweise auch die Positionen des Betriebs- oder Personalrats.

Ein Erfolg versprechender Weg scheint zu sein, auf dem **Wege der Kooperation** Einfluss auf die „mobile“ Unternehmensstrategie zu nehmen. Dies bedeutet, dass mit dem Ziel einer ergebnisorientierten Zusammenarbeit die Mitarbeitervertretung eigene Gestaltungsvorstellungen – und zwar möglichst von Beginn des Umstrukturierungsprozesses an – einbringt und die Unternehmensleitung die **Möglichkeiten der Partizipation** der Mitarbeiter als Chance begreift, die Effizienzvorteile mobiler Geschäftsprozesse auszuschöpfen.

Weiterführende Literatur und Hinweise

Balfanz, Dirk; Schröter, Welf (Hg.) (2010): Gestaltete Virtualität: Realität der neuen Medien in der Arbeitswelt. Standortbestimmung und Perspektiven, Mössingen-Talheim

Berg, Wilfried: Telemedizin und Datenschutz, in: MedR 2004, S. 411-414

Bundesdatenschutzgesetz (BDSG), Stand: 1. April 2010

Dierks, Christian/Nitz, Gerhard/Grau, Ulrich: Gesundheitstelematik und Recht – Rechtliche Rahmenbedingungen und legislativer Anpassungsbedarf, Frankfurt a.M. 2003

Düsseldorfer Kreis: Die obersten Aufsichtsbehörden für den Datenschutz im nicht-öffentlichen (privaten) Bereich haben sich nach dem Ort ihres ersten Zusammentreffens im Jahr 1977 als “Düsseldorfer Kreis” benannt. Die wichtigsten Ergebnisse ihrer Treffen werden in Beschlüssen bekannt gemacht.

Eckpunkte der 79. Konferenz der Datenschutzbeauftragten des Bundes und der Länder vom 17./18. März 2010: „Ein modernes Datenschutzrecht für das 21. Jahrhundert“

Entschließung der Konferenz der Datenschutzbeauftragten des Bundes und der Länder vom 22. Juni 2010, Beschäftigtendatenschutz stärken statt abbauen, Erscheinungsdatum: 16.09.2008

Gesetz über Rahmenbedingungen für elektronische Signaturen (Signaturgesetz - SigG): Signaturgesetz vom 16. Mai 2001 (BGBl. I S. 876), zuletzt geändert durch Artikel 4 des Gesetzes vom 17. Juli 2009 (BGBl. I S. 2091) (SigG)

Gesetzentwurf der Bundesregierung, Entwurf eines Gesetzes zur Regelung des Beschäftigtendatenschutzes, 25.08.2010

Hintergrundpapier zum Entwurf eines Gesetzes zur Regelung des Beschäftigtendatenschutzes - Kabinettbeschluss vom 25.08.2010

Katzenmeier, Christian; Schrag-Slavu, Stefania. (2009). Rechtsfragen des Einsatzes der Telemedizin im Rettungsdienst (Kölner Schriften zum Medizinrecht). Wien: Springer

Konferenz der Datenschutzbeauftragten des Bundes und der Länder

Naß, E., Renno, C., Rörtgen, D. und Skorning, M. (2010). Forschungsprojekt Med-on-@ix: Telemedizin im Rettungswesen. Deutsches Ärzteblatt 107, no. 14

OnFormA - Online-Forum mobiles Arbeiten - arbeitnehmerorientiertes, weitgehend kostenfreies Informations- und Beratungsangebot zum Thema mobiles Arbeiten, Ziel ist u.a. die Erstellung von Mustervereinbarungen und Handlungshilfen für die Interessenvertretungen. OnFormA ist ein Projekt der T-Mobile Deutschland GmbH Vereinte Dienstleistungsgewerkschaft ver.di, Initiative D21 e.V., debitel AG, ver.di-innotec gGmbH

Richtlinie 1999/93/EG des Europäischen Parlaments und des Rates vom 13. Dezember 1999 über gemeinschaftliche Rahmenbedingungen für elektronische Signaturen

Rump, Jutta; u.a. (2010): Managing Electronic Mobility. Eine Orientierungshilfe für Fach- und Führungskräfte zur Technikfolgenabschätzung, Sternenfels

Schaar, Peter (2010): Ein modernes Datenschutzrecht für das 21. Jahrhundert, Eckpunktepapier, http://www.bfdi.bund.de/

Verordnung zur elektronischen Signatur (Signaturverordnung - SigV) - Signaturverordnung vom 16. November 2001 (BGBl. I S. 3074), zuletzt geändert durch die Verordnung vom 17. Dezember 2009 (BGBl. I S. 3932)

Alle Veröffentlichungen des Förderschwerpunkts SimoBIT - Sichere mobile Informationstechnik in Mittelstand und Verwaltung sind auf der Website www.simobit.de zu finden.

SimoBIT-Förderprojekte im Überblick

Kompetenznetzwerk Gesundheitswirtschaft

- **Med-on-@ix -** E-Health in der Notfallmedizin (www.medonaix.de)
- **VitaBIT -** Offene Plattform für sichere Anwendung mobiler Informationsdienste in der Pflegelogistik **(**www.vitabit.org**)**
- **OPAL Health -** Optimierte und sichere Prozesse durch mobile und intelligente Überwachung und Lokalisierung von Betriebsmitteln und Inventar in Kliniken und Krankenhäusern (www.opal-health.de)

Kompetenznetzwerk Maschinenbau

- **Mobile Servicewelten** im Internationalen Service des Maschinen- und Anlagenbaus (www.infoman.de)
- **SiWear** - Sichere Wearable-Systeme zur Kommissionierung industrieller Güter sowie für Diagnose, Wartung und Reparatur (www.siwear.de)
- **R2B** - Robot to Business, Informationstechnische Integration teilautonomer Prozesse und mobiler Maschinen in Geschäfts- und Dienstleistungsmodellen (www.agrardienstleistungen.de/r2b/)

Kompetenznetzwerk Öffentliche Verwaltung

- **Mobis Pro** - Mobiles Informationssystem zur Prozessoptimierung in Feuerwehren und öffentlichen Verwaltungen (www.mobis-pro.de)
- **simoKIM** - Sicheres und mobiles kommunales Infrastruktur-Management (www.simokim.de)
- **Mobility@forest** - Entwicklung einer neuartigen nutzerorientierten IT-Infrastruktur eines mobilen Arbeitsplatzes für den Forstbetrieb (www.mobility-forest.de)

Kompetenznetzwerk Handwerk und kleine Unternehmen

- **MAREMBA** - Mobile Assistenz für das Ressourcenmanagement in der Bau-Auftragsabwicklung (www.maremba.de)
- **ModiFrame** - Ein Framework für mobile Dienste (www.modiframe.de)
- **M3V** - Mobile Multimediale Multilieferanten-Vertriebsinformationssysteme (www.m3v-projekt.de)

ISSN 2190-6467