

SOAinVO

Chancen und Risiken von
Service-orientierten Architekturen
in Virtuellen Organisationen



UNIVERSITÄT
KOBLENZ · LANDAU

Universität Koblenz-Landau

ULD



Unabhängiges Landeszentrum für
den Datenschutz Schleswig-Holstein

Johann Bizer
Rüdiger Grimm

Steffen Staab

Sebastian Meissner

Daniel Pähler

Christoph Ringelstein

Martin Rost

Jan Schallaböck

Felix Schwagereit

SOAinVO

Chancen und Risiken von Service-orientierten Architekturen in Virtuellen Organisationen

Version 1.0

**Gefördert vom Bundesministerium für Bildung und Forschung im
Rahmen der Innovations- und Technikanalyse**

Institut für Informatik der Universität Koblenz-Landau

Steffen Staab
Christoph Ringelstein
Felix Schwagereit

*Institut für Wirtschafts- und Verwaltungsinformatik der Universität
Koblenz-Landau*

Rüdiger Grimm
Daniel Pähler

Unabhängiges Landeszentrum für den Datenschutz Schleswig-Holstein

Johann Bizer
Sebastian Meissner
Martin Rost
Jan Schallaböck

Executive Summary

Ziele

Dienst-orientierte Architekturen (englisch: *Service-oriented Architectures – SOA*) stellen ein Paradigma dar, das geeignet ist, um neue und existierende sowie verteilte Softwareapplikationen zu integrieren. Gerade mit aktuellen Standards, wie den Web Services als konkrete Realisierung einer standardisierten SOA-Umgebung, lassen sich hierbei auch Unternehmensgrenzen überbrücken, um komplexe Netzwerke von Softwareanwendungen zu entwickeln und zu betreiben. Diese technische Innovation wird getrieben von der ökonomischen Motivation zur Fokussierung auf die Kernkompetenzen der individuellen Organisation, die eine Wertschöpfung in einer unternehmensübergreifenden *virtuellen Organisation* (VO) bedingt. Diese Zusammenstellung organisationsübergreifender Dienste benötigt technische und ökonomische Innovationen, sie benötigt aber auch eine Neubewertung rechtlicher Aspekte vor allem — aber nicht nur — im Bereich des Datenschutzes (vgl. Abbildung 1).

Das Ziel dieser Analyse ist es, in diesem Rahmen Gestaltungsvorschläge für eine beherrschbare SOA anhand rechtlicher und technischer Kriterien zu entwickeln.

Methodik

Die vorliegende Arbeit entwickelt zunächst einen rechtlichen und technischen Rahmen zur Ableitung von Kriterien für eine beherrschbare SOA. Die rechtlichen und technischen Kriterien sollen die grundlegenden Anforderungen nach Beherrschbarkeit von und Verantwortlichkeit in komplexen SOA-Anwendungen sichtbar machen. Die Kriterien werden für eine Analyse von fünf unterschiedlichen Anwendungsszenarien angewendet. Als Ergebnis der Analyse ergeben sich fünf klar identifizierbaren Aufgabenbereiche, die durch 33 detaillierte Gestaltungsvorschläge mit Lösungsansätzen ausgeführt werden. Daraus ergibt sich weiterer Forschungsbedarf zur Nutzung des Innovationspotentials einer beherrschbaren SOA.

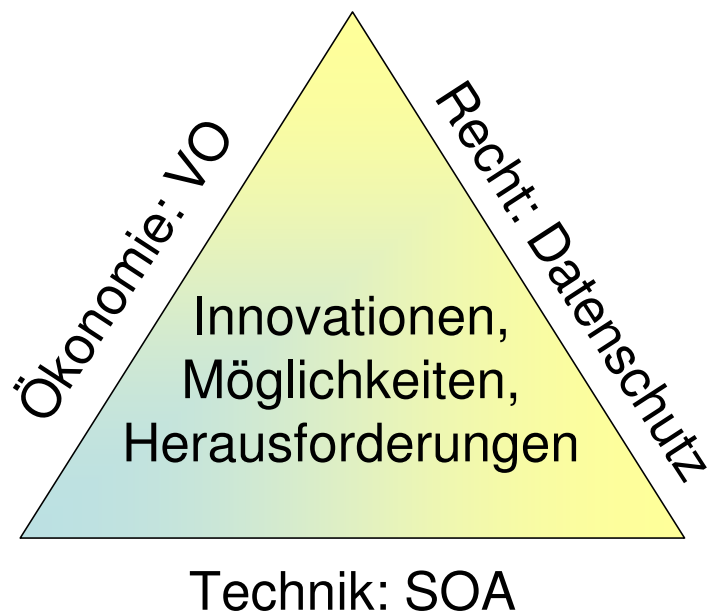


Abbildung 1: Ziel der Analyse: Herausforderungen und Möglichkeiten durch die Innovation mit SOA und Virtuellen Organisationen

Ergebnisse

Chancen und Risiken der neuen Service-orientierten Architektur liegen im Bereich der *Beherrschbarkeit* von SOA-Lösungen und des Nachvollzugs *verantwortlichen Handelns* mit SOA-Lösungen. Die vorliegende Analyse identifiziert vier aussichtsreiche Faktoren zur Beherrschbarkeit und Verantwortlichkeit:

1. Zusicherungen von Dienstqualität und Datenschutzkonformität,
2. Unterrichtung vor einem Dienst auf der Basis von Zusicherungen,
3. Protokollierung der Erbringung von Diensten und der Erhebung und Verarbeitung von Daten,
4. Auskunft zu jeder Zeit auf der Basis gegebener Zusicherungen und protokollierter Ereignisse.

Zusicherungen und Protokollierung repräsentieren eine eher technische Sicht. Sie erfordern vor allem eine standardisierte Sprache, die sowohl die Datenformate als auch ausreichend semantische Annotationen und Schlussregeln enthält. Unterrichtung und Auskunft repräsentieren eine eher rechtliche

Sicht zur Erfüllung der zugehörigen Anforderungen des Datenschutzes. Sie gehen aber über den Datenschutz hinaus und sind zu allgemeineren Faktoren der Beherrschbarkeit zu verallgemeinern. Sie lassen sich zu folgenden fünf Aufgabenkomplexen zur Gestaltung einer beherrschbaren SOA für verantwortliches Handeln führen:

1. Eine *Verallgemeinerung von Zusicherungen* über den Datenschutz hinaus. Eine standardisierte Sprache für Zusicherungen kann etwa folgende Themenbereiche ansprechen:
 - Datenschutzpolicies
 - Service-Level-Agreements
 - Quality-of-Service
 - Dienstleistungsverträge
2. *Protokolle* werden zurzeit auf verschiedenen Ebenen geführt, zum Beispiel an Firewalls (IP-Pakete), an Web-Servern (HTTP-Requestes und -Responses), an E-Mail-Servern (Annahme, Weiterleitung und Auslieferung von E-Mail). Dabei wird im Prinzip „alles“ in zeitlicher Abfolge protokolliert. Die Protokolldaten dienen teilweise zur Untersuchung von Fehlern oder Angriffen durch menschliche Experten, teilweise zum halbautomatisierten Data-Mining, um den unstrukturierten Datenmassen strukturierte inhaltliche Aspekte abzugewinnen. Tatsächlich haben Protokolldaten aber eine viel weitreichendere Bedeutung auch für
 - Forensik für die IT-Revision
 - Erteilen von Auskunft über den Dienst an Kunden und an Betroffene
 - Überprüfung von Zusicherungen für Kunden und Betroffene
 - Überprüfung von Zusicherungen und gesetzeskonformen Verhaltens durch unabhängiges Audit
3. *Aggregation von Zusicherungen*: Zusicherungen treten nicht isoliert auf. Zum einen erteilt *ein* Dienst oder *ein* Dienstleister mehrere Zusicherungen zu verschiedenen Dienstaspekten zu verschiedenen Zeiten, zum anderen geben *verschiedene* Dienste oder Dienstleister in einer SOA unterschiedliche Zusicherungen, die sich dabei gleichwohl auf einen gemeinsamen übergeordneten Dienst beziehen können. Daher sind einzelne Zusicherungen zu komplexen Zusicherungen zusammenzufassen. Dafür ist eine standardisierte Sprache erforderlich, die semantische Schlussfolgerungen zulässt. Hierfür ist auch eine geeignete Authentifizierung zur

Verfügung zu stellen, die solche Zusicherungen rechtsverbindlich absichert.

4. *Zusicherung und Protokollierung*: Apriori-Zusicherungen, Protokollierung im laufenden Dienst, sowie die Auskunft und Überprüfung gehören in einen gemeinsamen Dienstkontext. Zurzeit werden diese Aufgaben in ganz unterschiedlichen Formaten und Semantiken (d.h. informatorisch: in unterschiedlichen Sprachen) und zudem noch verteilt ausgeführt. Eine inhaltliche Zusammenführung ist hier nötig, um Zusicherungen in semantisch klarer Weise festzuhalten, zu komponieren, und später wiederfinden und interpretieren zu können.
5. *Nutzungskompetenz*: Der Umgang mit Zusicherungen und Protokollen für die Unterrichtung, Auskunft und Überprüfung muss nicht nur technisch *möglich* sein, sondern die Anwender müssen zu ihrer Nutzung auch *fähig* sein. Über die standardisierte Sprache hinaus bedarf es Abstraktions- und Interpretationsverfahren, die aus der großen Datenmenge zur rechten Zeit die rechte Menge und Struktur an relevanten Aussagen zur Verfügung stellen. Das gilt sowohl auf der Ebene der Benutzer als auch der Ebene der automatisierten Prozesse. Diese beiden Aufgaben kann man mit den Stichworten

- Abstraktion und
- Schlussfolgerungen

zusammenfassen.

Handlungsempfehlungen und Forschungsbedarf

Es werden konkrete, auf Basis existierender Technologien umsetzbare Handlungsempfehlungen für Unternehmen gegeben. Diese zeigen auf, wie in den Unternehmen bereits heute der Datenschutz verbessert und der Einsatz der im Abschnitt „Forschungsbedarf“ anvisierten technischen Lösungen vorbereitet werden kann.

Aus den fünf Gestaltungsaufgaben wird Forschungsbedarf abgeleitet in Bezug auf die Entwicklung von Beschreibungssprachen für Zusicherungen und Protokollierung, die untereinander kompatibel und für automatisiertes Schließen geeignet sind, auf eine Werkzeugentwicklung zur Nutzung dieser Sprachen, auf ihre Einbettung in relevante Anwendungsumgebungen, und schließlich auf die Entwicklung einer Referenz-API für eine Middleware, die die Beherrschbarkeitsfunktionen umsetzt.

Innovationspotenzial

Die verschiedenen Forschungsaufgaben eröffnen auf mehrere Arten Innovationspotenzial: Das Verständnis und die Kontrolle von Diensten und dienstübergreifenden Prozessen in Unternehmen werden gefördert. Neue Möglichkeiten der Vernetzung über Unternehmensgrenzen hinweg sowie der kontrollierten Weitergabe von Verantwortlichkeiten beim Zusammenschluss mehrerer Unternehmen ebnen den Weg für neuartige Organisationsformen und Geschäftsmodelle. Eine erleichterte Konformität der Unternehmen zu Compliance- und Auditing-Anforderungen kann, wie auch die verbesserte Unterstützung von Datenschutzprinzipien, sowohl den Unternehmen als auch ihren Kunden zum Vorteil gereichen.

Inhaltsverzeichnis

1	Einleitung	4
1.1	Ziel der Analyse	4
1.2	Gegenstand der Analyse	5
1.2.1	Was ist eine Virtuelle Organisation?	5
1.2.2	Was ist eine Service-orientierte Architektur (SOA), was sind Web Services?	6
1.3	Methodik der Analyse	8
1.4	Aufbau der Analyse	9
2	Juristischer Rahmen	11
2.1	Rechtliche Grundlagen	11
2.1.1	Datenschutzrecht	12
2.1.2	Schutz von Betriebs- und Geschäftsgeheimnissen	27
2.2	Weitere Rahmenbedingungen	29
2.2.1	Kosten	29
2.2.2	Akzeptanz	30
2.2.3	Sicherheit	31
2.3	Festlegung von Prüfungsschritten für die datenschutzrechtliche Analyse der Szenarien	31
2.3.1	Erläuterung des Prüfungsschemas	33
3	Technischer Rahmen	35
3.1	Einflussgrößen auf den Service-Lebenszyklus	35
3.2	Beherrschbarkeit	36
3.2.1	Faktoren, die Beherrschbarkeit konstituieren	37
3.2.2	Subjektive Beherrschbarkeit: Möglichkeit und Fähigkeit zur Beherrschung	40
3.2.3	Zusammenfassung	40
3.3	Zusicherungen und Unterrichtung	41
3.3.1	Situation heute	41
3.3.2	Angestrebtes Ziel	46

3.3.3	Ableitung von Analysefragen	47
3.4	Protokollierung und Auskunft	51
3.4.1	Situation heute	51
3.4.2	Angestrebtes Ziel	54
3.4.3	Ableitung von Analysefragen	56
4	Analyse der Szenarien	58
4.1	PotatoSystem: Basisszenario Datenschutz, virtuelle Güter . . .	58
4.1.1	Akteure	59
4.1.2	Beziehungen der Akteure	60
4.1.3	Datenflüsse zwischen den Akteuren	62
4.1.4	Verantwortlichkeit	63
4.1.5	Service-orientierte Architektur	63
4.1.6	Ursprung des Szenarios	67
4.2	Hanival: Fortgeschrittenes Datenschutzszenario, Netzservices .	69
4.2.1	Akteure	69
4.2.2	Beziehungen der Akteure	72
4.2.3	Datenflüsse zwischen den Akteuren	73
4.2.4	Verantwortlichkeit	74
4.2.5	Service-orientierte Architektur	75
4.2.6	Ursprung des Szenarios	82
4.3	Amazon Mechanical Turk: Länderübergreifendes Datenschutz-	
	szenario, Verantwortlichkeitsproblematik und Einbezug priva-	
	ter Endanbieter	84
4.3.1	Akteure	86
4.3.2	Beziehungen der Akteure	87
4.3.3	Datenflüsse zwischen den Akteuren	88
4.3.4	Verantwortlichkeit	89
4.3.5	Service-orientierte Architektur	91
4.3.6	Ursprung des Szenarios	95
4.4	PSB – Entwicklung von Produktionsstraßen: Basisszenario für	
	Betriebs- und Geschäftsgeheimnisse	95
4.4.1	Akteure	96
4.4.2	Beziehungen der Akteure	97
4.4.3	Datenflüsse zwischen den Akteuren	97
4.4.4	Verantwortlichkeit	98
4.4.5	Service-orientierte Architektur	98
4.4.6	Ursprung des Szenarios	102
4.5	PSB – Wartung von Produktionsstraßen: Fortgeschrittenes	
	Szenario für Betriebs- und Geschäftsgeheimnisse	102
4.5.1	Akteure	104

4.5.2	Beziehungen der Akteure	104
4.5.3	Datenflüsse zwischen den Akteuren	105
4.5.4	Verantwortlichkeit	106
4.5.5	Service-orientierte Architektur	106
4.5.6	Ursprung des Szenarios	109
4.6	Rechtliche Analyse der Szenarien	111
4.6.1	Allgemeine Bemerkungen	111
4.6.2	PotatoSystem	116
4.6.3	Hanival	122
4.6.4	Amazon Mechanical Turk	126
4.6.5	PSB – Entwicklung und Wartung von Produktionsstra- ßen	136
5	Anforderungen und Lösungsvorschläge	138
5.1	Methodik der Gestaltungsvorschläge	138
5.2	Zusicherungen und Unterrichtung	139
5.3	Protokolle und Auskunft	147
5.4	Aufgabenbereiche	153
6	Innovation und Forschungsbedarf	156
6.1	Ergebnisse der Analyse	156
6.2	Handlungsempfehlungen und Forschungsbedarf	158
6.2.1	Handlungsempfehlungen	158
6.2.2	Forschungsbedarf	159
6.3	Innovationspotenzial	161
	Index	163
	Literaturverzeichnis	164

Kapitel 1

Einleitung

1.1 Ziel der Analyse

Die Organisationsstrukturen von Unternehmen sind in den letzten 20 Jahren einem drastischen Wandel unterlegen, der sich knapp durch Stichworte wie „Fokussierung auf Kernkompetenzen“ und „Outsourcing von Nicht-Kernaufgaben“ beschreiben lässt. Dieser Wandel hält an und erfordert von den Organisationen eine schnelle Anpassbarkeit ihrer Geschäftsprozesse bei gleichzeitiger intensiver Kollaboration in *virtuellen Organisationen*.

Existierende etablierte IT-Strukturen erzielen nicht die erforderliche Flexibilität, um die Anpassbarkeit der Geschäftsprozesse innerhalb von Organisationen und über Organisationsgrenzen hinweg zu erbringen. Mit dem noch relativ neuen Paradigma der dienst-orientierten Architekturen (engl.: *Service-oriented architecture* — *SOA*) wird hingegen eine Art der Systemmodellierung implementiert, die es erlaubt, IT-Systeme unabhängig voneinander zu entwickeln, zu warten und zu betreiben und dennoch eine automatisierte IT-Kommunikation über Unternehmensgrenzen hinweg zu erreichen. Diese Aufteilung von Aufgaben ermöglicht den Einsatz einer SOA auch gerade in einer virtuellen Organisation.

Für die Realisierung von SOA-Lösungen existieren verschiedene herstellerabhängige Paradigmen (z.B. DotNet von MicrosoftTM) und offene Standards (WSDL, UDDI, SOAP, WS-BPEL, WS-Security, P3P, WS-Policy, ... von OASIS und W3C) und Plattformen (z.B. JBoss). In den vergangenen Jahren ist ein deutlich gestiegenes Interesse der Wirtschaft an SOA-Lösungen zu verzeichnen, das sich bisher aber noch auf Integrationsaufgaben innerhalb eines Unternehmens fokussiert. Die Größe des Interesses spiegelt einerseits die Bedeutsamkeit der Aufgabe wider, die Zurückhaltung beim unternehmensübergreifenden Einsatz von SOAs reflektiert aber auch, dass zahlreiche

offene Fragestellungen den Einsatz von SOAs in virtuellen Organisationen behindern. Das Ziel dieser Analyse ist es, Probleme beim Einsatz von SOAs in Virtuellen Organisationen zu identifizieren und sowohl die jeweiligen Risiken als auch die sich ergebenden Chancen zu benennen. Probleme, die hier auftreten, liegen auf der technischen Seite vor allem in der hohen Komplexität und der Intransparenz der Prozesse. Die Probleme auf der rechtlichen Seite ergeben sich vor allem durch die Weitergabe von Verantwortlichkeit und einem damit einhergehenden Kontrollverlust über die Zweckbindung von Daten. Ein Aufarbeitung dieser Probleme kann aber nicht nur zu einem zusätzlichen Aufwand führen, sondern zugleich zu einem Gewinn an Beherrschbarkeit über das SOA-basierte System und damit zu wirtschaftlichen Vorteilen bei gleichzeitiger besserer Compliance mit rechtlichen und vertraglichen Randbedingungen.

1.2 Gegenstand der Analyse

1.2.1 Was ist eine Virtuelle Organisation?

Eine Virtuelle Organisation besteht aus rechtlich unabhängigen Organisationen, ihren Elementen. Diese arbeiten in einer Virtuellen Organisation zum Zwecke der Erreichung bestimmter Ziele für einen begrenzten Zeitraum zusammen. Ist das Ziel wirtschaftlicher Natur und steht die Bearbeitung von Kundenaufträgen im Vordergrund, so spricht man auch von einer Virtuellen Unternehmung [Brü99]. Diese zeichnen sich gegenüber anderen Organisationsformen, wie beispielsweise strategischen Allianzen, durch eine größere Dynamik und eine stärkere Betonung von externer Integration aus.

Ein wesentlicher Grund für das Entstehen von Virtuellen Organisationen ist der beschleunigte Wandel des organisatorischen Umfeldes, der insbesondere durch einen sich verschärfenden Wettbewerb gekennzeichnet ist [Mös01]. Den wachsenden Anforderungen von außen kann eine Organisation nur dann entsprechen, wenn sie flexibel und gleichzeitig effizient ist. Diese Balance erreicht die virtuelle Organisation einerseits durch ihre Fähigkeit, sich durch flexibles Aufnehmen und Ausschließen von Elementen an die aktuellen Aufgaben anzupassen. Andererseits können sich die einzelnen Elemente sehr stark spezialisieren und so eine hohe Effizienz in ihren eigenen Abläufen erreichen. So ist eine Virtuelle Organisation gekennzeichnet durch die Charakteristika [Mös01]:

- Modularität: Die Elemente der Virtuellen Organisation sind modulare Einheiten mit dezentraler Entscheidungskompetenz und Ergebnisverantwortung.

- Heterogenität: Die Elemente der Virtuellen Organisation weisen unterschiedliche Leistungsprofile hinsichtlich ihrer Kompetenzen auf.
- Räumliche und zeitliche Verteiltheit: Für das Erfüllen des Ziels der Virtuellen Organisation ist der konkrete Ort und Zeitpunkt der Erbringung von Teilleistungen nicht relevant.

Das Charakteristikum der räumlichen Verteiltheit ist maßgeblich mitverantwortlich für die Notwendigkeit der Nutzung einer technischen Infrastruktur. Auf Grund der räumlichen Trennung der Elemente der virtuellen Organisation ist die Kommunikation nur über technische Hilfsmitteln möglich. Dies bedeutet insbesondere, dass auch die Informationssysteme, die schon aus Effizienzgründen in jeder Organisation vorhanden sind, miteinander kommunizieren müssen.

1.2.2 Was ist eine Service-orientierte Architektur (SOA), was sind Web Services?

Unter Service-orientierter Architektur versteht man ein Gestaltungsprinzip für die Orchestrierung von Diensten im Internet, für das die Standardisierung der Web-Service-Schnittstellen durch das World Wide Web Consortium (W3C) eine konkrete Ausprägung liefert. Web Services erfüllen in diesem Sinne das Bauprinzip von SOA. Das Bauprinzip einer SOA beruht auf Standards, die auf einfache und sichere Weise Dienste derart zusammenspielen lässt, dass sie modular aufgebaut und verteilt sind, lose gekoppelt bleiben (d.h. nur nach Bedarf genutzt und zusammengelegt werden - „event driven“), sowie aufgrund eines Verzeichnisdienstes gefunden werden können.

Web Services setzen eine SOA in Form von konkreten Spezifikationen und Produkten um. Dabei sind drei grundlegende Komponenten herauszustellen:

1. die Kommunikation, die in Form von SOAP-Nachrichten und Austauschregeln spezifiziert ist;
2. eine Dienstbeschreibung, die in Form von WSDL („Web Services Description Language“) spezifiziert ist und von der erwartet wird, dass alle Web Services ihre Dienste auf diese Weise beschreiben und nach außen darstellen;
3. ein Verzeichnisdienst, aufgrund dessen andere Dienste einen zusätzlich benötigten Dienst automatisch im Netz finden können. Für rein interne Web Services, die nur auf eigene Komponenten zugreifen, ist ein solcher Verzeichnisdienst nicht erforderlich. Er stellt aber einen wesentlichen Baustein zur Öffnung von Web Services nach außen dar.

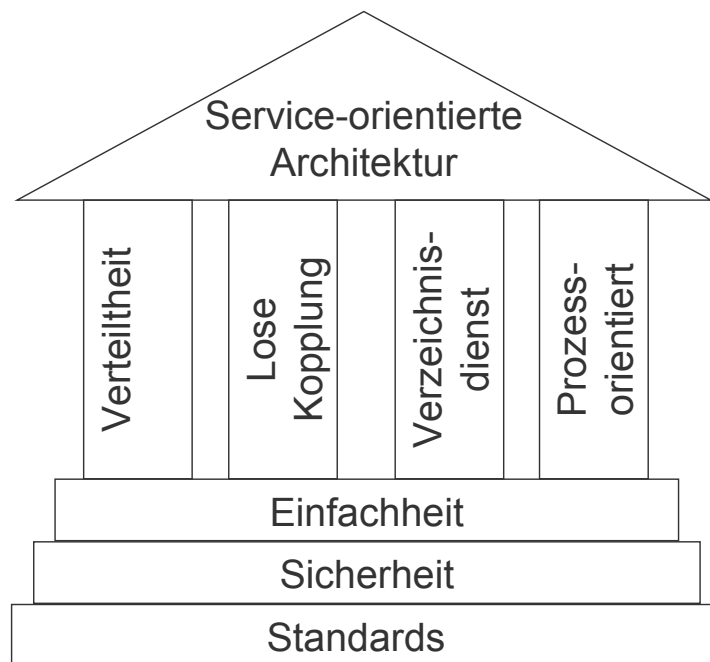


Abbildung 1.1: „SOA-Tempel“ nach [DJMZ05, S. 11]

Wesentlich für SOA ist demnach die klare Beschreibung der Schnittstellen nach einheitlichen Formaten zum Auffinden und Nutzen von Diensten. Die Schnittstellen bieten damit nicht nur die Gelegenheit zur Zusammenschaltung von Diensten zu komplexeren Diensten, sowie umgekehrt zur Zerlegung von komplexen Diensten in flexibel austauschbare modulare Komponenten, sondern sie bieten auch die Gelegenheit zur Beobachtung (Monitoring) von Diensten an ihren Nutzungsschnittstellen. Das ist ein wesentliches Motiv zur verbesserten Beherrschbarkeit von SOA-basierten Web Services.

Das World Wide Web Consortium (W3C) ist in der Standardisierung von Schnittstellen führend. Durch die Aktivitäten des W3C sind bereits eine Reihe von Bausteinen spezifiziert, andere befinden sich noch in Arbeit¹. Weitere Standardisierungsgremien, die zu Web-Services beitragen, sind OASIS (UDDI, BPEL) und IETF (vor allem SSL/TLS, IPSec und LDAP). Es gibt inzwischen eine Reihe von Herstellern, die ganze Plattformen zur Implementierung von Web-Services anbieten, die wichtigsten sind Software AG mit Crossvision, Microsoft mit .NET, IBM mit Websphere, BEA mit WebLogic und Red Hat Middleware mit JBoss.

¹siehe <http://www.w3.org/2002/ws>

1.3 Methodik der Analyse

Diese Analyse verfolgt einen interdisziplinären Ansatz, um Service-orientierte Architekturen in virtuellen Organisationen sowohl in rechtlicher als auch in technischer Hinsicht angemessen bearbeiten zu können. Die unterbreiteten Lösungsvorschläge beziehen sich auf konkrete Gestaltungsanforderungen, die zuvor aus allgemeinen rechtlichen und technischen Anforderungen sowie einer Analyse konkreter Szenarien entwickelt werden. Im Rahmen der Analyse werden also zunächst allgemeine rechtliche und technische Anforderungen identifiziert. Diese werden dann in mehreren Schritten immer weiter konkretisiert. Am Ende dieses Konkretisierungsprozesses stehen explizite Gestaltungsanforderungen an und Lösungsvorschläge für die Implementierung Service-orientierter Architekturen.

Ein erster Schritt der Analyse besteht darin, den rechtlichen und technischen Rahmen abzustecken, aus dem dann allgemeine rechtliche und technische Gestaltungsanforderungen abgeleitet werden. Grundlegende Gestaltungsanforderungen sind die Verantwortlichkeit in und die Beherrschbarkeit von Service-orientierten Architekturen. Diese allgemeinen Anforderungen werden in einem weiteren Schritt zu den vier Faktoren Zusicherung, Unterrichtung, Protokollierung und Auskunft konkretisiert.

Die Analyse beispielhafter, konkreter Szenarien unter Verwendung der allgemeinen rechtlichen und technischen Anforderungen dient zum einen der Beschreibung der Technik in einer konkreten SOA-Anwendung, zum anderen der Identifizierung verschiedener Aufgabenbereiche, auf deren Grundlage eine weitere Konkretisierung und Überprüfung der Gestaltungsanforderungen vorgenommen wird. Thematisch decken die Szenarien virtuelle Organisationen in unterschiedlicher Komplexität, bewährte und innovative Geschäftsmodelle, Dienstleistungen und virtuelle Güter, nationale und länderübergreifende virtuelle Organisationen sowie den Schutz von personenbezogenen Daten und von Betriebs- und Geschäftsgeheimnissen ab.

In einem weiteren Schritt werden auf Grundlage der zuvor identifizierten rechtlichen und technischen Anforderungen sowie der Ergebnisse der Szenarienanalyse 33 konkrete Gestaltungsanforderungen für SOA-Anwendungen formuliert, welche nach den vier Faktoren Zusicherung, Unterrichtung, Protokollierung und Auskunft strukturiert sind. Zu jeder dieser Gestaltungsanforderungen wird ein praktikabler Lösungsvorschlag unterbreitet.

Aus den in der Analyse herausgearbeiteten Gestaltungsanforderungen und Lösungsvorschlägen zur Sicherstellung der Beherrschbarkeit einer Service-orientierten Architektur und zur Nachvollziehbarkeit verantwortlichen Handelns innerhalb einer SOA ergeben sich schließlich zukünftige Aufgaben für Forschung und Entwicklung zur Nutzung des Innovationspotentials einer beherrschbaren SOA.

1.4 Aufbau der Analyse

Die Analyse entwickelt zunächst einen rechtlichen und technischen Rahmen zur Ableitung von Kriterien für eine strukturierte Beschreibung konkreter Anwendungsszenarien. Typische technische Kriterien sind Identifier, Absender- und Empfangsadressen und Datenflussabläufe in den Kommunikationsdaten in einem Service-Szenario. Typische rechtliche Kriterien sind Herkunft, Personenbezug und Verwendungszweck von diesen Daten. Das Zusammenspiel der rechtlichen und technischen Kriterien soll Faktoren der Beherrschbarkeit und Möglichkeiten zur Stärkung der Verantwortlichkeit sichtbar machen. Diese kommen in einigen klar identifizierbaren Aufgabenbereichen zum Ausdruck, die durch etwas detailliertere Gestaltungsvorschläge mit Lösungsansätzen ausgeführt werden. Daraus ergibt sich weiterer Forschungsbedarf zur Nutzung des Innovationspotentials einer beherrschbaren SOA.

Im Einzelnen ist die Analyse wie folgt aufgebaut:

In Kapitel 2 wird der juristische Rahmen gesetzt. Nach einer Darstellung der rechtlichen Grundlagen für den Datenschutz und zum Schutz von Betriebs- und Geschäftsgeheimnissen werden weitere Rahmenbedingungen wie Kosten, Akzeptanz und Sicherheit von Diensten ausgeführt.

Kapitel 3 liefert den technischen Rahmen. Hier werden grundlegende Faktoren entwickelt, die geeignet sind, die Chancen der Beherrschbarkeit zu nutzen. Dies sind einerseits Mechanismen zur Abgabe von Zusicherungen, wie etwa Datenschutzpolicies, Service Level Agreements oder Dienstleistungsverträge, andererseits Mechanismen zur Protokollierung, und zwar sowohl von technischen Kommunikationsdaten wie Server-Logs, als auch über die Verläufe von Diensten. Zusicherungen bilden die Basis für Unterrichtungen, auch (aber nicht nur) im Sinne des Datenschutzes vor einer Diensterbringung. Protokolle bilden die Basis für Auskünfte, auch (aber nicht nur) im Sinne des Datenschutzes im Laufe einer Diensterbringung. Diese beiden Faktoren für Zusicherungen und zur Protokollierung sind untereinander zu verknüpfen, damit ein wichtiges Beherrschbarkeitsziel erreicht werden kann, nämlich gegebene Zusicherungen später per Auskunft zu erfahren und – darüber hinausgehend – rechtsverbindlich festzustellen. Die Verallgemeinerung von Beherrschbarkeitsfaktoren über den Datenschutz hinaus zu allgemeineren Sicherheits- und Qualitätsanforderungen ist dabei ein Ziel unserer Analyse zur Chancenauswertung von SOA.

In Kapitel 4 werden fünf verschiedene Anwendungsszenarien von SOA im Detail analysiert. Die Szenarien sind so konstruiert, dass sie eine gewisse Anwendungsbreite repräsentieren und dabei nicht nur Datenschutzaspekte, sondern auch den Schutz von Geschäfts- und Betriebsgeheimnissen ansprechen. Aus der Datenflussanalyse anhand der in Kapitel 2 und 3 entwickelten

rechtlichen und technischen Kriterien ergeben sich die Gestaltungsvorschläge in Kapitel 5. Die Gestaltungsvorschläge in Kapitel 5 werden in übersichtliche Aufgabenbereiche gegliedert, die durch insgesamt 33 detailliertere Gestaltungsvorschläge mit Lösungsansätzen untermauert werden.

Nach einer Zusammenfassung der Ergebnisse dieser Analyse werden dieser Forschungsbedarf und das Innovationspotential einer beherrschbaren SOA in Kapitel 6 ausgeführt.

Kapitel 2

Juristischer Rahmen

2.1 Rechtliche Grundlagen

Wie oben (siehe Abschnitt 1.2.2) schon ausführlich beschrieben worden ist, bezeichnet der Begriff SOA ein Architekturkonzept, welches sich an Geschäftsprozessen orientiert und die Verbindung verschiedener Systeme und Datenbestände mit Hilfe standardisierter Formate und Schnittstellen ermöglichen soll. Dabei werden eine Vielzahl grob-granulierter Services verwendet, um die unterschiedlichen Geschäftsprozesse flexibel abzubilden.

Bereits diese Definition von SOA zeigt, dass sich in diesem Kontext aufgrund der großen Anzahl an in Betracht kommenden Geschäftsprozessen und der zu ihrer Realisierung nötigen Services auch vielfältige rechtliche Fragestellungen ergeben können. Entscheidend wird hierbei stets der konkrete Zusammenhang sein, also die Frage, welche Dienste für welchen Anwendungszweck zum Einsatz kommen, wie diese im Einzelnen ausgestaltet sind und von wem sie angeboten werden. In dieser Untersuchung werden einige typische rechtliche Fragestellungen im Rahmen einer juristischen Analyse ausgewählter Szenarien dargestellt.

Die folgenden rechtlichen Strukturfragen werden bei der Implementierung einer SOA regelmäßig tangiert:

Zunächst stellen sich bei der Inanspruchnahme von (Web) Services vertrags- und haftungsrechtliche Fragen, so etwa nach dem einschlägigen Vertragstyp oder der Haftung für Schäden, die durch die Inanspruchnahme eines Services entstehen¹.

Sofern personenbezogene Daten – etwa von Kunden oder Mitarbeitern – erhoben, verarbeitet oder genutzt werden, sind zudem die jeweils einschlä-

¹Zu entsprechenden Fragestellungen bei der Inanspruchnahme von Web Services vgl. [Spi05]

gigen datenschutzrechtlichen Bestimmungen zu berücksichtigen². Eine der Kernfragen ist die nach der datenschutzrechtlichen Verantwortung in einem verteilten System der Datenverarbeitung. Schon jetzt sei kurz angemerkt, dass sich in diesem Zusammenhang nicht zuletzt die Frage stellt, ob und inwieweit die Einhaltung dieser Vorschriften mit Hilfe eines automatisierten Datenschutzmanagements sichergestellt werden kann.

Darüber hinaus geht es bei einem Einsatz von SOA in virtuellen Organisationen nicht nur um den Schutz personenbezogener Daten, sondern auch um die Wahrung von Betriebs- und Geschäftsgeheimnissen, die für ein Unternehmen oft von immenssem wirtschaftlichem Wert sind. Beide Schutzgüter weisen in Hinblick auf die strukturellen Fragen der Verantwortung für die Wahrung der erforderlichen Vertraulichkeit sowie der Gewährleistung der Datensicherheit Parallelen auf.

Im Rahmen dieser Untersuchung werden verschiedene Szenarien aus rechtlicher Sicht analysiert, wobei der Fokus auf dem Bereich des Datenschutzrechts liegen wird. Wo erforderlich und sinnvoll, wird auch der Schutz von Betriebs- und Geschäftsgeheimnissen thematisiert werden. Deshalb werden nachfolgend die Grundlagen dieser beiden rechtlichen Themenbereiche vorgestellt.

2.1.1 Datenschutzrecht

Nachfolgend werden die rechtlichen Grundlagen für eine Verarbeitung personenbezogener Daten vorgestellt. Dabei wird sowohl auf die Rechtslage auf Ebene der Europäischen Union als auch auf die einschlägigen Regelungen in der Bundesrepublik Deutschland eingegangen. Zudem werden die Chancen und Risiken benannt, die sich für den Datenschutz aus den typischen SOA-Charakteristika wie z. B. der Kapselung spezifischer Aufgaben ergeben. Vorab erfolgen allerdings zunächst einmal einige kurze Ausführungen zu dem Thema Datenschutz als Akzeptanz- und Wettbewerbsfaktor.

2.1.1.1 Datenschutz als Akzeptanz- und Wettbewerbsfaktor

Wie demoskopische Erkenntnisse zeigen, zählt Datenschutz sowohl in Deutschland als auch international zu den grundlegenden Akzeptanzkriterien, weshalb diese Thematik u. a. die Entwicklung des E-Commerce wesentlich mitbestimmt. Datenschutz als Akzeptanzfaktor³ ist damit auch im Kontext Service-orientierter Architekturen und insbesondere im Verhältnis Business to Consumer (B2C) von großer Bedeutung. Darüber hinaus muss aber auch

²Zum Thema Datenschutz bei Web-Services vgl. [Sch03a]

³Hierzu vgl. die Ausführungen in Abschnitt 2.2.2.

in Business to Business (B2B)-Verhältnissen die Compliance mit den datenschutzrechtlichen Anforderungen stets sichergestellt sein. Dies gilt zum einen, wenn der Geschäftsvorfall in der Verarbeitung personenbezogener Daten besteht, zum anderen aber auch für die Gewährleistung einer ausreichenden Datensicherheit für die informationellen Güter der Geschäftsbeziehung. Die Verletzung der rechtlichen und sicherheitstechnischen Vorgaben ist für die Unternehmen risikoträchtig: So kann das Bekanntwerden von Datenschutzmängeln zu massiven Imageschäden führen. Bei Datenschutzverstößen können im Übrigen auch Sanktionen der zuständigen Aufsichtsbehörde drohen⁴.

Eine Möglichkeit für Unternehmen, sich Datenschutz als Wettbewerbsvorteil nutzbar zu machen, besteht in der Zertifizierung von Produkten und Verfahren als konform zu den Anforderungen des Datenschutzrechts. So gibt es in Schleswig-Holstein seit mehreren Jahren eine solche Zertifizierungsmöglichkeit von IT-Produkten (sog. Datenschutz-Gütesiegel)⁵. Die Verleihung des Gütesiegels für die Produkte Microsoft Update Service 6.0 und Windows Server Update Service 2.0. sowie Windows Genuine Advantage (WGA) für Windows XP hat gezeigt, dass solche Zertifizierungsverfahren mittlerweile auch von international operierenden Unternehmen wie der Microsoft Corporation nachgefragt werden⁶. Des Weiteren ist im Juni 2007 das Projekt EuroPriSe⁷ (European Privacy Seal) gestartet worden, durch welches die Voraussetzungen für die Verleihung eines Europäischen Datenschutz-Gütesiegels geschaffen werden sollen.

Moderne Unternehmen identifizieren und steuern („managen“) ihre Risiken. Die Herausforderung besteht in einer effizienten Gestaltung der Aufbau- und Ablauforganisation, um möglichen Verletzungen des Datenschutzes vorzubeugen bzw. im Schadensfall unmittelbar handlungsfähig zu sein. Vor diesem Hintergrund gewinnt ein Datenschutz- und Sicherheitsmanagement, in dem die Zuständigkeiten, aber auch die für einen proaktiven Datenschutz erforderlichen Prozesse definiert sind, an Bedeutung: Datenschutz durch Pro-

⁴So kann die Aufsichtsbehörde bei Datenschutzverstößen beispielsweise ein Bußgeld in Höhe von bis zu 250.000 € verhängen (vgl. § 43 BDSG). Im Übrigen sind einige besonders schwere Verstöße nach § 44 BDSG sogar mit Strafe bewehrt.

⁵Nähere Informationen hierzu finden sich unter <https://www.datenschutzzentrum.de/guetesiegel/index.htm>. Im Übrigen werden in Schleswig-Holstein auf freiwilliger Basis auch Verfahren der Datenverarbeitung der Behörden auditert.

⁶Vgl. hierzu die entsprechenden Pressemitteilungen des Unabhängigen Landesentrums für Datenschutz Schleswig-Holstein vom 16.02.2007 und 03.09.2007, abrufbar unter <https://www.datenschutzzentrum.de/presse/>.

⁷Informationen hierzu finden sich unter <http://www.european-privacy-seal.eu/>

zessmanagement⁸. Die Anforderungen des Datenschutzes sind mit anderen Worten in die Prozesse der Daten verarbeitenden Stellen zu integrieren.

2.1.1.2 Rechtliches Rahmengerüst

Die einzelnen Services, die im Rahmen einer Service-orientierten Architektur gebündelt werden, können von unterschiedlichen Service Providern via Internet angeboten werden. Die Firmensitze dieser Provider können dabei quer über den Globus verteilt sein. Aus diesem Grunde stellen sich mit der SOA-Thematik immer auch Rechtsfragen des internationalen Datenverkehrs. Deshalb soll nachfolgend nicht nur die rechtliche Situation in Deutschland, sondern auch die Rechtslage auf Ebene der EU vorgestellt werden⁹.

Europäische Union Der Europäische Gerichtshof hat schon vor langem anerkannt, dass der Schutz personenbezogener Daten Grundrechtsqualität genießt. Mittlerweile ist ein Grundrecht auf Datenschutz auch ausdrücklich in Artikel 8 der Charta der Grundrechte der Europäischen Union vom 07. Dezember 2000 kodifiziert worden. Hiernach hat jede Person das Recht auf Schutz der sie betreffenden personenbezogenen Daten.

Einfachgesetzlich geben die EG-Datenschutzrichtlinie (EG-DatSchRL) 1995/46/EG und die EG-Datenschutzrichtlinie für elektronische Kommunikation (EKom-EG-DatSchRL) 2002/58/EG datenschutzrechtliche Mindeststandards vor. Sie gewährleisten EU-weit einen festgelegten datenschutzrechtlichen Standard, zumal die beiden Richtlinien von jedem der mittlerweile 27 Mitgliedsstaaten der Europäischen Union in innerstaatliches Recht umgesetzt worden sind.

Während die EG-Datenschutzrichtlinie allgemeine Vorschriften zum Schutz der Privatsphäre natürlicher Personen bei der Verarbeitung personenbezogener Daten enthält, strebt die Datenschutzrichtlinie für elektronische Kommunikation ein einheitliches Rechtsregime für alle Arten elektronischer Kommunikation an¹⁰. Sie regelt die Datenerhebung und -Verarbeitung

⁸Hierzu siehe [Biz07]. Datenschutz durch Prozessmanagement gehört zu den vier Säulen eines modernen Datenschutzes – bei den übrigen drei Säulen handelt es sich um Datenschutz durch Recht, Datenschutz durch Technik und Datenschutz durch Wettbewerb.

⁹Dargestellt wird dabei allerdings nicht das nationale Recht in anderen EU-Staaten, sondern lediglich die Mindestanforderungen, die durch die EU-Datenschutzrichtlinie und die EU-Datenschutzrichtlinie für elektronische Kommunikation festgelegt worden sind. Nicht behandelt werden kann im Rahmen dieser Untersuchung allerdings die geltende Rechtslage in – außerhalb der EU liegenden – Drittstaaten.

¹⁰Anders als das deutsche Recht differenziert sie daher auch nicht zwischen Telekommunikations- und Telemediendiensten.

der elektronischen Kommunikation unabhängig von der jeweils zugrunde liegenden Technologie. Die EKom-EG-DatSchRL ergänzt also die EU-Datenschutzrichtlinie als bereichsspezifische Regelung auf dem Gebiet der elektronischen Kommunikation, weshalb ihre Vorgaben auch im Zusammenhang mit Service-orientierten Architekturen zu berücksichtigen sind.

Deutschland In Deutschland hat das Bundesverfassungsgericht erstmals in seinem Volkszählungsurteil, durch das das deutsche Datenschutzrecht entscheidend geprägt worden ist, ein Grundrecht auf informationelle Selbstbestimmung anerkannt und dieses in seiner nachfolgenden Rechtsprechung immer wieder bestätigt¹¹. Es stellt eine spezielle Ausprägung des Allgemeinen Persönlichkeitsrechts dar und gibt dem jeweiligen Grundrechtsträger die Befugnis, grundsätzlich selbst über die Preisgabe und Verwendung seiner persönlichen Daten zu entscheiden. Mit diesem Grundrecht unvereinbar wäre dem Bundesverfassungsgericht zufolge eine Rechts- und Gesellschaftsordnung, in der die Bürger nicht mehr erkennen können, wer was wann und bei welcher Gelegenheit über sie weiß.

Auf einfachgesetzlicher Ebene richtet sich die Erhebung, Verarbeitung und Nutzung personenbezogener Daten durch private Stellen nach dem Bundesdatenschutzgesetz (BDSG). Die Bestimmungen des BDSG gelten allerdings nur, soweit nicht bereichsspezifische Gesetze speziellere Regelungen vorsehen. Diese gehen dann nämlich gem. § 1 Abs. 3 S. 1 BDSG den Vorschriften des Bundesdatenschutzgesetzes vor.

Service-orientierte Architekturen werden üblicherweise mit Hilfe von Web Services implementiert, wobei die jeweiligen Services unter Verwendung von Internetverbindungen realisiert werden. In diesem Kontext geben das Telekommunikationsgesetz (TKG) und das Telemediengesetz (TMG) spezialgesetzliche Regelungen vor. Insoweit muss also stets untersucht werden, welches der drei genannten Gesetze (TKG, TMG und BDSG) für die jeweils in Rede stehende Datenverarbeitung einschlägig ist.

Dies wird in Anlehnung an das OSI-Referenzmodell mit Hilfe eines Dreischichten-Modells bewerkstelligt¹². Hierbei wird zwischen einer Kommunikationsebene, einer Interaktionsebene und einer Inhaltsebene unterschieden: Die Kommunikationsebene betrifft den reinen Datentransport, auf entsprechende Dienste wie ISDN, DSL, E-Mail und Telefon ist das Telekommunikationsgesetz¹³ anwendbar. In Abgrenzung hierzu geht es auf der Interaktionsebe-

¹¹Urteil vom 15.12.1983: BVerfGE 65, 1 = NJW 1984, 419

¹²Einzelheiten hierzu finden sich bei Rost, Welches Gesetz gilt eigentlich?, abrufbar unter <https://www.datenschutzzentrum.de/systemdatenschutz/meldung/sm91.htm/>. Verwiesen sei außerdem auf die Ausführungen von Schleipfer in [Sch04].

¹³Der Gesetzestext des TKG kann unter http://bundesrecht.juris.de/tkg_2004/

ne um eine technisch-standardisierte Kommunikation zwischen Nutzer und Diensteanbieter, wie sie etwa beim Abrufen eines Webseitenangebots stattfindet. In solchen Fällen ist auf die Datenverarbeitung auf Server Client-Ebene das Telemediengesetz¹⁴ anwendbar, das am 1. März 2007 in Kraft getreten ist. Schließlich betrifft die Inhaltsebene die individuelle Kommunikation und damit Fragen, die sich im Online- wie im Offline-Bereich gleichermaßen stellen. Als Beispiel für eine solche individuelle Kommunikation ist die Datenverarbeitung zu nennen, die sich aus dem Ausfüllen eines Web-Formulars im E-Commerce-Kontext ergibt. In solchen Konstellationen sind die bereichsspezifischen Regelungen von TKG und TMG nicht anwendbar, sondern die für die jeweilige datenverarbeitende Stelle geltenden Rechtsregeln. Im Fall einer nichtöffentlichen Stelle sind also die Regelungen des Dritten Abschnitts des Bundesdatenschutzgesetzes (§§ 27 ff. BDSG) anwendbar¹⁵.

2.1.1.3 Grundprinzipien des Datenschutzrechts

Den genannten nationalen und EU-Regelwerken zum Datenschutz lassen sich verschiedene Grundprinzipien entnehmen, die das gesamte Datenschutzrecht prägen. Diese Grundprinzipien können als Leitlinien für eine datenschutzkonforme Implementierung von SOA fruchtbar gemacht werden und sollen deshalb nachfolgend kurz vorgestellt werden. Wegen des bereits erwähnten starken internationalen Bezugs des Themas Service-orientierte Architekturen sollen die verschiedenen Datenschutzgrundsätze nachfolgend aus den Bestimmungen der Datenschutzrichtlinien der Europäischen Union, durch die die EU-weit geltenden datenschutzrechtlichen Mindestanforderungen festgelegt werden, abgeleitet werden.

Personenbezug als Voraussetzung für die Anwendbarkeit der EG-DatSchRL Bevor die einzelnen Grundprinzipien des Datenschutzes vorgestellt werden, ist zunächst noch darauf hinzuweisen, dass die EU-Datenschutzrichtlinie – entsprechendes gilt für das BDSG – nach Artikel 3 EG-DatSchRL nur dann anwendbar ist, wenn eine Verwendung personenbezogener Daten in Rede steht. Was unter personenbezogenen Daten zu verstehen ist, wird in Artikel 2 lit. a der Richtlinie definiert: Personenbezogene Daten sind danach alle Informationen über eine bestimmte oder bestimmbare natürliche Person; als bestimmbar wird dabei eine Person angesehen, die direkt oder indirekt identifiziert werden kann.

abgerufen werden.

¹⁴Der Gesetzestext des TMG kann unter <http://www.gesetze-im-internet.de/tmg/> nachgelesen werden.

¹⁵Der Text des BDSG kann unter http://bundesrecht.juris.de/bdsg_1990/ abgerufen werden.

Dieser Definition lässt sich im Übrigen auch entnehmen, dass nur natürliche Personen von der EU-Datenschutzrichtlinie und dem Grundrecht auf Datenschutz des Artikels 8 der Grundrechte-Charta geschützt werden. Auf juristische Personen finden die einschlägigen Regelungen hingegen keine Anwendung. Gesetzlich geschützt werden dagegen u. a. Betriebs- und Geschäftsgeheimnisse von Unternehmen, worauf an anderer Stelle noch näher einzugehen sein wird¹⁶.

Für die Datenverarbeitung Verantwortlicher Wie der Name schon sagt, ist der für die Datenverarbeitung Verantwortliche – nachfolgend: Verantwortlicher – für die Verarbeitung personenbezogener Daten und damit für die Einhaltung der Vorschriften der EG-DatSchRL und sonstiger Datenschutzvorschriften verantwortlich. Von dem Verantwortlichen sind die betroffene Person, der Auftragsverarbeiter sowie Dritte zu unterscheiden.

Nach der Legaldefinition des Artikels 2 lit. d EG-DatSchRL ist Verantwortlicher die natürliche oder juristische Person, Behörde, Einrichtung oder jede andere Stelle, die allein oder gemeinsam mit anderen über die Zwecke und Mittel der Verarbeitung von personenbezogenen Daten entscheidet. In Abgrenzung hierzu bezeichnet der Begriff Auftragsverarbeiter nach Artikel 2 lit. e EG-DatSchRL eine Person oder Stelle, die personenbezogene Daten im Auftrag des für die Verarbeitung Verantwortlichen verwendet. Einzelheiten zur Auftragsverarbeitung regeln die Artikel 16 f. EG-DatSchRL.

Im Falle einer Auftragsdatenverarbeitung ist nicht der Auftragnehmer, sondern weiterhin der Auftraggeber für die Einhaltung der gesetzlichen Datenschutzbestimmungen verantwortlich. Den Auftraggeber trifft die Verpflichtung, den Auftragnehmer sorgfältig auszusuchen und sich von der Einhaltung der gesetzlichen Vorschriften zu überzeugen. Der Auftragnehmer muss hingegen die Datenverarbeitung nach den Weisungen des Auftraggebers sowie die Durchführung der erforderlichen technisch-organisatorischen Maßnahmen sicherstellen.

Werden vertraglich Aufgaben von einer rechtlichen Einheit auf eine andere übertragen und ist insoweit auch die Verarbeitung personenbezogener Daten betroffen, so stellt sich stets die Frage, ob eine Auftragsdatenverarbeitung oder eine sog. Funktionsübertragung vorliegt¹⁷. Dabei ist von einer Auftragsdatenverarbeitung auszugehen, wenn die Verarbeitung personenbezogener Daten das wesentliche Element der Aufgabenübertragung darstellt und der Auftragnehmer lediglich eine Hilfs- und Unterstützungsfunktion in-

¹⁶Siehe Abschnitt „Schutz von Betriebs- und Geschäftsgeheimnissen“ auf Seite 27.

¹⁷Zur Abgrenzung von Auftragsdatenverarbeitung und Funktionsübertragung (nach deutschem Recht) vgl. etwa [Sim06, § 11 Rn. 17 ff], [GS05, § 11 Rn. 6 ff.].

nehat. In Abgrenzung hierzu liegt eine Funktionsübertragung vor, wenn auch die der Datenverarbeitung zugrunde liegenden Aufgaben ganz oder teilweise übertragen werden. Ist dies der Fall, so wird die Stelle, an die die Aufgaben übertragen worden sind, zum Verantwortlichen i. S. d. EG-DatSchRL.

Dritter ist schließlich jede Person oder Stelle, die nicht für die Verarbeitung Verantwortlicher oder Auftragsverarbeiter – bzw. für diese tätig – ist und auch nicht selbst als natürliche Person von der Datenverarbeitung betroffen wird.

Zulässigkeit der Datenverarbeitung Personenbezogene Daten dürfen erhoben, verarbeitet und genutzt werden, wenn dies zulässig ist. Nach Artikel 7 EG-DatSchRL ist das nur dann der Fall, wenn eine der dort abschließenden Voraussetzungen erfüllt ist (sog. Verbot mit Erlaubnisvorbehalt). Bei der Inanspruchnahme von Services im Rahmen einer SOA ist also stets zu prüfen, ob eine wirksame Einwilligung der von einer Verarbeitung personenbezogener Daten betroffenen Person vorliegt oder eine Rechtsvorschrift die Datenverwendung erlaubt oder anordnet.

Nach Artikel 2 h) ist eine Einwilligung der betroffenen Person jede Willensbekundung, die ohne Zwang für den konkreten Fall und in Kenntnis der Sachlage erfolgt und mit der die betroffene Person akzeptiert, dass personenbezogene Daten, die sie betreffen, verarbeitet werden. Als Rechtsgrundlage für eine Datenverarbeitung genügt also nicht jede beliebige, sondern nur eine informierte und freiwillige Einwilligung. Außerdem muss die Einwilligung ohne jeden Zweifel vorliegen, d. h. Voraussetzung für die Bejahung des Vorliegens einer Einwilligung ist eine eindeutige und bewusste Handlung der betroffenen Person. Nach Erwägungsgrund 17 der EKom-EG-DatSchRL kann eine Einwilligung im Bereich der elektronischen Kommunikation etwa auch durch das Markieren eines Feldes auf einer Internet-Website erteilt werden¹⁸.

Nachfolgend seien noch zwei Beispiele für Erlaubnisnormen der EU-Datenschutzrichtlinie, die eine Verarbeitung personenbezogener Daten legitimieren, genannt¹⁹:

Gemäß Artikel 7 lit. b EG-DatSchRL ist die Verarbeitung personenbezogener Daten zulässig, wenn sie für die Erfüllung eines Vertrags, dessen Vertragspartei die betroffene Person ist, erforderlich ist. Gleiches gilt auch hinsichtlich der Durchführung vorvertraglicher Maßnahmen, die auf Antrag der betroffenen Person erfolgen.

Artikel 7 lit. f EG-DatSchRL hingegen erklärt die Verarbeitung personen-

¹⁸Vgl. im deutschen Recht die Möglichkeiten einer elektronischen Einwilligung gem. §§ 94 TKG, 13 Abs. 2 TMG.

¹⁹Entsprechende Vorschriften finden sich in § 28 Abs. 1 Satz Nr. 1 + 2 BDSG

bezogener Daten dann für zulässig, wenn die Verarbeitung zur Verwirklichung des berechtigten Interesses, das von dem für die Verarbeitung Verantwortlichen wahrgenommen wird, erforderlich ist²⁰. Dies gilt aber dann nicht, wenn das Interesse oder die Grundrechte und Grundfreiheiten der betroffenen Person überwiegen.

Spezialfall: Übermittlung personenbezogener Daten in Drittstaaten Ein spezielles Zulässigkeitsproblem stellt die Übermittlung personenbezogener Daten in Drittstaaten, welche außerhalb der Europäischen Union (EU) und des Europäischen Wirtschaftsraums (EWR) liegen, dar. Diese Problematik ist insbesondere im Internetumfeld und damit oftmals auch im Zusammenhang mit unternehmensübergreifenden Service-orientierten Architekturen von großer Bedeutung. Artikel 25 f. EG-DatSchRL regeln, wann eine solche Übermittlung von Daten in einen Drittstaat zulässig ist.

Eine Übermittlung personenbezogener Daten in Drittstaaten setzt zunächst voraus, dass eine der Voraussetzungen des Artikels 7 EG-DatSchRL (Einwilligung oder Erlaubnisnorm) gegeben ist. Weitere Voraussetzung für eine zulässige Übermittlung ist aber außerdem, dass das jeweilige Drittland ein angemessenes Schutzniveau gewährleistet.

Dabei ist die Angemessenheit des Schutzniveaus, das ein Drittland bietet, unter Berücksichtigung aller Umstände zu beurteilen, die bei einer Datenübermittlung oder einer Kategorie von Datenübermittlungen eine Rolle spielen. Artikel 26 EG-DatSchRL sieht bestimmte Ausnahmefälle vor, in denen personenbezogene Daten auch in sog. unsichere Drittländer übermittelt werden dürfen – dies ist dann der Fall, wenn aufgrund anderer Umstände die Wahrung angemessener Datenschutzstandards sichergestellt ist.

Eine Übermittlung von Daten in Drittstaaten ist im Ergebnis insbesondere dann zulässig, wenn

- die EU-Kommission für das jeweils in Rede stehende Land das Bestehen eines angemessenen Schutzniveaus anerkannt hat,
- Daten an US-amerikanische Unternehmen übermittelt werden, die dem sog. Safe Harbor²¹-Abkommen zwischen der Europäischen Union und den Vereinigten Staaten von Amerika beigetreten sind,
- das Unternehmen, an das die Daten übermittelt werden, bindende Unternehmensregeln zum Datenschutz umgesetzt hat (sog. binding corporate rules),

²⁰Gleiches gilt für die Verwirklichung berechtigter Interessen, die von Dritten, denen die Daten übermittelt werden, wahrgenommen werden.

²¹<http://www.export.gov/safeharbor/>

- für die jeweilige Übermittlung oder für eine bestimmte Art von Übermittlungen die Geltung spezieller, von der EU-Kommission genehmigter Standardvertragsklauseln vereinbart worden ist oder
- der Betroffene in die Übermittlung der Daten eingewilligt hat.

Grundsatz der Erforderlichkeit Ein weiterer fundamentaler Grundsatz des Datenschutzrechts ist der der Erforderlichkeit der Datenverarbeitung. Hiernach müssen Art und Umfang der personenbezogenen Daten geeignet und notwendig sein, um den jeweiligen Zweck der Datenverarbeitung zu erfüllen. Es dürfen also nur solche personenbezogenen Daten verarbeitet werden, die tatsächlich benötigt werden. Das Erforderlichkeitsprinzip lässt sich auf Ebene des EU-Rechts insbesondere aus Artikel 6 Absatz 1 lit. c („dafür erheblich sind und nicht darüber hinausgehen“) und Artikel 7 b) - f) EG-DatSchRL (jeweils „erforderlich“) ableiten.

Der Erforderlichkeitsgrundsatz beinhaltet auch, dass die jeweils einschlägigen Lösungsfristen eingehalten werden. Nicht mehr benötigte Daten sind nach Artikel 6 e) EG-DatSchRL unverzüglich zu löschen. Dem korrespondiert ein Anspruch des Betroffenen auf Löschung solcher Daten gemäß Artikel 12 lit. b EG-DatSchRL. Die Löschung ist Dritten, denen die Daten übermittelt worden sind, nach Artikel 12 lit. c EG-DatSchRL mitzuteilen, sofern sich dies nicht als unmöglich erweist oder kein unverhältnismäßiger Aufwand damit verbunden ist. Keiner Frist unterliegt im Übrigen die Aufbewahrung von Daten, die anonymisiert worden sind.

Grundsatz der Datenvermeidung und -sparsamkeit Konkretisiert wird das Erforderlichkeitsprinzip durch den Grundsatz der Datenvermeidung und -sparsamkeit²². Hiernach haben sich Gestaltung und Auswahl von Datenverarbeitungssystemen an dem Ziel auszurichten, keine oder so wenig personenbezogene Daten wie möglich zu erheben, zu verarbeiten oder zu nutzen. Dabei ist insbesondere von den Möglichkeiten der Anonymisierung und Pseudonymisierung Gebrauch zu machen. Dieser Grundsatz kann Erwägungsgrund 9 EKom-EG-DatSchRL entnommen werden, wonach als Ziele bei der Weiterentwicklung von Technologien insbesondere die Beschränkung der Verarbeitung personenbezogener Daten auf das erforderliche Mindestmaß und die Verwendung anonymer oder pseudonymer Daten zu berücksichtigen sind. Außerdem lässt sich der genannte Grundsatz auch aus einer Gesamtschau der in Artikel 6 und 7 EG-DatSchRL niedergelegten Grundsätze ableiten.

²²Dieser findet sich im deutschen Recht in § 3a BDSG.

Zweckbindungsgrundsatz In engem Zusammenhang mit dem Grundsatz der Erforderlichkeit steht der sog. Zweckbindungsgrundsatz, welcher sich aus Artikel 6 Absatz 1 lit. b und c ableiten lässt. Hiernach dürfen Daten nur zu vorher konkret festgelegten eindeutigen und rechtmäßigen Zwecken erhoben, verarbeitet oder genutzt werden. Die EG-DatSchRL schließt eine nachträgliche Änderung der Zweckbestimmung nicht aus, lässt eine solche aber nur dann zu, wenn sie mit der ursprünglichen Zweckbestimmung vereinbar ist. Darüber hinaus setzt eine zulässige Zweckänderung immer auch eine dem neuen Zweck entsprechende Rechtsgrundlage voraus. Schließlich ist zu beachten, dass Zweckänderungen stets auch erneute Informationspflichten auslösen.

Transparenzgrundsatz Natürliche Personen können ihr Grundrecht auf Datenschutz nur dann sinnvoll ausüben, wenn sie darüber informiert sind, welche Erhebungen, Verarbeitungen oder Nutzungen ihrer personenbezogenen Daten geplant sind bzw. gerade stattfinden. Der Transparenzgrundsatz legt das hierfür erforderliche Wissensfundament und kann insbesondere aus Artikel 10 f. EG-DatSchRL abgeleitet werden.

Damit das notwendige Maß an Transparenz gewährleistet ist, sollen personenbezogene Daten im Regelfall direkt bei der betroffenen Person erhoben werden (Grundsatz der Direkterhebung)²³.

Darüber hinaus treffen den für die Verarbeitung Verantwortlichen vielfältige Unterrichts-, Benachrichtigungs- und Informationspflichten. Werden beispielsweise personenbezogene Daten bei der betroffenen Person erhoben, so ist diese nach Artikel 10 EG-DatSchRL insbesondere über die Identität der verantwortlichen Stelle, die Zweckbestimmungen der Erhebung, Verarbeitung oder Nutzung und die Empfänger oder Kategorien von Empfängern zu unterrichten.

Diese Unterrichts- und Informationspflichten werden um einen Auskunftsanspruch der betroffenen Person ergänzt. Nach Artikel 12 lit. a EG-DatSchRL²⁴ hat diese das Recht, von dem für die Verarbeitung Verantwortlichen zumindest Informationen über die Zweckbestimmungen der jeweiligen Datenverarbeitung, die Kategorien der Daten, die verarbeitet werden, und die Empfänger oder Kategorien der Empfänger, an die die Daten übermittelt werden, zu erhalten.

Qualität der Daten Nach Artikel 6 Absatz 1 lit. d EG-DatSchRL muss gewährleistet sein, dass personenbezogene Daten sachlich richtig sind. Wenn

²³Dieser Grundsatz findet sich im deutschen Recht in § 4 Abs. 2 BDSG.

²⁴Im deutschen Recht ist der Auskunftsanspruch in § 34 BDSG geregelt.

nötig, müssen die Daten also auf den neuesten Stand gebracht werden. Der für die Verarbeitung Verantwortliche muss folglich die inhaltliche Korrektheit der jeweils in Rede stehenden Daten sicherstellen.

Auch hier korrespondiert zur Verpflichtung des für die Verarbeitung Verantwortlichen wieder ein Anspruch der betroffenen Person: Diese hat gemäß Artikel 12 lit. b bzw. c EG-DatSchRL²⁵ ein Recht auf Berichtigung von Daten, die unvollständig oder unrichtig sind, sowie darauf, dass Dritten, denen die Daten übermittelt worden sind, die Berichtigung dieser Daten mitgeteilt wird.

Sicherheit der Daten Die Sicherheit personenbezogener Daten ist nur dann gewährleistet, wenn ein dem jeweiligen Risiko angemessenes Maß an IT-Sicherheit sichergestellt ist. Nach Artikel 17 Absatz 1 EG-DatSchRL²⁶ muss der für die Verarbeitung Verantwortliche die geeigneten technischen und organisatorischen Maßnahmen durchführen, die für einen Schutz der Daten vor Zerstörung, Verlust, unberechtigter Änderung, Weitergabe oder Zugang sowie jede weitere Form der unrechtmäßigen Verarbeitung erforderlich sind. Dies gilt insbesondere dann, wenn im Rahmen der Verarbeitung Daten in einem Netz übertragen werden, so wie dies im SOA-Kontext der Fall ist.

Die technischen und organisatorischen Maßnahmen müssen unter Berücksichtigung des Standes der Technik und der bei ihrer Durchführung entstehenden Kosten ein Schutzniveau gewährleisten, das den von der Verarbeitung ausgehenden Risiken und der Art der zu schützenden Daten angemessen ist. Der für die Verarbeitung Verantwortliche muss sich also am jeweiligen „state of the art“ der IT-Entwicklung orientieren, um ein angemessenes Maß an Datensicherheit sicherstellen zu können.

Konkret gehören zu den zu ergreifenden technischen und organisatorischen Maßnahmen etwa die Verwendung sicherer Verschlüsselungsmechanismen bei der Übermittlung personenbezogener Daten und ihre sichere, gegen Zugriffe unbefugter Dritter geschützte Verwahrung. Zu den zentralen technisch-organisatorischen Maßnahmen der Datensicherheit gehört außerdem die (teilweise) Protokollierung der Gestaltung eines IT-Systems durch die Administratoren und der Verarbeitung personenbezogener Daten durch die jeweiligen Nutzer des Systems.

Betroffenenrechte An dieser Stelle sollen die verschiedenen Betroffenenrechte noch einmal in ihrer Gesamtheit dargestellt werden²⁷:

²⁵§ 35 Abs. 1 BDSG

²⁶Im deutschen Recht ist § 9 BDSG nebst Anlage einschlägig.

²⁷Vgl. im deutschen Recht § 34 f. BDSG

Nach Artikel 12 lit. a EG-DatSchRL hat die betroffene Person einen Anspruch auf Auskunft über Verarbeitungen sie betreffender Daten. Diesen Anspruch muss sie frei und ungehindert in angemessenen Abständen sowie ohne unzumutbare Verzögerung oder übermäßige Kosten geltend machen können.

Gemäß Artikel 12 lit. b EG-DatSchRL kann die betroffene Person außerdem die Berichtigung, Löschung oder Sperrung von Daten verlangen, deren Verarbeitung nicht bzw. nicht mehr den Bestimmungen der EG-DatSchRL entspricht. Jede Berichtigung, Löschung oder Sperrung von Daten ist anschließend allen dritten Personen mitzuteilen, denen die Daten übermittelt worden sind. Dies gilt nur dann nicht, wenn es sich als unmöglich erweist oder ein unverhältnismäßiger Aufwand damit verbunden ist.

Schließlich erkennt Artikel 14 EG-DatSchRL der betroffenen Person noch ein Widerspruchsrecht zu. Danach kann in bestimmten Fällen Widerspruch gegen die jeweilige Datenverarbeitung eingelegt werden.

2.1.1.4 SOA & Datenschutz: Chancen und Risiken

Service-orientierte Architekturen als ein Architekturkonzept können durch verschiedene Technologien und in völlig unterschiedlichen Kontexten realisiert werden. Der Begriff SOA kann deshalb realiter in ganz unterschiedlicher Art und Weise mit Leben gefüllt werden.

Dennoch lassen sich aus einigen typischen SOA-Charakteristika wie der Kapselung spezifischer Aufgaben, der – unternehmensübergreifenden – losen Koppelung unterschiedlicher Services sowie der Verwendung deklarativer, maschinell verarbeitbarer Verträge Chancen und Risiken ableiten, die bei nahezu jeder Implementierung einer SOA von Belang sein dürften.

Chancen für den Datenschutz Die Implementierung einer SOA bietet zunächst eine Vielzahl von Chancen für die Realisierung eines hohen Datenschutzstandards. Im Einzelnen lassen sich vor allem Möglichkeiten für eine – automatisierte – Sicherstellung von Transparenz, Zweckbindung und Datenqualität identifizieren. Gleiches gilt für eine konsequente Realisierung des Grundsatzes der Datenvermeidung und -sparsamkeit. Insgesamt bietet das Thema SOA gute Voraussetzungen für das Design und die Etablierung eines automatisierten Datenschutzmanagements.

1. Chancen für mehr Transparenz

Prämisse für die Implementierung einer SOA ist die Standardisierung von Formaten und Schnittstellen. Hierfür sind eine Dokumentation von Formaten, Protokollen etc. und eine Kommunikation der Beteiligten über diese Themen erforderlich. Diese – organisationsübergreifende –

Kommunikation und Dokumentation bietet die Gelegenheit dazu, Datenbestände und Datenflüsse transparent(er) zu machen.

Weiterhin führt die oftmals über Unternehmensgrenzen hinweg erfolgende Verschränkung von Workflows zu einer erhöhten Abhängigkeit der Beteiligten. Diese erhöhte Abhängigkeit erzeugt ihrerseits wiederum ein starkes Bedürfnis nach Prüfbarkeit fremder und nach Nachweisbarkeit des Funktionierens und der Compliance eigener Prozesse. Prüfbarkeit und Nachweisbarkeit können durch eine automatisierte, beweissichere, kostengünstige und missbrauchssichere Protokollierung der Prozesse realisiert werden. Hierdurch würde gleichzeitig ebenfalls zu einer größeren – nachträglichen – Transparenz beigetragen.

2. Chancen für die Sicherstellung von Zweckbindung

Im Rahmen einer SOA werden zur Umsetzung von Geschäftsprozessen spezifische Aufgaben gekapselt. Jeder Service dient einem bestimmten, relativ eng umrissenen Zweck (Authentifizierung, Payment etc.). Dabei ist jeder Service bzw. Service Provider für „seine“ Daten verantwortlich – ein Service Consumer hingegen muss sein Interesse am Service und den jeweiligen Daten beim Service Provider anmelden. Der eng zweckgebundene Zuschnitt von Services und Verantwortlichkeiten schafft – im Zusammenhang mit datenschutzverträglichen Protokollierungstechniken – gute Voraussetzungen für eine automatisierte Überprüfung der Beachtung des Zweckbindungsgrundsatzes. Er legt es außerdem nahe, auch darüber nachzudenken, ob und inwieweit sich über eine automatisierte Überprüfung hinaus auch eine automatisierte Durchsetzung der Beachtung des Zweckbindungsgrundsatzes realisieren lässt²⁸.

3. Chancen hinsichtlich Datenvermeidung und -sparsamkeit

Der soeben geschilderte eng zweckgebundene Zuschnitt von Services erlaubt es, schon im Vorfeld der Implementierung einer SOA einfach feststellen zu können, welche – personenbezogenen – Daten zur Realisierung eines jeden Services tatsächlich benötigt werden. Bei der Implementierung der einzelnen Services kann dies dann gleich mit berücksichtigt werden.

Hierdurch wäre dann also sichergestellt, dass nur die Daten für die Realisierung des Services verwendet werden, die auch tatsächlich hierfür benötigt werden. Im SOA-Kontext bietet sich demnach also eine

²⁸Mehr zu den Möglichkeiten eines automatisierten Datenschutzmanagements im Abschnitt „Chancen für ein automatisiertes Datenschutzmanagement“ auf Seite 25

einfach zu realisierende Möglichkeit, dem Grundsatz der Datenvermeidung und -sparsamkeit zu genügen. Soweit dies im jeweiligen Kontext in Betracht kommt, kann das Maß an Datenvermeidung und -sparsamkeit außerdem z. B. noch durch die Verwendung anonymer Credentials erhöht werden²⁹.

4. Chancen für eine höhere Datenqualität

Die Orientierung an SOA legt nicht nahe, große Datenbestände, aus denen die verschiedenen Funktionalitäten bedient werden, zentral zu halten, sondern sie gebietet vielmehr eine dezentrale Datenhaltung. Solche zweckmäßig eng zugeschnittenen, dezentralen Datenbestände würden so nah wie möglich an der jeweiligen Datenquelle liegen. Hierdurch würde eine möglichst große Aktualität, Verlässlichkeit und Richtigkeit der Daten und damit ein hohes Maß an Datenqualität gewährleistet.

5. Chancen für ein automatisiertes Datenschutzmanagement

Die technische Integration von SOA erfolgt typischerweise auf der Basis von Web Services und XML. Bisher existierende Standards für ein automatisiertes Datenschutzmanagement basieren ebenfalls auf XML und könnten deshalb auch innerhalb einer SOA problemlos zum Einsatz kommen. Darüber hinaus ist mit WS-Privacy für Web Services bereits eine datenschutzspezifische Erweiterung des Standards WS-Security angedacht worden.

Folglich bietet sich im SOA-Kontext die Chance für ein Design und für eine Etablierung eines automatisierten Datenschutzmanagements. Im Fokus stehen hierbei die Themen Generierung maschinenlesbarer – rechtskonformer – Privacy Policies, automatisiertes Aushandeln sowie Prüfbarkeit der Einhaltung solcher Policies und automatisierte Durchsetzung von Datenschutz-Policies.

Es erscheint als möglich, diese Ziele z. B. mit Hilfe der folgenden Bausteine realisieren zu können: Lösungsansätze für eine revisionssichere Protokollierung, Digital Rights Management (DRM) und Trusted Computing.

Im Einzelnen könnten etwa die folgenden Standards eingesetzt werden:

- Platform for Privacy Preferences (P3P1.1),
- Enterprise Privacy Authorisation Language (EPAL1.1),

²⁹Hierbei handelt es sich um digitale Beglaubigungen, die für einen datenschutzfreundlichen Nachweis von Eigenschaften im Internet verwendet werden können.

- Extensible Access Control Markup Language (XACML2.0),
- Open Digital Rights Language (ODRL) und
- Web Services Privacy als Erweiterung des Standards Web Services Security (WSS1.1).

Risiken für den Datenschutz Die Implementierung einer SOA bietet aber nicht nur Chancen zur Realisierung eines hohen Datenschutzstandards, sondern birgt auch Risiken für die informationelle Selbstbestimmung von Personen, die von einer Datenverarbeitung betroffen sind.

1. Risiko von Intransparenz bei vielen verschiedenen Diensteanbietern

Wie bereits ausgeführt, bietet die Implementierung einer SOA Chancen für eine Erhöhung der Transparenz der Datenverarbeitung – um einen Automatismus handelt es sich hierbei allerdings nicht. Vielmehr kann gerade bei einer Beteiligung vieler verschiedener Anbieter von Services auch leicht ein so hohes Maß an Komplexität bei der Verarbeitung personenbezogener Daten erreicht werden, dass die betroffenen Personen nicht mehr überblicken können, wer welche Daten über sie verarbeitet.

2. Einfache Verkettbarkeit zuvor separierter Datenbestände

SOA ermöglicht die Verbindung verschiedener Systeme und Datenbestände durch die Verwendung standardisierter Formate und Schnittstellen. Hierdurch wird prinzipiell ein einfacher Zugriff auf zuvor separierte Datenbestände möglich. Von besonderer Bedeutung ist dieser Umstand bei virtuellen Organisationen, wo Datenbestände unterschiedlicher Unternehmen, Behörden und weiterer Organisationen leicht miteinander verkettet und zu umfangreichen Profilen über die betroffenen Personen verdichtet werden können.

Da zunächst einmal keine effektiven Kontrollmöglichkeiten der – internen – Verwendung von Daten vorhanden sind, kann die Implementierung einer SOA ein erhöhtes Risiko einer rechtswidrigen Verwendung von Daten zu unzulässig erweiterten bzw. neuen Zwecken mit sich bringen.

3. Integrierung vieler verschiedener Services in einem Meta-Service

Zwar ist für Service-orientierte Architekturen die Kapselung bestimmter Funktionalitäten in Services und ein eng zweckgebundener Zuschnitt der einzelnen Services charakteristisch, jedoch könnte ein Service Provider auf die Idee kommen, viele verschiedene Services in einen Meta-Service zu integrieren.

Ein solcher Service Provider würde also als Service Consumer viele Datenquellen von anderen Services zusammenfassen und dann anderen Service Consumern zur Verfügung stellen. Je mehr Services in einem solchen Falle integriert würden, umso mehr personenbezogene Daten würden durch den Meta-Service de facto zur Verfügung gestellt werden können. Letztlich besteht also auch insoweit wieder das Risiko einer Erstellung umfassender Profile der betroffenen Personen³⁰.

2.1.2 Schutz von Betriebs- und Geschäftsgeheimnissen

Im SOA-Kontext werden Workflows und die diese abbildenden IT-Prozesse vielfach unternehmensübergreifend verschränkt. Dies bringt nicht nur Risiken für das informationelle Selbstbestimmungsrecht der von Datenverarbeitungen betroffenen Personen mit sich, sondern birgt auch neue Möglichkeiten der Betriebsspionage³¹. Die enge Verschränkung der IT-Prozesse und die Verwendung gemeinsamer Standards und Formate dürfte es nämlich in vielen Fällen erleichtern, auf Betriebs- und Geschäftsgeheimnisse zuzugreifen. Auch mag es im Einzelfall gewollt sein, diese Geheimnisse mit bestimmten anderen Unternehmen oder Personen zu teilen, allerdings wird dann regelmäßig nicht erwünscht sein, dass auch Dritte hiervon Kenntnis erlangen.

Es wird also im Rahmen der Implementierung einer – unternehmensübergreifenden – SOA in vielen Fällen auch darum gehen, Betriebs- und Geschäftsgeheimnisse vor unbefugter Kenntnisnahme durch Dritte zu schützen. Deshalb soll nachfolgend skizziert werden, welche rechtlichen Rahmenbedingungen hinsichtlich des Schutzes von Betriebs- und Geschäftsgeheimnissen einschlägig sind.

2.1.2.1 Begriff der Betriebs- und Geschäftsgeheimnisse

Voraussetzung für ein Betriebs- und Geschäftsgeheimnis ist zunächst einmal, dass die jeweils betroffene Tatsache im Zusammenhang mit einem Betrieb steht und nicht offenkundig, sondern nur einem eng begrenzten Personenkreis bekannt ist. Darüber hinaus muss der auf einem ausreichenden wirtschaftlichen Interesse beruhende und bekundete Wille des Betriebsinhabers dahin gehen, dass diese Tatsache geheim gehalten werden soll³².

³⁰Die Rechtmäßigkeit eines solchen Vorgehens müsste im Einzelfall natürlich überprüft werden, faktisch ergeben sich aber auch bei einer rechtmäßigen Vorgehensweise durch die Akkumulierung der Daten Risiken für den Datenschutz, da diese eine missbräuchliche Verwendung erst ermöglichen oder zumindest vereinfachen kann.

³¹Durch Betriebsspionage erwachsen Schätzungen zufolge alleine Unternehmen in Deutschland jährlich Schäden in Höhe von mehreren Milliarden Euro [KH06].

³²Vom Bundesgerichtshof (BGH) verwendete Definition in BGH GRUR 2003, 356 (358) = NJW-RR 2003, 618.

Dabei betrifft ein Betriebsgeheimnis einen technischen Sachverhalt wie z. B. einen Konstruktionsplan, ein Geschäftsgeheimnis hingegen einen kaufmännischen Sachverhalt wie etwa eine Kundenkartei.

2.1.2.2 Internationales Recht: TRIPS-Abkommen

Das sog. TRIPS-Abkommen³³ (Agreement on Trade-Related Aspects of Intellectual Property Rights) ist eine internationale Vereinbarung auf dem Gebiet des Immaterialgüterrechts, welche Mindestanforderungen für nationale Rechtssysteme festlegt. Ziel des Abkommens ist es, sicherzustellen, dass die Maßnahmen und Verfahren zur Durchsetzung der Rechte des geistigen Eigentums nicht ihrerseits zu Schranken für den rechtmäßigen Handel werden. Auf internationaler Ebene sind alle EU-Mitgliedsstaaten wie auch die EU selbst an dieses Abkommen gebunden.

Im TRIPS-Abkommen werden Rechtsgebiete wie Urheberrecht, Markenrecht und Patentrecht geregelt, dabei wird von den Mitgliedsstaaten die Sicherstellung gewisser Mindeststandards verlangt. Artikel 39 enthält Regelungen zum Schutz nicht offenbarer Informationen, gibt also einen Mindestschutz von Betriebs- und Geschäftsgeheimnissen vor, der in allen Mitgliedsstaaten sichergestellt sein muss.

Innerhalb der Europäischen Union gehen die gesetzlichen Regelungen der einzelnen Mitgliedsstaaten zumeist deutlich über die Mindeststandards des TRIPS hinaus.

2.1.2.3 Rechtslage in Deutschland

Das deutsche Recht schützt Betriebs- und Geschäftsgeheimnisse sowohl durch strafrechtliche als auch durch zivilrechtliche Vorschriften.

Strafrechtlicher Schutz Strafrechtlichen Schutz erfahren Unternehmensgeheimnisse in Deutschland in erster Linie durch §§ 17 und 18 UWG.

Hinsichtlich einer möglichen Betriebsspionage im Zusammenhang mit einer Service-orientierten Architektur ist insoweit § 17 Absatz 2 Nr. 1 a) UWG einschlägig, wonach bestraft wird, wer sich ein Geschäfts- oder Betriebsgeheimnis durch Anwendung technischer Mittel unbefugt verschafft oder sichert. Der Betreffende muss dabei zu Zwecken des Wettbewerbs, aus Eigennutz, zugunsten eines Dritten oder in der Absicht, dem Inhaber des Unternehmens Schaden zuzufügen, handeln. Bestraft wird dieses Verhalten mit Freiheitsstrafe bis zu drei Jahren oder mit Geldstrafe, in besonders schweren

³³Der (Original)Text des Abkommens ist abrufbar unter http://www.wto.org/english/docs_e/legal_e/27-trips.pdf.

Fällen – etwa bei gewerbsmäßigem Handeln – mit Freiheitsstrafe bis zu fünf Jahren.

Der zweite für SOA relevante Fall, dass eine Person ihr anvertraute Betriebs- und Geschäftsgeheimnisse an Dritte weitergibt, wird von § 18 UWG geregelt. Danach macht sich strafbar, wer die ihm im geschäftlichen Verkehr anvertrauten Vorlagen oder Vorschriften technischer Art zu Zwecken des Wettbewerbs oder aus Eigennutz unbefugt verwertet oder jemandem mitteilt. Durch diese Vorschrift werden nicht alle Arten von Betriebs- und Geschäftsgeheimnissen, sondern nur Vorlagen oder Vorschriften technischer Art geschützt. Zu diesen gehören insbesondere Zeichnungen, Modelle, Schablonen, Schnitte und Rezepte. Bestraft wird das genannte Verhalten mit Freiheitsstrafe bis zu zwei Jahren oder mit Geldstrafe. Zu beachten ist noch, dass es sich bei dieser Vorschrift um ein sog. Antragsdelikt handelt, weshalb die Tat prinzipiell nur auf Antrag des geschädigten Unternehmens verfolgt wird³⁴.

Zivilrechtlicher Schutz Neben der strafrechtlichen Sanktionierung kann gegen Betriebsespionage und die unbefugte Verwertung oder Weitergabe von Unternehmensgeheimnissen auch zivilrechtlich vorgegangen werden. Einschlägig sind insoweit §§ 4 Nr. 11 UWG, 823I, II, 826 BGB sowie vertragsrechtliche Vorschriften.

Im Übrigen vereinbaren miteinander kooperierende Unternehmen in vielen Fällen vertragliche Geheimhaltungspflichten (sog. non-disclosure agreement), gegen deren Verletzung dann auf dem Zivilrechtswege vorgegangen werden kann.

2.2 Weitere Rahmenbedingungen

2.2.1 Kosten

Durch die Verarbeitung personenbezogener Daten entstehen einer Organisation Kosten, die sich aus der Erfüllung von Anforderungen des Datenschutzrechtes (aber auch durch Kundenanforderungen an den Datenschutz) ergeben. So muss bspw. für die Beantwortung von Auskunftersuchen geschultes Personal vorhanden sein. Eine frühzeitige Einbeziehung von Anforderungen bereits in die Architekturgestaltung kann hier helfen Kosten zu sparen. Neben diesen unmittelbaren Einsparungen können sich weitere, sekundäre Ein-

³⁴Etwas anderes gilt aber dann, wenn die Strafverfolgungsbehörde wegen des besonderen öffentlichen Interesses an der Strafverfolgung ein Einschreiten von Amts wegen für geboten hält.

spareffekte ergeben. Eine systematische Analyse der Prozesse, die für eine datenschutzfreundliche Architektur erforderlich ist, kann gleichzeitig bei der Optimierung der Prozesse zu höherer wirtschaftlicher Effizienz dienen.

2.2.2 Akzeptanz

Akzeptanz bei der jeweiligen Klientel ist ein wesentliches Kriterium für den Erfolg oder Misserfolg einer Organisation. So ist ein hohes Maß an Akzeptanz bei (potentiellen) Kunden eine elementare Voraussetzung für die erfolgreiche Markteinführung neuer Produkte oder Dienstleistungen. Folglich haben Organisationen ein vitales Interesse an einer möglichst frühzeitigen Identifizierung der Akzeptanzfaktoren, die im jeweiligen Kontext von Bedeutung sind. Betrachtet man das IT-Umfeld, so sind als wichtige Akzeptanzfaktoren für neue Produkte, Dienstleistungen oder Technologien u. a. deren Leistungsmerkmale, Stabilität, Benutzerfreundlichkeit und (wirtschaftlicher) Nutzen zu nennen.

Darüber hinaus zeigen die Ergebnisse valider demoskopischer Umfragen, dass es sich auch beim Datenschutz um einen bedeutenden Akzeptanzfaktor handelt [Sch03b]. Dieser kann gerade im Bereich des eCommerce einen wesentlichen Einfluss auf das Kaufverhalten (potentieller) Kunden ausüben: Für mehr als die Hälfte (52 %) der 2006 in Deutschland im Rahmen einer Europäischen Umfrage³⁵ zur Nutzung von Informations- und Kommunikationstechnologien befragten Internetnutzer, die noch nie oder zumindest ein Jahr lang nicht online eingekauft haben³⁶, sind Sicherheits- und Datenschutzbedenken ein Grund für den Verzicht auf Online-Einkäufe. Des Weiteren wird dem Datenschutz auch zukünftig eine große Bedeutung beigemessen: Einer im Jahre 2005 von der Europäischen Kommission in Auftrag gegebenen Meinungsumfrage³⁷ zufolge sind gut zwei Drittel (67 %) der befragten EU-Bürger der Ansicht, dass der Schutz von privaten Informationen vor Missbrauch oder Ausnutzung für unsere Gesellschaft in zehn Jahren sehr wichtig sein wird.

³⁵Mohr, Sabine: Informations- und Kommunikationstechnologien in privaten Haushalten – Ergebnisse der Erhebung 2006 in: Statistisches Bundesamt, Wirtschaft und Statistik 6/2007, S. 545 (554), abrufbar unter <http://www.destatis.de/jetspeed/portal/cms/Sites/destatis/Internet/DE/Content/Publikationen/Querschnittsveroeffentlichungen/WirtschaftStatistik/Informationsgesellschaft/IKTPrivhaushalte0607,property=file.pdf>

³⁶Der Erhebung zufolge hatten 2006 ein Viertel aller Internetnutzer noch nie etwas online bestellt oder gekauft, weitere 7 % hatten dies zumindest während der letzten zwölf Monate nicht mehr getan.

³⁷Special EUROBAROMETER 225 – Social values, Science and Technology, Befragung im Auftrag der Europäischen Kommission, Juni 2005, S. 63 f., abrufbar unter http://ec.europa.eu/public_opinion/archives/ebs/ebs_225_report_en.pdf

2.2.3 Sicherheit

IT-Sicherheit umfasst die Robustheit der Informationstechnik gegen unerlaubte Manipulationen und Fehler, sowie den Schutz der Anwendungsumgebung gegen unerwünschte Effekte. Ersteres ist die Verlässlichkeit, letzteres die Beherrschbarkeit der Informationstechnik durch Menschen und Organisationen. Beherrschbarkeit und Verlässlichkeit sind dabei nicht voneinander unabhängig, sondern bedingen einander. Datenschutz ist ein besonderer Aspekt der Beherrschbarkeit, der bei der Konzeption und bei der Nutzung von IT zu beachten ist.

Beherrschbarkeit und Datenschutz sind nicht ohne weitergehende Sicherheitseigenschaften durchzusetzen. So ist ein System, das funktional korrekt gebaut ist, so lange verlässlich für die Anwendung, so lange es nicht gezielt angegriffen wird. Jeder unautorisierte Lauschangriff verletzt das Vertraulichkeitsgebot des Datenschutzes, und jede Löschung oder Verfälschung von Daten macht eine zuverlässige Auskunft, wie sie vom Datenschutz gefordert wird, zunichte. Darüber hinaus sind Systeme gegen Ausfälle, gegen Ressourcendiebstahl und gegen das Abstreiten verbindlicher Willenserklärungen (wie zum Beispiel Zusicherungen von Geschäftszielen und Zweckbindungen personenbezogener Daten) abzusichern.

Glücklicherweise helfen klassische Sicherungsmaßnahmen wie Verschlüsselung und Signatur auch zur Verwirklichung von Datenschutzzielen. Weiterhin können Zugriffskontrollmaßnahmen, wie sie für die IT-Sicherheit etabliert sind, elektronische Auskunfts-, Löschungs- und Berichtigungsersuchen absichern und dadurch zu einer datenschutzfreundlichen Ausgestaltung von Services im Netz beitragen. In diesem Sinne bildet Sicherheit nicht nur einen zusätzlichen Aufwand, der über den Datenschutz hinaus zu bewältigen wäre, sondern es ergeben sich auch synergetische Effekte zwischen diesen beiden Bereichen.

2.3 Festlegung von Prüfungsschritten für die datenschutzrechtliche Analyse der Szenarien

Die technische und rechtliche Bewertung verschiedener Szenarien bildet einen wesentlichen Bestandteil der SOAinVO-Analyse (siehe Kapitel 4). In diesem Kapitel sind die rechtlichen Grundlagen geschildert worden, die für das Verständnis der rechtlichen Analyse der Szenarien erforderlich sind. Auf diesen Grundlagen baut auch das nachfolgende Prüfungsschema auf, das zur

Erleichterung und Strukturierung der datenschutzrechtlichen Prüfung entwickelt worden ist. Die Szenarienanalyse wird primär am Maßstab des deutschen Rechts durchgeführt werden, weshalb auch das Prüfungsschema auf das deutsche Recht ausgerichtet ist. Das Schema wird im weiteren Verlauf dieses Abschnitts näher erläutert.

Prüfungsschritt 1 Analyse des Datenflusses: Szenarienbeschreibung

- Generelle Analyse des Datenflusses
- Eruierung besonderer Gefahren für die informationelle Selbstbestimmung

Prüfungsschritt 2 Anwendbarkeit der Datenschutzgesetze, Beteiligte

- Verwendete Daten
- Personenbezug dieser Daten
- Zweck der Datenverwendung
- Betroffener
- Verantwortliche Stelle (ggf. Abgrenzung Auftragsdatenverarbeitung - Funktionsübertragung)

Prüfungsschritt 3 Ermittlung des jeweils einschlägigen Gesetzes

- Anwendbarkeit deutschen Datenschutzrechts
- Einschlägigkeit bereichsspezifischer Gesetze
- 3-Schichten-Modell zur Abgrenzung von TKG, TMG, BDSG

Prüfungsschritt 4 Abarbeitung der rechtlichen Kriterien

- Zulässigkeit der Datenverwendung
- Spezialfall: Übermittlung in Drittstaaten
- Erforderlichkeit der Datenverwendung (inklusive Einhaltung der jeweils einschlägigen Lösungsfristen)
- Zweckbindungsgrundsatz
- Grundsatz der Datenvermeidung und Datensparsamkeit
- Transparenz (Grundsatz der Direkterhebung, Einhaltung von Unterrichtungs-, Benachrichtigungs- und Informationspflichten, Auskunftsanspruch des Betroffenen)

- Anforderungen an die Datensicherheit: Aktueller Stand der Technik

Prüfungsschritt 5 Ergebnisse

- Konsequenzen der in Prüfungsschritt 4 erzielten Ergebnisse
- Schlussfolgerungen im Hinblick auf die vier Beherrschbarkeitsfaktoren
 - Zusicherung
 - Unterrichtung
 - Protokollierung
 - Auskunft

2.3.1 Erläuterung des Prüfungsschemas

Prüfungsschritt 1, also die Analyse des Datenflusses, ist die notwendige Voraussetzung für den Eintritt in die juristische Prüfung. Ohne eine genaue Kenntnis der jeweiligen Datenflüsse kann eine fundierte rechtliche Analyse nicht durchgeführt werden. Informationen hierzu finden sich stets in einem separaten Abschnitt der jeweiligen Szenarienbeschreibung („Datenflüsse zwischen den Akteuren“).

In Prüfungsschritt 2 wird ermittelt, ob die jeweils verwendeten Daten einen Personenbezug aufweisen und folglich Datenschutzrecht (überhaupt) zur Anwendung kommt. Außerdem wird an dieser Stelle geprüft, zu welchem Zweck die Daten verwendet werden. Sofern personenbezogene Daten ausschließlich für persönliche oder familiäre Tätigkeiten verwendet werden, ist der Anwendungsbereich des Datenschutzrechts nämlich nicht eröffnet. Schließlich wird an dieser Stelle auch bereits geprüft, welche Betroffenen und welche verantwortlichen Stellen an dem jeweiligen Szenario beteiligt sind.

Prüfungsschritt 3 dient der Ermittlung des jeweils einschlägigen Gesetzes. Dabei geht es zunächst um die Frage, ob überhaupt deutsches Datenschutzrecht anwendbar ist. Sodann ist zu klären, ob bereichsspezifische Regelungen einschlägig sind oder ob die allgemeinen Datenschutzgesetze (insbesondere das Bundesdatenschutzgesetz - BDSG) zur Anwendung kommen. Speziell im Internetkontext ist anhand des sogenannten 3-Schichten-Modells die Abgrenzung zwischen Telekommunikationsgesetz (TKG), Telemediengesetz (TMG) und BDSG vorzunehmen.

Die eigentliche rechtliche Bewertung findet in Prüfungsschritt 4 statt, in dem zu prüfen ist, ob die jeweilige Datenverwendung durch eine wirksame Rechtsgrundlage legitimiert wird (Zulässigkeit der Datenverwendung). Des

Weiteren ist zu klären, ob die Datenverarbeitung die Grundsätze der Erforderlichkeit, der Zweckbindung, der Datenvermeidung und Datensparsamkeit sowie der Transparenz einhält. Schließlich ist zu untersuchen, ob die nach dem aktuellen Stand der Technik erforderlichen technischen und organisatorischen Maßnahmen von der verantwortlichen Stelle getroffen worden sind.

Im Prüfungsschritt 5 werden die Ergebnisse der rechtlichen Prüfung dargestellt. Es werden also – sofern vorhanden – Verstöße gegen die im vorherigen Prüfungsschritt untersuchten Kriterien und die hieraus folgenden Konsequenzen aufgezeigt. An dieser Stelle folgen insbesondere auch Ausführungen zu den vier Beherrschbarkeitsfaktoren Zusicherung, Unterrichtung, Protokollierung und Auskunft.

Die oben genannte Abfolge von Prüfungsschritten wird in der nachfolgenden rechtlichen Szenarienanalyse nur insoweit explizit dargestellt, als sie von besonderer Bedeutung für die Analyse ist. So werden etwa die vier Beherrschbarkeitsfaktoren Zusicherung, Unterrichtung, Protokollierung und Auskunft, die im nächsten Kapitel (Technischer Rahmen) ausführlich vorgestellt werden, eingehender rechtlich gewürdigt. Aufgrund ihrer zentralen Bedeutung für die Analyse von Service-orientierten Architekturen in virtuellen Organisationen werden diese Faktoren in jedem der zu analysierenden Szenarios genauer betrachtet. An dieser Stelle genügt es festzuhalten, dass mit den genannten Beherrschbarkeitsfaktoren aus rechtlicher Hinsicht insbesondere die folgenden Gesichtspunkte korrespondieren:

Der Zusicherung korrespondiert die Datenverwendung zu bestimmten Zwecken (Zweckbindung) und der Unterrichtung die Erfüllung von Unterrichtungs-, Benachrichtigungs- und Informationspflichten. Bei der Protokollierung stehen mehrere korrespondierende rechtliche Aspekte in Rede, nämlich insbesondere die Ermöglichung einer vollständigen Auskunftserteilung sowie die (datenschutzrechtlich relevante) Protokollierung personenbezogener Daten. Schließlich entspricht dem Beherrschbarkeitsfaktor Auskunft der Anspruch des Betroffenen auf Auskunft über die zu seiner Person gespeicherten Daten.

Kapitel 3

Technischer Rahmen

In diesem Kapitel werden die technischen Rahmenbedingungen erläutert, welche eine SOA determinieren. Grundlegend hierfür ist die Betrachtung der Entwicklung einer SOA im Rahmen des SOA-Lebenszyklus. Aus diesem Grund enthält der erste Abschnitt eine Darstellung des Spannungsfeldes wichtiger Einflussgrößen auf den Entwicklungsprozess einer SOA. Ausgehend von diesem grundlegenden Problembereich wird im zweiten Abschnitt die Beherrschbarkeit als Blickwinkel für weitere Betrachtungen identifiziert und durch das Ableiten einzelner Beherrschbarkeitsfaktoren operationalisiert. Die Abschnitte drei und vier enthalten detaillierte Analysen der einzelnen Beherrschbarkeitsfaktoren.

3.1 Einflussgrößen auf den Service-Lebenszyklus

Bei der Erstellung von Services und ihrem Betrieb innerhalb einer SOA werden, wie in Abbildung 3.1 schematisch dargestellt, unterschiedliche Ziele verfolgt. Zunächst sollen sie einzelne Dienstleistungen realisieren, die in ihrer Komposition dazu geeignet sind, ganze Geschäftsprozesse abzubilden – dies entspricht dem Einsatzzweck von Services im Rahmen einer SOA. Die Anforderungen der einzelnen Dienstleistungen bestimmen direkt alle Phasen des Service-Lebenszyklus, von der Entwicklungsphase, die sich aufgliedert in Analyse, Entwurf und Implementation, bis hin zur Produktivphase, die aus dem so genannten „Deployment“ (d.h. Einfügen eines Service in die Service-Landschaft) und dem anschließenden Betrieb des Service besteht.

Neben den Geschäftszielen werden auch durch den Datenschutz Anforderungen wie Datensparsamkeit, Zweckbindung und Transparenz an die Services gestellt, die nicht immer mit erstgenannten Zielen vereinbar sind, sich

jedoch ebenso auf den Lebenszyklus auswirken. Während aus Geschäftssicht nur die Dienstleistung wichtig ist, fordert der Datenschutz auch, dass die Services die Unterrichtung und Auskunftserteilung vom Unternehmen an den Kunden unterstützen¹; als Mittel hierzu werden über den gesamten Service-Lebenszyklus Zusicherungen sowie in der Produktivphase das Logging eingesetzt.

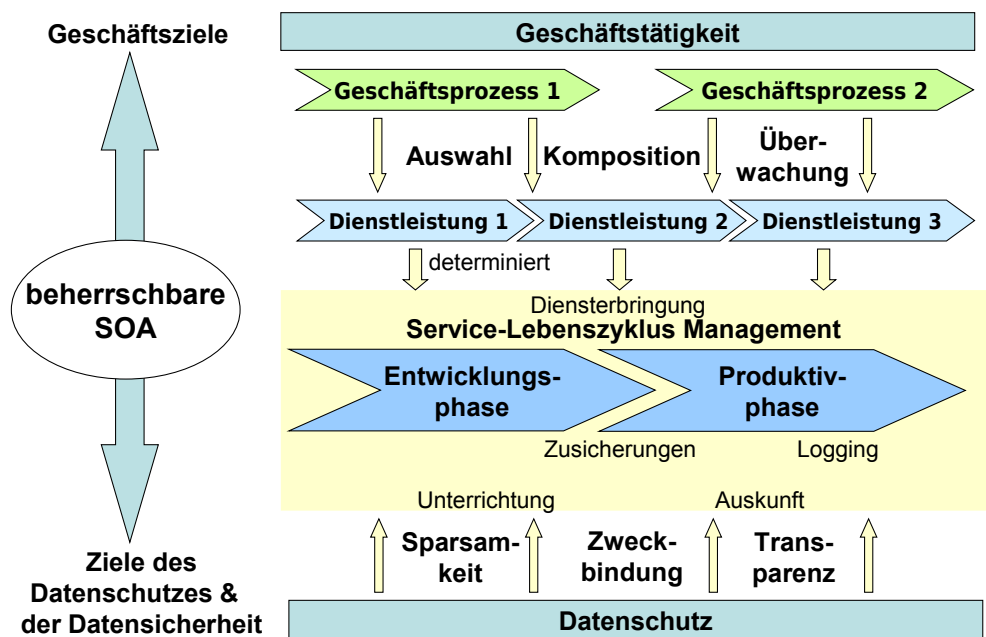


Abbildung 3.1: Service-Lebenszyklus

3.2 Beherrschbarkeit

Beherrschbarkeit der Datenverarbeitung ist ein Schlüsselkonzept für die Behandlung der sich in einer VO ergebenden Probleme. Beherrschbarkeit kann in diesem Kontext definiert werden als „Sachlage, bei der Rechte oder schutzwürdige Belange der Betroffenen durch das Vorhandensein oder die Nutzung von IT-Systemen nicht unzulässig beeinträchtigt werden“ [Die04]. Beherrschbarkeit wird von Funktionen zur verlässlichen Handhabe eines Systems unterstützt. Die Betroffenen können hierbei die Kunden der VO sein, deren personenbezogene Daten, und indirekt auch deren Datenschutzrechte in einem

¹Zu diesen Forderungen siehe auch Abschnitt 3.2.1.

beherrschbaren System geschützt sind. Darüber hinaus sind auch die Unternehmen einer VO Betroffene, da sie die Einhaltung der Datenschutzgesetze sicher stellen müssen. Im Folgenden wird nun dargestellt, wie die Betrachtung der Beherrschbarkeit helfen kann, die aus dem Datenschutzrecht für die VO entstehenden Probleme zu lösen.

3.2.1 Faktoren, die Beherrschbarkeit konstituieren

Zunächst ist zu beachten, dass sich der Schutz der personenbezogenen Daten aus dem „Recht auf informationelle Selbstbestimmung“² ableitet. Dieses Recht ist in den verschiedenen Gesetzen zum Datenschutz konkretisiert. Wesentliche Rechte und Pflichten, die dem Kunden ein Mittel der Beherrschbarkeit über seine Daten zugestehen, sind hierin das Recht des Kunden auf Auskunft und die Pflicht des Unternehmens zur Unterrichtung. Diese Rechte und Pflichten führen nun dazu, dass für die Unternehmen eine Notwendigkeit entsteht, geeignete organisatorische Maßnahmen und Schnittstellen zu implementieren, um Unterrichtung und Auskunft unter Verwendung einer SOA geben zu können. Hierfür ist es jedoch erforderlich, dass ein Unternehmen seine eigene Datenverarbeitung beherrscht. Grundlegende Mechanismen, die zur Erfüllung dieses Erfordernisses beitragen können, sind Protokollierung und Zusicherungen.

In den folgenden Abschnitten geben wir zunächst einen Überblick über die einzelnen Beherrschbarkeitsfaktoren und ihr Verhältnis zueinander.

3.2.1.1 Unterrichtung

Um natürliche Personen gesetzeskonform über die Erhebung ihrer personenbezogenen Daten zu unterrichten, ist eine Weitergabe von Informationen betreffend (i) die „Identität der verantwortlichen Stelle“, (ii) die „Zweckbestimmungen der Erhebung, Verarbeitung oder Nutzung“ der Daten, und (iii) unter Umständen die „Kategorien von Empfängern“ der Daten³ erforderlich. Die Unterrichtung von Kunden stellt für Unternehmen eine gesetzliche Verpflichtung dar, von der sie auch beim Zusammenschluss mehrerer einzelner Unternehmen zu einer VO nicht entbunden werden. In der Regel hat die Unterrichtung im Vorfeld der Datenerhebung zu erfolgen. Falls jedoch ein unterrichtungswürdiger Sachverhalt nach der Datenerhebung auftritt, besteht die Pflicht einer nachträglichen Benachrichtigung⁴. Die Relevanz der Unterrich-

²In Deutschland basiert dieses Recht auf einer Entscheidung des Bundesverfassungsgericht vom 15.12.1983; Az.: 1 BvR 209/83; NJW 84, 419.

³In Anlehnung an die Definition von Unterrichtung in § 4 Abs. 3 BDSG.

⁴vgl. § 33 Abs. 1 BDSG.

tung für die Beherrschbarkeit des Systems bzw. der SOA ergibt sich daraus, dass der Kunde nur auf Basis der Unterrichtung eine begründete Entscheidung treffen kann, ob er sein Recht auf informationelle Selbstbestimmung geschützt oder gefährdet sieht und ob er dementsprechend seine Daten preisgibt oder zurückhält.

Die Unterrichtung hat zwei Dimensionen: die rechtliche Dimension, die eine Beachtung der Unterrichtungspflicht durch Unternehmen verlangt, und die technische Dimension, welche die Implementierung von gesetzeskonformen Informationssystemen erfordert.

3.2.1.2 Auskunft

Das gesetzlich vorgeschriebene Recht auf Auskunft erlaubt es natürlichen Personen, von datenverarbeitenden Stellen, also insbesondere auch von Unternehmen, Informationen über ihre personenbezogenen Daten zu erhalten. Diese Informationen umfassen Angaben (i) zur Existenz, dem Inhalt und der Herkunft der Daten, (ii) zu den Empfängern und (iii) zum Zweck, dem die Datenspeicherung dient⁵. Im Gegensatz zur Unterrichtung muss die Auskunft vom Kunden aktiv eingeholt werden. Mit der Auskunft steht dem Kunden ein Beherrschbarkeitsinstrument zur Verfügung, da er zunächst Kenntnis seiner schutzwürdigen Belange benötigt, um eine Beeinträchtigung dieser Belange vermeiden zu können. So ist die Auskunft oft eine Voraussetzung des Kunden für die Inanspruchnahme weiterer Datenschutzrechte [Wei06]; sobald der Kunde Kenntnis über die Speicherung seiner personenbezogenen Daten besitzt, kann er deren Löschung, Sperrung oder Korrektur verlangen.

Ähnlich wie bei der Unterrichtung impliziert die rechtliche Dimension des Auskunftsanspruchs eine technische Dimension der Bereitstellung von Mitteln, dem Auskunftsanspruch entsprechen zu können.

3.2.1.3 Zusicherungen

Zusicherungen sind Mengen von verbindlichen Regeln für die Aktivitäten eines Unternehmens. Das Gegenstück zu Zusicherungen sind Präferenzen der Kunden, die Aktivitäten beschreiben, deren Ausführung die Kunden dem Unternehmen erlauben. Zusicherungen können generell für alle Geschäftstätigkeiten formuliert sein, oder für einzelne Verträge separat. Sie stellen ein geeignetes Mittel dar, um auf ihrer Basis die Unterrichtung des Kunden zu realisieren, wobei sie wesentlich präzisere als die vom Gesetz geforderten Angaben über die Datenverarbeitung im Unternehmen zulassen.

⁵In Anlehnung an die Definition von Unterrichtung in § 4 Abs. 3 BDSG.

Aus technischer Sicht haben Zusicherungen starke Ähnlichkeit mit Constraints, wie sie in der Softwaretechnik Anwendung finden. Hierin beschränken Constraints mögliche „Inhalte, Zustände oder die Semantik“ der Elemente [Oes04]. In den Datenschutz übertragen bedeutet eine Zusicherung somit einen verbindlichen Ausdruck über Möglichkeiten, die das Unternehmen zur Verarbeitung der personenbezogenen Daten besitzt bzw. nicht besitzt. So können Zusicherungen als Mittel angesehen werden, um a priori Beherrschbarkeit herzustellen, und somit die Gesetzeskonformität der Prozesse des Unternehmens zu gewährleisten. Bei der Formulierung von Zusicherungen sollte das Unternehmen jedoch sicher stellen, dass nur notwendige Informationen enthalten sind und keine Geschäftsgeheimnisse enthüllt werden.

3.2.1.4 Protokollierung

Die Aufgabe der Protokollierung, im Sinne der Erzeugung und des Befüllens von Log-Dateien, ist die Ermöglichung der nachträglichen Rekonstruktion von Verhalten (vgl. [KE05] für Protokollierung im Datenbankkontext). So bietet sich Protokollierung zur Nutzung in vielen Anwendungsgebieten an, etwa zur Unterstützung der Suche nach Fehlern in komplexen Informationssystemen, oder zur Sicherstellung der Konsistenz in Datenbanken. Im Gegensatz zu Zusicherungen eignet sich Protokollierung jedoch nur a posteriori als Hilfsmittel zur Gewährung von Beherrschbarkeit. Um ihrem Bestimmungszweck, der Rekonstruktion von Verhalten im Nachhinein, gerecht werden zu können, muss die Protokollierung das Aufzeichnen der Aktivitäten spezieller Einheiten zusammen mit der Zeit und ihrem Kontext umfassen.

Protokollierung ist für den Datenschutz aus mehreren Gründen zu betrachten. Zunächst können Protokolle ein geeignetes technisches Mittel sein, um die Auskunft zu erzeugen, die dem Anfragenden erteilt wird; anhand von Protokollen kann (detaillierter als vom Gesetz gefordert) genau festgehalten werden, welches personenbezogene Datum wann, wie und von wem verarbeitet wurde. So erlaubt das Protokoll als objektive Aufzeichnung die nachträgliche Rekonstruktion von Datenflüssen auch aus unvorhergesehenen Perspektiven. Zusätzlich zur Unterstützung der Auskunft können Protokolle auch als Informationsquelle für das Auffinden von Verstößen gegen Datenschutzaufgaben oder Verträge genutzt werden. Deshalb sind Unternehmen zur Protokollierung der Zugriffe auf sensible personenbezogene Daten verpflichtet [Leo06]. Die Protokolle können jedoch selbst personenbezogene Daten enthalten und unterliegen somit auch dem Datenschutzrecht.

3.2.2 Subjektive Beherrschbarkeit: Möglichkeit und Fähigkeit zur Beherrschung

Die vorgestellten Faktoren stellen die Basis zur Gewährleistung von Beherrschbarkeit dar. Ihr Vorhandensein und ihr korrektes Funktionieren geben Nutzern (hierzu zählen sowohl die Kunden einer VO als auch die Verantwortlichen der jeweiligen Unternehmen) erst die *Möglichkeit*, die Datenverarbeitung zu beherrschen. Allerdings ist diese Möglichkeit alleine nicht immer ausreichend⁶. Soll die Datenverarbeitung wirklich beherrschbar sein, so muss (vor allem bei den Kunden einer VO) auch die *Fähigkeit* vorhanden sein, sie zu beherrschen. Informationssysteme allgemein und speziell SOA können schnell einen Grad an Komplexität erreichen, der die Fähigkeiten der betroffenen Personen übersteigt und somit ein subjektives Beherrschen der Datenverarbeitung unmöglich macht. Als geeignete Mittel, um diese Komplexität in den Griff zu bekommen und somit die Beherrschbarkeitsfaktoren vom bloßen Funktionieren zur wirklichen Nutzbarkeit aufzuwerten, bieten sich Abstraktion und (Teil-)Automatisierung an. Die Informationssysteme einer VO, die beherrschbar sein soll, müssen somit nicht nur die genannten Beherrschbarkeitsfaktoren technisch unterstützen, sondern auch an geeigneten Stellen die von den Nutzern zu verwaltenden Informationen und durchzuführenden Aktionen reduzieren und ordnen.

3.2.3 Zusammenfassung

In den vorangegangenen Abschnitten wurde der Begriff der Beherrschbarkeit und vier grundlegende Faktoren Unterrichtung, Auskunft, Zusicherungen und Protokollierung, durch die Beherrschbarkeit erreicht werden kann, vorgestellt. Anschließend wurde die Bedeutung subjektiver Beherrschbarkeit hervorgehoben. Um einen besseren Überblick über die Beherrschbarkeitsfaktoren und ihre Beziehungen zueinander zu erhalten, empfiehlt sich ein Blick auf Abbildung 3.2. Die Skala auf der linken Seite soll verdeutlichen, dass Unterrichtung und Auskunft überwiegend rechtliche Mittel zur Gewährleistung von Beherrschbarkeit sind, während Zusicherungen und Protokollierung technische Mittel sind. Die Doppelpfeile zwischen den rechtlichen und den technischen Mitteln deuten an, dass Zusicherungen die technische Basis für die Unterrichtung bilden während die Auskunft auf Basis der Protokollierung realisiert wird. Den Faktoren übergeordnet sind die Abstraktionsmechanismen, die den Nutzern erst Kontrollfähigkeit verleihen.

⁶So schildert z.B. Abschnitt 3.3 unter anderem die Probleme von Unterrichtungen, die zwar vorhanden und zugänglich, aber nur schwer verständlich sind.

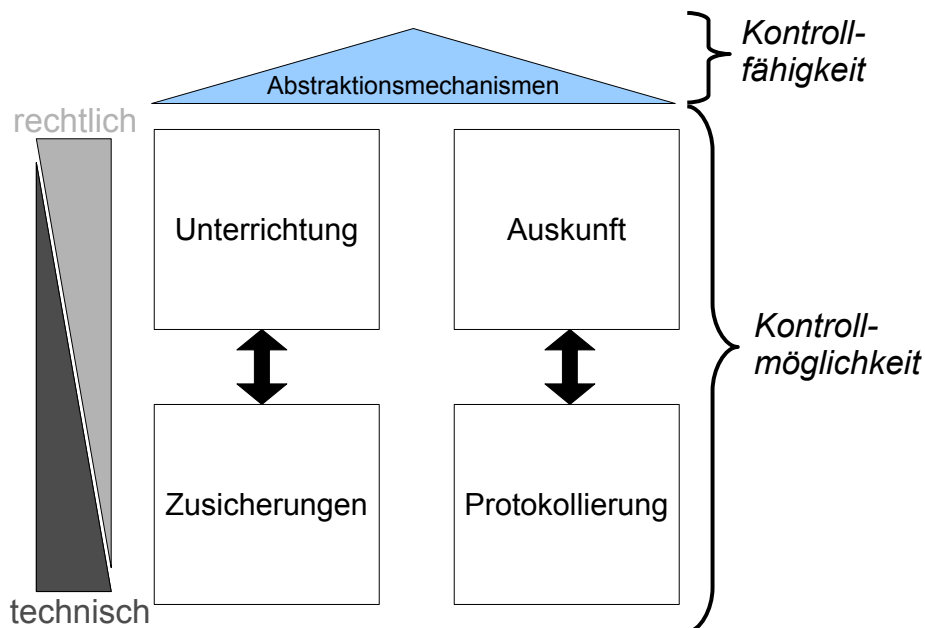


Abbildung 3.2: Beherrschbarkeitsfaktoren

3.3 Zusicherungen und Unterrichtung

Im diesem Abschnitt werden die im Kapitel 3.2 identifizierten Beherrschbarkeitsfaktoren Zusicherung und Unterrichtung detailliert analysiert. Hierfür beginnen wir mit einer Übersicht der verfügbaren Standards für Umsetzungen dieser Beherrschbarkeitsfaktoren in der Praxis sowie einer Betrachtung sonstiger relevanter Ansätze. Aus diesen Informationen werden im zweiten Abschnitt Ziele identifiziert, die im Rahmen einer Weiterentwicklung der bisherigen Ansätze anzustreben sind. Den Abschluss bildet die Ableitung von Analysefragen für die Szenarien.

3.3.1 Situation heute

3.3.1.1 Unterrichtung

In der Praxis greift ein Nutzer auf eine im Web angebotene Dienstleistung überwiegend mit Hilfe eines Webbrowsers zu und nicht über ein Web-Service-Interface.

Unterrichtung wird von der Mehrzahl der Unternehmen als Text in einer Datenschutzerklärung bzw. Datenschutzrichtlinie gegeben [JP04]. Der Inhalt der Datenschutzerklärung ist auf der Webseite publiziert und wird durch Ver-

linkung während der Beauftragung der Dienstleistung als Unterrichtung wirksam bzw. Vertragsbestandteil. Eine Datenschutzerklärung ist typischerweise umfangreich⁷ und für Personen ohne spezielle rechtliche Vorbildung schwer verständlich [MCG06]. Diese Tatsache lässt sich dadurch begründen, dass Datenschutzerklärungen überwiegend von Spezialisten mit rechtlicher Ausbildung erstellt werden um den gesetzlichen Anforderungen zu entsprechen. Auch führt die permanente Weiterentwicklung und Anpassung der Datenschutzerklärung an die konkrete unternehmerische Tätigkeit, beispielsweise durch die Aufnahme von Spezialfällen, zu einem Anwachsen des Textumfangs.

Der P3P-Standard (Platform for Privacy Preferences) [WS06] des World Wide Web Consortium (W3C) in seiner aktuellen Entwurfsversion 1.1 ist der am weitesten verbreitete Ansatz zum formalen Ausdruck von Datenschutzerklärungen eines Unternehmens gegenüber seinen Kunden. P3P basiert auf XML und enthält Definitionen von Anwendungsfällen, Empfängern, Kategorien von Daten und weiteren Datenschutzangaben, die es einem Unternehmen erlauben eine Datenschutzerklärung in P3P zu kodieren. Ein P3P Dokument liegt üblicherweise auf dem Webserver des Unternehmens in einem definierten Verzeichnispfad⁸ und kann vom Kunden, ähnlich wie eine rein textuelle Datenschutzerklärung abgerufen werden. Es ist anzumerken, dass diese Vorgehensweise der Unterrichtung impliziert, dass eine nachträgliche Unterrichtung mit P3P nicht erreicht werden kann. Hierfür müsste der Kunde eine spezifische P3P-kodierte Mitteilung erhalten, welche die für ihn relevanten Änderungen im Umgang mit seinen personenbezogenen Daten enthält.

Um eine P3P-Datenschutzerklärung zu lesen benötigt der Kunde ein Computerprogramm, das neben einer verständlichen Darstellung von P3P-Aussagen über Funktionalität zum Abgleich dieser mit den Datenschutzpräferenzen des Kunden verfügen kann. Ein zu P3P komplementärer Standard zum Formulieren von Datenschutzpräferenzen ist APPEL [CLM02]. Die erwähnten Funktionalitäten sind üblicherweise in Webbrowser enthalten oder können durch Plugins integriert werden. Die Implementierungen in aktuellen Webbrowsern sind nach Aussagen der mit der Weiterentwicklung von P3P betrauten Arbeitsgruppe unzureichend⁹. Unabhängig davon kann jedoch festgestellt werden, dass, obwohl die Verbreitung von P3P nach wie vor sehr eingeschränkt ist, eine steigende Anzahl von Unternehmen P3P-konforme Datenschutzerklärungen in ihre Webseiten einbinden [ECC06].

⁷Im US-amerikanischen Raum beispielsweise umfasst sie durchschnittlich 2000 Wörter.

⁸Üblicherweise unter: „<Domainname.com>/w3c/p3p.xml“

⁹<http://www.w3.org/P3P/>

3.3.1.2 Zusicherungen

Die Unterrichtung, die der Kunde einer VO erhält, sollte den Zusicherungen der Unternehmen der VO über den Umgang mit personenbezogenen Daten des Endkunden entsprechen. Nur in diesem Fall ist die Unterrichtung des Kunden inhaltlich korrekt. Dennoch werden solche Zusicherungen in der Realität zwischen Unternehmen entweder gar nicht oder manuell ausgehandelt und existieren textuell als Bestandteil eines Vertrages. Es existieren jedoch Standardisierungsbemühungen und Forschungsprojekte mit dem Ziel Zusicherungen zu formalisieren und an die Ausführung von Web Services zu koppeln. Der Schwerpunkt dieser Ansätze liegt in der Vorgabe, wie Zusicherungen zu formulieren sind und wie für die Zusicherungen definiert werden kann für welche Web Services sie gelten. Der Prozess einer Aushandlung von Zusicherungen ist nicht Gegenstand dieser Standardisierungsbemühungen. Im Folgenden geben wir einen Überblick der wichtigsten Ansätze, die geeignet sind in der SOA einer VO Anwendung zu finden. Eine Gemeinsamkeit dieser Ansätze ist, dass sie auf dem XML-Standard aufsetzen.

Unsemantische Ansätze Zusicherungen, die nach diesen Standards formuliert sind, beruhen in der Regel nicht auf einer Sprache mit integrierter Semantik (bspw. OWL). Daher sind die für eine Verarbeitung der Zusicherungen, insbesondere auf Seiten des Zusichernden zur Gewährleistung der Einhaltung, spezielle Anwendungsprogramme oder Software-Komponenten notwendig. Häufig sind diese zusammen mit den Standards entwickelt worden, um die Funktionsweise sicher zu stellen.

Die hier vorzustellenden Standards umfassen lediglich einen Teil der für den Einsatz von Zusicherungen in VO notwendigen Spezifikation. So bestehen Zusicherungen, aus Elementen, die den folgenden Schichten¹⁰ zugeordnet werden können: (i) „vocabulary layer“, welche die Begriffe definiert, über die Zusicherungen ausgedrückt werden (bspw. „Adressdaten“); (ii) „constraints layer“, die spezifiziert, welche Form eine Zusicherungsaussage besitzen darf (bspw. „falls Adressdaten vorhanden...“; (iii) „framework layer“, die standardisiert, wie Zusicherungsaussagen zu Mengen zusammengefasst werden und wie mit diesen Mengen umzugehen ist; (iv) „binding layer“, die spezifiziert, wie Mengen von Zusicherungsaussagen den Web Services zugeordnet werden können für die sie gelten sollen. Es findet in der Regel keine Standardisierung des Vokabulars, also der Sachverhalte selbst statt. Deshalb ist trotz Einsatz der folgenden Standards für eine Anwendung in einer VO erforderlich, ein einheitliches Vokabular zwischen allen Beteiligten zu entwickeln.

¹⁰vgl. [AD05] für diese Schichtenarchitektur.

- Die Enterprise Privacy Authorization Language (EPAL) in seiner aktuellen Version 1.2 [PS03] wurde beim W3C von IBM im Jahr 2003 eingereicht. Es wurde jedoch noch nicht zu einem offiziellen Standard erklärt. Das Ziel bei der Entwicklung von EPAL war, eine formale Sprache für Zusicherungen zur Nutzung in Unternehmen zu definieren. EPAL-Zusicherungen bestehen aus Regeln die Aktionen für Daten bestimmter Kategorien zulassen oder verweigern. Während mit Hilfe von P3P Zusicherungen in Form von Datenschutzerklärungen zur Veröffentlichung formalisiert werden können, dient EPAL der Beschreibung von Regeln für die datenschutzrelevanten innerorganisatorischen Prozesse.
- Die Web Services Policy Language (WSPL) [Mos03] basiert auf der eXtensible Access Control Markup Language (XACML) [Mos05], die es ermöglicht, Zusicherungen für Zugriffskontrolle, Authorisation und Datenschutz zu formalisieren. WSPL als eine Untermenge von XACML beschreibt einen Standard für die Beschreibung von Datenschutzzusicherungen für Web Services. Ähnlich wie in EPAL, bestehen die WSPL-Zusicherungen aus Regeln. Im Unterschied zu EPAL, bietet WSPL jedoch eine höhere Funktionalität [And06a]. Aktuell befindet sich WSPL im Entwurfsstadium und wird maßgeblich von SUN weiterentwickelt.
- WS-Policy [Ved07] ist ein Standard, der es ermöglicht, Zusicherungen für Web Services zu formulieren. Da es sich bei WS-Policy jedoch nur um ein Framework handelt, stellt es lediglich Konstrukte zur Deklaration von beliebigen XML-Ausdrücken als Aussagen innerhalb von Zusicherungen und über deren alternative Anwendung und Optionaltät zur Verfügung. Es kann durch eine Kombination mit weiteren Standards um bereichsspezifische Semantik für die Aussagen erweitert werden. Ein Vorschlag für eine solche Erweiterung von WS-Policy ist WS-PolicyConstraints [And06b]. Hiermit lassen sich XACML-konforme Zusicherungen beschreiben. Darüber hinaus sind Spezifikationen für die Bildung der Schnittmenge mehrerer Zusicherungsdokumente in WS-PolicyConstraints enthalten. Es ist anzumerken, dass auch für WS-Policy über kein standardisiertes Vokabular datenschutzrelevanter Sachverhalte (z.B. „Personenbezug“) existiert.

Semantische Ansätze Neben den o.g. Standardisierungsbemühungen, die maßgeblich von der Industrie vorangetrieben werden, existieren Forschungsprojekte, welche Formalisierungen von datenschutzrelevanten Zusicherungen untersuchen und fortentwickeln. Zur Formulierung semantischer Zusicherungen bedient man sich meist semantischer Formalisierungen wie der Web On-

tology Language (OWL) [Dea04]. Basierend auf diesen Formalismen werden Ontologien definiert. Zusicherungen und Ontologien können als Eingabedaten von automatischen Schlussfolgerungsprozessen dienen. Ein sich hieraus ergebender Vorteil ist, dass zur Ableitung solcher Schlussfolgerungen bereits frei verfügbare Anwendungsprogramme (Reasoner) existieren, welche kontinuierlich erweitert und optimiert werden. Ein Nachteil semantischer Ansätze nach [AD05] ist die zu geringe Kenntnis der Web-Service-Programmierer von semantischen Sprachen.

Prominente Beispiele für Forschungsprojekte dieser Art sind Rei [KFJ03] und KAoS [UBJ⁺03].

- Rei [KFJ03] ist ein Framework, das ursprünglich für den Einsatz im sog. „Pervasive Computing“ konzipiert wurde. Kernstück von Rei ist eine OWL-Lite Ontologie, welche die wesentlichen Konzepte definiert. Die Grundkonzepte von Rei umfassen Rechte, Verbote, Verpflichtungen und die Freistellung von Verpflichtungen. Die Zusicherungen werden in Form von Ontologien formuliert. Diese enthalten Regeln über entsprechend der Grundkonzepte beschränkte Aktionen von Entitäten. Auch für die Nutzung von Rei als Formalisierung für Zusicherungen ist es notwendig, das anwendungsbereichsspezifische Vokabular im Vorfeld einheitlich zu definieren.
- KAoS [UBJ⁺04] besteht aus Services und Werkzeugen, welche Spezifizierung, Management, Konfliktlösung und Durchsetzung von Zusicherungen ermöglichen [UBJ⁺03]. Zusicherungen werden in KAoS, ähnlich wie in Rei, als OWL-Ontologien formalisiert. Grundkonzepte, die hierin Verwendung finden, sind Authorisierung, Verpflichtung und die jeweilige Negation. Für eine konkrete Zusicherung werden diese Grundkonzepte instantiiert und mit Eigenschaftswerten versehen. Obwohl die Basisontologie¹¹ von KAoS weit über 100 Konzepte umfasst, ist auch hier für die konkrete Nutzung eine anwendungsspezifische Erweiterung erforderlich.

¹¹<http://ontology.ihmc.us/ontology.html>

Übersicht der Ansätze

	EPAL	WSPL	WS-Policy	Rei	KAoS
innerorganisatorische Verwendung	X	X	X	X	X
außerorganisatorische Verwendung		X	X	X	X
datenzentriert	X	X			
aktionenzentriert				X	X
semantisch				X	X
vocabulary layer					
constraints layer	X	X		X	X
framework layer	X	X	X	X	X
bindings layer					
offizieller Standard			X		

3.3.2 Angestrebtes Ziel

Abschnitt 3.3.1 zeigt die verschiedenen Ansätze, um Unterrichtung mit Hilfe von Zusicherungen durchzuführen. All diese Ansätze haben gemein, dass sie nicht als Lösung für die Erteilung von Auskunft geeignet sind. Umgekehrt sind die Ansätze zur Erteilung von Auskunft nicht geeignet, um Unterrichtung durchzuführen (siehe Abschnitt 3.4.1). Außerdem wird in Abschnitt 3.2 gefordert, dass die Einhaltung einer vorab mitgeteilten Zusicherung vom Kunden später jederzeit durch eine Auskunft überprüft werden kann. Dieser Vorgang kann durch die Verwendung eines maschinen-verständlichen, semantischen Formalismus, der auf einer gemeinsamen Ontologie aufbaut, für Auskunft und Zusicherung teilautomatisiert werden. Gleiches gilt für den Abgleich von Nutzerpräferenzen und Zusicherungen. Eine solche Teilautomatisierung erleichtert die Überprüfung der Einhaltung von Nutzerpräferenzen beziehungsweise mitgeteilten Zusicherungen durch den Nutzer und somit dessen Beherrschbarkeit über die Verarbeitung seiner Daten. Die gemeinsame Ontologie definiert allgemein verständlich die Datenschutz-relevanten Begrifflichkeiten, sowie die der Domäne des Dienstes. Auf diese Weise können Verständnisprobleme und der Aufwand für eventuell notwendige Übersetzungen zwischen verschiedenen Formalismen verringert werden.

Im Folgenden werden die Teile des angestrebten Ziels vorgestellt, die Nutzerpräferenzen, Zusicherungen und Unterrichtung betreffen:

Abgleich von Nutzerpräferenzen und Zusicherungen

Mit Hilfe der Nutzerpräferenzen beschreibt der Kunde, welche Aktionen er auf seinen Daten erlaubt. Würden die Nutzerpräferenzen semantisch be-

schrieben, könnten diese mit ebenfalls semantisch beschriebenen Zusicherungen teilautomatisiert abgeglichen werden. Nur im Fall, dass ein Widerspruch auftritt, der nicht automatisch aufgelöst werden kann, muss der Kunde entscheidend eingreifen.

Zusammensetzen von Zusicherungen

Damit eine VO für die Unterrichtung, welche Aktionen sie auf den persönlichen Daten ausführen will und zu welchem Zweck, Zusicherungen einsetzen kann, muss sie die Zusicherungen der verschiedenen einzelnen Unternehmen zu einer gemeinsamen Zusicherung kombinieren können, da jedes dieser Unternehmen gewisse Aktionen zu bestimmten Zwecken auf den Daten durchführt, der Kunde aber nur mit einem Unternehmen der VO interagiert. Der geforderte maschinen-verständliche, semantische Formalismus erlaubt die Teilautomatisierung dieser Aufgabe. Nur in den Fällen, dass sich Zusicherungen widersprechen oder gegenseitig ausschließen, muss eines der Unternehmen der VO eingreifen.

3.3.3 Ableitung von Analysefragen

Ausgehend von dem im obigen Abschnitt dargelegten technischen Rahmen werden im Folgenden Analysefragen spezifiziert. Diese determinieren die Perspektiven, aus denen die Szenarien in Kapitel 4 beschrieben und analysiert werden. Der Schwerpunkt der Analysefragen liegt somit auf Aspekten, welche für die Analyse einer SOA im Hinblick auf die Beherrschbarkeitsfaktoren Zusicherungen und Unterrichtung ausschlaggebend sind. Darüber hinaus wird bei den in Abschnitt 5.2 enthaltenen Lösungsvorschlägen Bezug auf die hier erläuterten Analysefragen genommen.

1. An welchen Stellen treten Zusicherungen auf?

Zur weiteren Analyse der Zusicherungen muss zunächst identifiziert werden, wo überhaupt Zusicherungen anfallen. Dies hängt vom Verhältnis von Dienstanbieter und -aufrufer ab, aber auch vom angebotenen Dienst selbst.

2. Für welche Daten werden Zusicherungen mitgeteilt?

Während der Dienstbringung können Daten anfallen, die nicht besonders schützenswert sind, so dass für sie keine Zusicherungen gemacht werden müssen. Ihnen gegenüber stehen personenbezogene Daten, die im Interesse der jeweiligen Person Gegenstand von Zusicherungen über den Datenschutz sein müssen; unter Umständen müssen auch hier nicht

für alle Daten Zusicherungen gemacht werden, wenn durch geltendes Recht bereits hinreichend beschrieben ist, wie mit ihnen verfahren werden darf. Schließlich können in einer VO auch sensible Geschäftsdaten bewegt werden, an deren Schutz ein finanzielles Interesse einer oder mehrerer Parteien besteht. Es ist daher zu klären, welche Daten die Zusicherungen überhaupt betreffen.

3. Wer sichert zu? (Wer steht gegenüber dem Kunden für die Verbindlichkeit der Zusicherung ein?)

Da die Zusicherungen auch rechtlich verbindlich sein sollen, muss es stets möglich sein, einen Verantwortlichen zu identifizieren. Rechtlich interessant könnte hier auch die Unterscheidung sein, ob ein Dienstanbieter seinem Kunden eine Zusicherung macht, die sich auch über alle von ihm aufgerufenen Dienste anderer Anbieter erstreckt, oder ob er deren Zusicherungen nur „weiterreicht“.

4. Wem wird zugesichert?

Je nachdem, wie die Verantwortung für die Einhaltung der Zusicherungen aufgeteilt ist (vgl. vorige Frage), kann ein Dienstanbieter seine Zusicherung dem unmittelbaren Aufrufer machen oder auch einer anderen Instanz, z.B. der Person, deren Daten behandelt werden. Um zu wissen, wer gegebenenfalls gegen nicht eingehaltene Zusicherungen vorgehen kann, muss folglich geklärt werden, wem die Zusicherung gemacht wurde.

5. Wer teilt die Zusicherung mit?

Wie schon in Frage 3 angedeutet, muss der Dienstanbieter, der dem Kunden die Zusicherung mitteilt, nicht zwangsläufig auch der sein, der dafür einsteht. Besonders im Interesse des Kunden stellt sich daher die Frage, wer die Zusicherung mitteilt.

6. Was wird zugesichert?

Hier ist vor allem interessant, wie detailliert die Zusicherungen sein sollen. Je mehr die Zusicherungen ins Detail gehen, desto höher wird der Aufwand, sie geeignet zu beschreiben und gegen Nutzerpräferenzen abzugleichen (implizit betrifft dies auch den Detailgrad der Protokolle). Andererseits kann es aus vertraglichen bzw. sonstigen rechtlichen Gründen für einen Dienstanbieter nötig sein, dem Aufrufer bestimmte Zusicherungen zu machen. Es ist also zu klären, was genau zugesichert wird.

7. Wie werden die Zusicherungen ausgedrückt?

Je nach Geschäftsbeziehung zwischen Dienstaufrufer und -anbieter können die Zusicherungen in verschiedenen Formen ausgedrückt werden, z.B. als ausformulierter schriftlicher Vertrag, als Teil der AGB, etc. Vor allem im Hinblick darauf, dass sie nicht von beiden beteiligten Parteien unterschiedlich ausgelegt werden können sollen, ist die Frage wichtig, wie die Zusicherungen ausgedrückt werden.

8. Wie wird Verbindlichkeit von Zusicherungen hergestellt?

Selbst unmissverständliche Zusicherungen werden wertlos, wenn der Zusichernde leugnet, sie in dieser Form gemacht zu haben; folglich muss die Verbindlichkeit der Zusicherung gewährleistet werden. Da dies unterschiedlich realisiert sein kann und z.B. bei Zusicherungen in rein digitaler Form anders gelöst werden muss als bei schriftlichen Verträgen, muss jeweils für den konkreten Fall betrachtet werden, wie die Verbindlichkeit hergestellt wird.

9. Wird die Flexibilität der virtuellen Organisation durch die mitgeteilten Zusicherungen beeinflusst?

Ein wesentliches Konzept der SOA besteht darin, dass dynamisch Dienste ersetzt werden können oder neue Dienste dazu kommen. Wurden gegenüber dem Kunden bereits Zusicherungen darüber gemacht, was mit seinen Daten geschieht, so kann es passieren, dass die VO bestimmte Dienste nicht mehr austauschen kann, weil dadurch die Zusicherungen verletzt würden. Um diesen möglichen Nachteil der VO zu erkennen, muss betrachtet werden, inwieweit Zusicherungen mitgeteilt werden, die diese Flexibilität beeinträchtigen.

10. Wie würden Änderungen an der virtuellen Organisation die mitgeteilten Zusicherungen beeinflussen?

Diese Frage ist im gleichen Kontext wie die vorige Frage zu betrachten; dort wurde angenommen, dass die Zusicherungen starr sind und die Flexibilität der VO möglicherweise darunter leidet – andererseits kann es aber auch erwünscht sein, Änderungen an der VO in jedem Fall zuzulassen und dann gegebenenfalls die bereits mitgeteilten Zusicherungen anzupassen. Es muss also betrachtet werden, ob bzw. wie diese Zusicherungen geändert werden, wenn die VO sich ändert.

11. Wie wird die Einhaltung der mitgeteilten Zusicherung überprüft?

Zusicherungen sind insbesondere dann wirksam, wenn sie nach der Serviceausführung überprüft werden, oder die Überprüfung zumindest möglich ist. Aus diesem Grund ist der Frage der Überprüfbarkeit von Zusicherungen ein großes Gewicht beizumessen.

12. Wie wird die Einhaltung der mitgeteilten Zusicherungen sicher gestellt?

Neben der Überprüfbarkeit der Einhaltung von Zusicherungen nach Abarbeitung des Services besteht ein anderer Aspekt in der Verhinderung eines nicht zusicherungskonformen Verhaltens schon während der Serviceausführung. Insbesondere der Serviceanbieter hat ein großes Interesse daran, eine von ihm unbeabsichtigte Verletzung der Zusicherungen zu vermeiden.

13. Wie werden Nutzerpräferenzen ausgedrückt?

Die Präferenzen als Gegenstück der Zusicherungen sind vor allem für die Auswahl des Kunden der für ihn geeigneten Services relevant. Insbesondere wenn die Serviceauswahl nicht vom potentiellen Servicenutzer manuell durchgeführt wird, sondern semiautomatisch erfolgt, ist zu klären, in welcher Repräsentationsform die Nutzerpräferenzen vorliegen.

14. Wer drückt die Nutzerpräferenzen aus?

Die Nutzerpräferenzen entsprechen den Eigenschaften, die ein Service besitzen muss, um vom potentiellen Nutzers aufgerufen zu werden. Diese Präferenzen müssen, um wirksam zu werden, vom Nutzer geäußert werden. Um jedoch für den gesamten Service-Workflow in der der VO Geltung besitzen zu können, ist zu klären, an welchen Stellen diese Präferenzen im Geflecht der Einzelorganisationen zum Tragen kommen.

15. Wie werden Nutzerpräferenzen und Zusicherungen abgeglichen?

Da die Nutzerpräferenzen vom Kunden gewünschte Serviceeigenschaften und die Zusicherungen die Eigenschaften des angebotenen Services repräsentieren, ist für eine Übereinkunft zwischen beiden Parteien ein Abgleich zwischen Nutzerpräferenzen und Zusicherungen erforderlich. Insbesondere für den Suchprozess des Nutzers nach für ihn geeigneten Services ist die Frage zu erörtern, wie der Abgleich für einen mehrstufigem Service-Workflow in einer VO ermöglicht werden kann.

16. Wer gleicht die Nutzerpräferenzen mit den Zusicherungen ab?

Im Rahmen der Durchführung des Abgleichsprozesses ist eine Einflussnahme zugunsten einer Partei denkbar. Deshalb stellt sich die Frage, wer mit dem Abgleich beauftragt werden kann und sollte.

17. Wie findet die Unterrichtung statt?

Im Falle des Eintretens der Unterrichtungspflicht entsteht insbesondere bei Vorliegen einer Verkettung von Services in einer VO, die Situation, dass eine Unterrichtung nur durch Zusammenarbeit mehrerer Beteiligter durchgeführt werden kann. Aus diesem Grund ist zu klären, wie eine Unterrichtung unter den gegebenen Rahmenbedingung umsetzbar ist.

18. Wann wird unterrichtet?

Entsprechend der gesetzlichen Vorgaben zur Unterrichtungspflicht stellt sich die Frage, wie die Beteiligten der VO in die Lage versetzt werden können, zu erkennen wann eine Unterrichtung erforderlich ist und wann nicht (z.B. § 16 Absatz 3 BDSG).

3.4 Protokollierung und Auskunft

Im diesem Abschnitt werden die im Kapitel 3.2 identifizierten Beherrschbarkeitsfaktoren Protokollierung und Auskunft detailliert analysiert. Hierfür beginnen wir mit einer Übersicht der verfügbaren Standards für Umsetzungen dieser Beherrschbarkeitsfaktoren in der Praxis sowie einer Auflistung relevanter Forschungsansätze. Aus diesen Informationen werden im zweiten Abschnitt Ziele identifiziert, die im Rahmen einer Weiterentwicklung der bisherigen Ansätze anzustreben sind. Den Abschluss bildet die Ableitung von Analysefragen für die Szenarien.

3.4.1 Situation heute

3.4.1.1 Auskunft

Das BDSG verpflichtet jedes Unternehmen, das personenbezogene Daten nutzt, Betroffenen auf Antrag Auskunft darüber zu erteilen, welche Daten es gespeichert hat, wo sie erhoben wurden, an wen die Daten weitergegeben werden und zu welchem Zweck sie gespeichert wurden (§ 19 Abs. 1 BDSG).

Dies bedarf der Initiative des Betroffenen; um den Antrag auf Auskunftserteilung zu stellen, muss dieser im allgemeinen Fall zunächst das Unternehmen kennen, an das er seinen Antrag richten will. Er muss die Post-Adresse des Unternehmens ermitteln, idealerweise direkt auch den verantwortlichen Datenschutzbeauftragten. Schließlich muss er ein Schreiben formulieren, in dem er seinen Auskunftsanspruch geltend macht – mit Bezugnahme auf das BDSG, um sicher zu stellen, dass das Unternehmen sich seiner Verpflichtungen bewusst ist – und es postalisch zustellen. Im Idealfall erhält er vom Unternehmen nach wenigen Tagen eine umfassende Auskunft als Antwort.

Das Internet und die damit zusammenhängenden Technologien haben zwar einen zunehmenden Einfluss auf das Konsumverhalten vieler Personen, d.h. auf die Dienstleistungen, die in Anspruch genommen werden, sowie auf die Art, wie Kundendaten in Unternehmen verarbeitet werden. Die schnelle technische Entwicklung hat jedoch die Auskunftsproblematik nur geringfügig verbessert: für ein konkretes Unternehmen kann über dessen Webseite leichter eine E-Mail-Adresse gefunden werden, an die der Betroffene sich wenden kann (dies wird unter Umständen noch durch den Einsatz von P3P begünstigt), und die E-Mail kann schneller verschickt werden als vormals ein Brief.

Nach wie vor jedoch muss der Betroffene seine Anfrage selber verfassen; je nachdem, wo das Unternehmen seinen Firmensitz hat, kann dies nicht nur zu sprachlichen Problemen, sondern auch zu Rechtsunsicherheiten führen. Auch kann der Betroffene nach wie vor nur bei jedem an der Datenverarbeitung beteiligten Unternehmen direkt Auskunft einholen, wozu er diese Unternehmen zunächst überhaupt identifizieren muss. Dies kann, je nach Anzahl der beteiligten Unternehmen, für den Betroffenen nicht nur schwer zu überblicken sein, sondern sich auch über einen Zeitraum von mehreren Monaten erstrecken [Wei06]. Schließlich werden Auskunftsersuchen oft nicht oder nur unzureichend beantwortet, was auch daran liegt, dass viele Unternehmen organisatorisch und technisch nicht in der Lage sind, Auskunft zu erteilen [Wei06].

3.4.1.2 Protokollierung

Protokollierung kann ein geeignetes technisches Mittel sein, um die Auskunft zu erzeugen. Darüber hinaus können durch Protokollierung auch die Abläufe innerhalb eines Unternehmens nachvollzogen werden, was nicht nur bei einem Audit hilfreich ist, sondern allgemein die Beherrschbarkeit des Systems steigert.

Die meisten Software-Systeme sind in der einen oder anderen Weise imstande, Protokolle über bestimmte Ereignisse zu führen. Der Detailgrad dieser Logdateien reicht dabei von kurzen, auf den einzelnen Rechner bezogenen Meldungen (wie in UNIX) über ausführliche, anwendungsspezifische Meldun-

gen moderner Software-Systeme bis hin zu vollständigen Kommunikationsprotokollen, in denen alle ein- und ausgehenden Nachrichten eines Systems festgehalten werden. Wie der Detailgrad kann auch der Anwendungszweck ganz unterschiedlich sein: Logdateien können dazu verwendet werden, das fehlerfreie Arbeiten des Systems sicherzustellen, um mögliche Angriffe aufzudecken, oder zur Performance-Analyse.

Das automatisierte Verarbeiten von Protokollen ist dank standardisierter (wenngleich oft nicht weit verbreiteter) Dateiformate wie beispielsweise dem „Extended Log File Format“ des W3C [HBB96] schon länger möglich; auch für eine zentrale Protokollierung in verteilten Systemen innerhalb von Unternehmen existieren bereits Lösungen (z.B. durch Software wie „syslog“). Dennoch bleiben noch einige Probleme offen:

- Jedes Unternehmen protokolliert nur seine eigenen Daten. Im Falle einer virtuellen Organisation bedeutet dies, dass Protokolle, die sich auf die Daten einer einzelnen Person bzw. deren Verarbeitung beziehen, über das ganze System verstreut sind. Dies ist besonders dann problematisch, wenn einzelne Unternehmen die Organisation verlassen, da dies bedeuten kann, dass die Verarbeitung bestimmter Datensätze nicht mehr rekonstruiert werden kann.
- Informationen auf hohem Abstraktionsniveau können in Logdateien verloren gehen. Selbst bei umfangreichen systemnahen Protokollen, die für administrative Zwecke innerhalb eines Unternehmens geeignet sind, können die Kontextinformationen fehlen, die für die Rekonstruktion des Prozesses benötigt werden, den ein bestimmter Datensatz durchlaufen hat. Für die Protokollierung auf höherem Niveau existieren jedoch bislang kaum Standards [Wol06].

Existierende Forschungsansätze umfassen z.B. [BB05], in dem einfache (nicht semantische) Protokolle mit semantischen Informationen angereichert werden, um sie gemeinsam analysieren zu können. Es werden jedoch keine Informationen erzeugt, die nicht bereits in den einfachen Protokollen vorlagen. Andere Ansätze bieten zwar „semantische Protokollierung“, haben aber durch ihre speziellen Einsatzgebiete nichts mit SOA zu tun¹²

- Sicherheit ist nach wie vor ein Problem. Dies beinhaltet naheliegende Anforderungen wie z.B., dass das protokollierende System vor (versehentlichen und gezielten) Manipulationen geschützt werden muss, aber

¹²Als Beispiel kann hier „Magpie“ [DDM04] genannt werden, ein System, das die Informationssuche im Semantic Web unterstützen soll.

auch, dass das System, von dem eine Log-Nachricht stammt, und das protokollierende System sich gegenüber dem anderen authentifizieren müssen. Da es kein einheitliches Protokollierungssystem gibt, das für alle Zwecke gleichermaßen geeignet ist, werden in der Praxis unterschiedliche Protokollformate eingesetzt, deren Verwaltung wiederum einen Mehraufwand mit sich bringt [Wol06] und dadurch die Beherrschbarkeit des Systems einschränkt.

3.4.2 Angestrebtes Ziel

Ausgehend von den Problemen, die Auskunft und Protokollierung zur Zeit mit sich bringen, werden im Folgenden einige Anforderungen definiert, deren technische Umsetzungen zur Lösung der Probleme geeignet sind.

Organisationsweite Auskunft

Die Komplexität der virtuellen Organisation soll vor dem Kunden verborgen werden: eine einzelne Anfrage des Kunden an das Unternehmen, mit dem er unmittelbaren Kontakt hat, und das für ihn die Organisation repräsentiert, soll ausreichen, um eine Auskunft zu erzeugen, die sich über die Speicherung und Nutzung seiner Daten in allen beteiligten Unternehmen äußert.

Vielseitiger Protokollierungsstandard

In Protokollen wird festgehalten, wie mit den Daten einzelner Personen verfahren wird; aus diesen Protokollen können bei Bedarf die benötigten Informationen bezogen werden, mit denen schließlich die Auskunft erteilt wird. Dieser Prozess lässt sich unterstützen durch eine Kombination folgender Anforderungen:

- Maschineninterpretierbares Protokollformat
- Mechanismus, der geeignet ist, Datenschutz-relevante Aktionen zu protokollieren
- Maschineninterpretierbares Format für die Auskunft (siehe auch vorangegangene Forderung)

Ein Protokollierungsstandard, der diese drei Aspekte abdeckt, kann mit der (ebenfalls bereits geforderten) standardisierten Anfrage genutzt werden, um den ganzen Prozess des Auskunft-Ersuchens (wenigstens teilweise) zu automatisieren und dadurch zu erleichtern.

Auditfähigkeit

Unternehmensinterne und durch Behörden ausgeführte Audits sollen vereinfacht werden. Darüber hinaus soll auch (in begrenztem Umfang) dem Kunden ermöglicht werden, durch einen Vergleich der Zusicherungen, die er von einem Unternehmen oder der ganzen virtuellen Organisation erhalten hat, mit der Auskunft darüber, die mit seinen Daten verfahren wurde, zu prüfen, ob die Zusicherungen eingehalten wurden. Ein einheitlicher Formalismus für Zusicherung und Auskunft kann hier eine (Teil-) Automatisierung ermöglichen und somit Audits vereinfachen.

Zugreifbarkeit der Protokolldaten

Um eine organisationsweite Auskunft zu erreichen, ist es zwingend nötig, dass das Unternehmen, das den direkten Kontakt zum Kunden hat, auf alle relevanten Protokolldaten der anderen Unternehmen zugreifen kann. Dies kann durch einen „zentralen Zugriffspunkt“ erreicht werden, an dem alle benötigten Daten gesammelt vorliegen und abgerufen werden können.

Langfristige Verfügbarkeit der Protokolldaten

Protokolle sollen auch dann noch verfügbar und die auf ihnen basierende Auskunft möglich sein, wenn einzelne Unternehmen eine virtuelle Organisation verlassen haben. Dies lässt sich wie auch die vorangegangene Anforderung durch die Speicherung der Protokolle an einem zentralen Zugriffspunkt erreichen.

Datensparsamkeit, Zweckbindung

Dem Wunsch, möglichst umfassende Protokolle zu erstellen, die später möglichst vielseitig genutzt werden können, stehen die datenschutzrechtlichen Forderungen nach Datensparsamkeit und Zweckbindung entgegen.

Um Datensparsamkeit zu erreichen, d.h. nur die Daten zu speichern, die unbedingt notwendig sind, muss, wie bereits gefordert, bei der Protokollierung ein Mechanismus eingesetzt werden, der über die datenschutzrechtliche bzw. anderweitige Relevanz eines Protokolleintrages entscheiden und ihn gegebenenfalls verwerfen kann.

Die Bindung der gespeicherten Daten an einen bestimmten Zweck, z.B. die Bestimmung, dass Protokolldaten nur zu Zwecken der Auskunftserteilung genutzt werden dürfen, lässt sich bewerkstelligen, indem den Daten Metadaten angeheftet werden, die über die Art der Daten sowie über den Zweck

ihrer Speicherung Aufschluss geben. Soll ein auf diese Weise annotiertes Datum später verwendet werden, so lässt sich unmittelbar feststellen, ob seine Verwendung im konkreten Zusammenhang legitim ist.

3.4.3 Ableitung von Analysefragen

Ausgehend von dem im obigen Abschnitt dargelegten technischen Rahmen werden im Folgenden Analysefragen spezifiziert. Diese determinieren die Perspektiven, aus denen die Szenarien in Kapitel 4 beschrieben und analysiert werden. Der Schwerpunkt der Analysefragen liegt somit auf Aspekten, welche für die Analyse einer SOA im Hinblick auf die Beherrschbarkeitsfaktoren Protokollierung und Auskunft ausschlaggebend sind. Die folgende Liste setzt den in Abschnitt 3.3.3 begonnenen Katalog von Analysefragen fort. Darüber hinaus wird bei den in Abschnitt 5.3 enthaltenen Lösungsvorschlägen Bezug auf die hier erläuterten Analysefragen genommen.

19. An welchen Stellen wird protokolliert?

Die Protokollierung der Aktionen, die ein Dienst ausführt, kann an verschiedenen Stellen geschehen. Zum Beispiel kann der Dienst selbst oder die Dienstplattform, auf der der Dienst ausgeführt wird, die Protokollierung durchführen. Für die spätere Auswertung der Protokolle ist es daher wichtig zu wissen, auf welchen Systemen die Protokolle liegen.

20. Was wird protokolliert?

Während der Dienstleistung fallen viele Informationen über die Verarbeitung der Daten an. In diesem Zusammenhang muss geklärt werden, welche dieser Information die einzelnen Partner überhaupt protokollieren beziehungsweise welche Informationen sie protokollieren müssten.

21. Wie wird protokolliert?

Es ist zu klären, welche Formate und welche Detailgrade bei der Erstellung der Protokolle von den verschiedenen Partnern verwendet werden.

22. Wer kann auf die Protokolle zugreifen?

Die Protokolle enthalten die Informationen, die für die Erfüllung der Auskunfts- und Informationspflicht gebraucht werden. Daher stellt sich die Frage, welcher Partner auf welche Protokolle zugreifen kann und ob alle benötigten Partner Zugriff haben.

23. Wie wird Verbindlichkeit von Protokollen hergestellt?

Für die rechtliche Verwertbarkeit der Protokolle ist es entscheidend, dass diese verbindlich sind. Hierfür muss festgestellt werden, wie die einzelnen Partner die Verbindlichkeit ihrer Protokolle gewährleisten.

24. Wie wird Auskunft erteilt?

Auf Anfrage einer Privatperson oder eines sonstigen Kunden, falls vertraglich geregelt, sind Dienstanbieter zur Auskunft über die Verwendung von Personenbezogenen oder sonstigen Daten verpflichtet. Daher stellt sich die Frage, über welche Wege dies von den Partnern ermöglicht wird.

25. Wer erteilt wem Auskunft?

In der komplexen Struktur einer VO ist zu klären, welcher Partner wem Auskunft erteilen muss.

26. Wie wird Verbindlichkeit der Auskunft hergestellt?

Für die rechtliche Verwertbarkeit einer Auskunft ist es entscheidend, dass diese verbindlich ist. Hierfür muss festgestellt werden, wie der Auskunftserteilende die Verbindlichkeit seiner Auskunft garantiert.

27. Wie wird die zukünftige Auskunftsfähigkeit sichergestellt?

Da die VO eventuell kürzer besteht als die Auskunftspflicht einzelner Partner, muss festgestellt werden, dass Auskunftsfähigkeit mindestens solange wie vorgeschrieben sichergestellt wird.

28. Wie werden Berichtigung, Löschung und Sperrung durchgeführt?

Auf Antrag einer Privatperson sind Dienstanbieter zur Berichtigung, Löschung oder Sperrung von personenbezogenen Daten (der beantragenden Person) verpflichtet. Daher stellt sich die Frage, über welche Wege die Partner einen solchen Antrag ermöglichen und wie die Berichtigung, Löschung beziehungsweise Sperrung ausgeführt werden.

Kapitel 4

Analyse der Szenarien

Im diesem Kapitel werden fünf Szenarien des Einsatzes von SOA in virtuellen Organisationen vorgestellt. Sie enthalten sowohl eine technische Analyse der eingesetzten Informationssysteme als auch eine rechtliche Analyse der aus Datenschutzsicht relevanten Problembereiche. Bei der Auswahl der Szenarien wurde versucht, ein breites Spektrum virtueller Organisationen abzudecken. So sind:

1. VO unterschiedlicher Komplexität,
2. bewährte wie auch innovative Geschäftsmodelle,
3. sowohl Dienstleistungen als auch virtuelle Güter,
4. nationale und länderübergreifende VO,
5. sowohl der Schutz personenbezogener Daten als auch von Betriebs- und Geschäftsgeheimnissen

betrachtet worden.

4.1 PotatoSystem: Basisszenario Datenschutz, virtuelle Güter

Bei dem PotatoSystem handelt es sich um ein System zum Vertrieb digitaler Güter (im vorliegenden Szenario MP3s), welches durch die 4FriendsOnly.com Internet Technologies AG betrieben wird. Das PotatoSystem realisiert dabei eine alternative Geschäftsidee: Im Gegensatz zu anderen Vertriebssystemen werden die Musikdateien nicht durch DRM-Mechanismen geschützt. Durch

ein Provisionssystem soll den Nutzern ein zusätzlicher Anreiz geboten werden, für heruntergeladene Musik zu zahlen – Käufer, die sich im Potatosystem registrieren lassen, können selbst wieder als Verkäufer auftreten und erhalten Provisionen für verkaufte Dateien.

Die Verantwortlichkeiten des Anbieters und des PotatoSystem sind klar aufgeteilt: Der Anbieter muss die Musikdateien, die er verkaufen will, auf seiner Web-Seite selbst bewerben. Auch werden die Dateien nicht dauerhaft auf Servern des PotatoSystem gespeichert, der Anbieter muss also auch dafür Sorge tragen, dass sie permanent für die Server des PotatoSystem zugreifbar sind. Diese wiederum verwalten zu allen verfügbaren Musikdateien Meta-Informationen wie Liedtitel, Interpret, Preis, etc.. Der Anbieter kann diese Informationen so in seine Webseite integrieren, dass sie direkt vom PotatoSystem abgerufen werden, welches auch eine Warenkorb-Funktion bereitstellt. Entscheidet sich ein Kunde zum Kauf, übernimmt das PotatoSystem die Transaktionsverwaltung und die Berechnung möglicher Provisionen. Für die Bezahlung der Dateien kommt das Payment-System Paybest zum Einsatz, welches ebenfalls (vom PotatoSystem unabhängig nutzbar) durch die 4FO AG betrieben wird. In Paybest sind verschiedene Bezahlssysteme gebündelt, die teilweise auch von Drittanbietern zur Verfügung gestellt werden - exemplarisch wird im Folgenden PayPal¹ als einer dieser Drittanbieter behandelt.

4.1.1 Akteure

4.1.1.1 4FO AG

Die 4FO AG stellt das PotatoSystem sowie den auch unabhängig nutzbaren Payment-Service Paybest bereit und verdient anteilig an den verkauften Musikdateien. 4FO betreibt weder eine eigene Downloadplattform, noch speichern sie selber Musikdateien, daher muss hierfür auch keine Infrastruktur bereit gestellt werden.

In der weiteren Beschreibung wird die 4FO AG in verschiedene Einzelakteure (wie den Payment-Server und den HTML-Server, vgl. Abb. 4.2 auf Seite 66) untergliedert. Hierdurch wird eine genauere Technikbeschreibung ermöglicht, als wenn die 4FO AG als ein geschlossener Akteur betrachtet würde. Faktisch finden Datenflüsse zwischen diesen Einzelakteuren alle innerhalb des Akteurs 4FO AG statt.

¹<http://www.paypal.de>

4.1.1.2 Paypal

PayPal ist der Anbieter eines eigenen Bezahlsystems. Von der Einbettung dieses Bezahlsystems in Paybest profitieren beide beteiligten Anbieter: Die 4FO AG ermöglicht den Kunden, die schon einen PayPal-Account haben, in gewohnter Weise zu bezahlen, und macht ihnen dadurch die Nutzung des PotatoSystems einfacher. PayPal kassiert dafür die für Geschäftskunden üblichen Gebühren von der 4FO AG.

4.1.1.3 Anbieter

Es gibt verschiedene Gruppen von Anbietern, für die das PotatoSystem interessant ist:

Label kann DRM-freie Musikdateien vertreiben. Durch das Provisionsmodell soll gewährleistet werden, dass das Label trotz des nicht vorhandenen Kopierschutzes Gewinn macht.

Einzelkünstler kann ohne großen Kostenaufwand eigenen Bekanntheitsgrad steigern, da durch die Weiterverkäufe mehr Kunden erreicht werden, als dies bei einer einzelnen Webseite der Fall wäre.

4.1.1.4 Käufer

Der Käufer kann DRM-freie Musik kaufen und diese problemlos kopieren, brennen, etc. Er kann die gekaufte Musik auch legal und einfach auf seiner eigenen Webseite über einen speziellen Verkaufslink, der zu einem Warenkorb im PotatoSystem führt, weiterverkaufen und erhält dafür die Provision.

4.1.2 Beziehungen der Akteure

In Abb. 4.1 sind die Beziehungen zwischen den Akteuren dargestellt:

1. Der Anbieter bewirbt auf seiner Webseite die Musikdateien, die der Käufer über das PotatoSystem kaufen kann. Außer dieser Werbung stehen Anbieter und Käufer nur indirekt über die 4FO AG in Beziehung zueinander.
2. Entscheidet sich der Käufer für den Erwerb von Musikdateien, so geht er mit der 4FO AG einen Kaufvertrag ein. Nimmt er darüber hinaus noch am Provisionssystem teil (wozu er einen Account erstellen muss), so beinhaltet der Kaufvertrag auch das Recht zum Weiterverkauf im Rahmen des PotatoSystem. Die 4FO AG verpflichtet sich, die

Kaufabwicklung zu übernehmen, und zahlt dem Käufer Provision für weiterverkaufte Dateien.

3. Der Vertrag zwischen Anbieter und 4FO AG legt fest, dass der Anbieter zur Abwicklung des Verkaufs seiner Musikdateien das PotatoSystem nutzen kann, wobei die Dateien nicht DRM-geschützt sein dürfen und der Anbieter mit dem Provisionssystem einverstanden sein muss. Überdies muss er die Dateien selbst online vorhalten, da die Server des PotatoSystem sie nicht dauerhaft speichern.
4. Um die erworbenen Musikdateien zu bezahlen, wendet sich der Käufer zunächst an das Paybest-System, das von der 4FO AG bereitgestellt wird (siehe auch 2). Dieses bietet ihm unter anderem die Möglichkeit, die Zahlung über verschiedene Drittanbieter abzuwickeln. Der Kunde entscheidet sich für PayPal und benötigt dementsprechend einen PayPal-Account, um dort bezahlen zu können.
5. Die 4FO AG hat einen Account bei PayPal, auf dem das von ihren Kunden eingezahlte Geld eingeht und von dem es weiter auf ein reguläres Bankkonto transferiert werden kann. Für diese Leistung muss die 4FO AG Gebühren an PayPal zahlen.

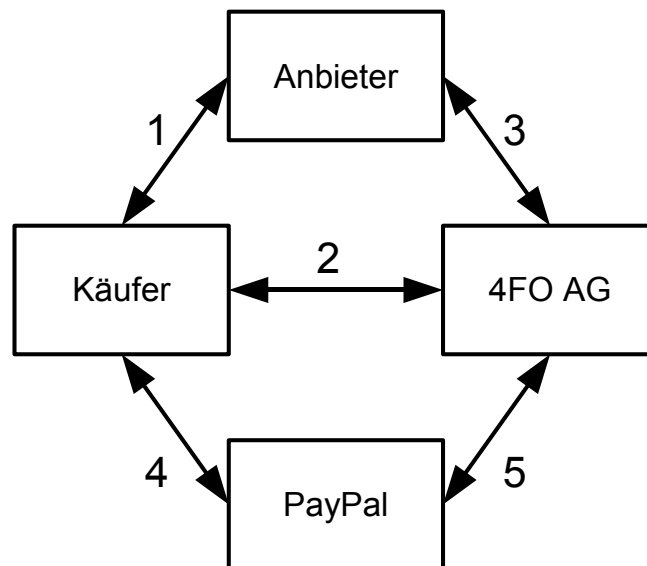


Abbildung 4.1: Beziehungen der Akteure im PotatoSystem-Szenario

4.1.3 Datenflüsse zwischen den Akteuren

- Sobald der Nutzer sich zum Kauf einer oder mehrerer Dateien entscheidet, wird er vor die Wahl gestellt:
 - Legt er einen Account an (oder meldet sich mit einem existierenden Account an), so muss er einen selbstgewählten Account-Namen und ein Passwort sowie seine E-Mail-Adresse angeben und hat fortan die Möglichkeit, am Provisionssystem teilzunehmen; zu diesem Zweck werden seine Daten an den Accounting-Server übermittelt.
 - Er kann den Kauf auch anonym abwickeln, ist dann allerdings vom Provisionssystem ausgeschlossen.
- Der HTML-Server leitet den Kunden an den Payment-Server weiter und teilt diesem mit, welche Dateien bezahlt werden sollen und wieviel sie kosten. Die spätere Zuordnung von Kunde, Warenkorb und Bezahlung erfolgt nur durch den Accounting-Server anhand einer ebenfalls übermittelten Session-ID; die eigentlichen Kundendaten werden nicht übermittelt.
- Das verwendete Payment-System Paybest ermöglicht die Zahlung über verschiedene Drittanbieter (PayPal, T-Pay, etc.). Entscheidet sich der Nutzer dafür, einen dieser Drittanbieter zu nutzen, so wird er direkt dorthin verwiesen, wobei außer einer Transaktionsnummer, die die spätere Zuordnung zu einem konkreten Bezahlvorgang ermöglicht, keine Daten an den Drittanbieter fließen.
- Je nachdem, welcher Drittanbieter genutzt wird, muss der Nutzer auch dort einen Account anlegen und verschiedene Daten wie z.B. seine Kreditkartennummer oder seine Bankverbindung angeben. Im hier betrachteten Fall von PayPal muss der Kunde mindestens seinen Namen und seine Post- und E-Mail-Adresse angeben.
- PayPal informiert den Payment-Server, dieser wiederum informiert den HTML-Server über den Abschluss einer Zahlung. Außer der Information, dass die Ware bezahlt wurde (oder ggf., dass der Bezahlvorgang gescheitert ist), werden keine neuen Informationen übermittelt.
- Der Proxy lädt die ausgewählten Dateien vom File-Server des Anbieters herunter und speichert sie zwischen, so dass der Nutzer sie von dort herunterladen kann.

4.1.4 Verantwortlichkeit

In diesem Szenario werden personenbezogene Daten von Nutzern des PotatoSystems verwendet. Wie die Beschreibung der Datenflüsse zwischen den Akteuren gezeigt hat, erfolgt die Datenverarbeitung durch verschiedene Stellen, nämlich den jeweiligen Musikanbieter, die 4FO AG und den jeweiligen Zahlungsmittelanbieter (z. B. PayPal). Da keine besonderen vertraglichen Vereinbarungen existieren, sind die genannten Stellen auch jeweils für die von ihnen durchgeführte Datenverarbeitung verantwortlich.

4.1.5 Service-orientierte Architektur

In diesem Abschnitt wird eine mögliche Service-orientierte Architektur (SOA) für dieses Szenario beschrieben, indem zu jedem Akteur die Services, die er anbietet, samt Ein- und Ausgabedaten erläutert werden.

4.1.5.1 Services

4FO AG - Paybest

Bezahlung Dieser Dienst wird vom PotatoSystem für die Bezahlung von Warenkörben verwendet. Er stößt für den Kunden den Bezahlvorgang beim gewählten Drittanbieter an und meldet der 4FO AG Erfolg, wenn die Bezahlung abgeschlossen ist.

Eingabedaten

Datum	Verwendungszweck	Personenbezug
Transaktionsnummer	Zuordnung zu Warenkorb	-
Preis	Abwicklung der Bezahlung	-
Zahlungsanbieter	Auswahl des (Dritt-)anbieters durch den Kunden	-

Ausgabedaten

Datum	Verwendungszweck	Personenbezug
Transaktionsnummer	Zuordnung zu Warenkorb	-
Erfolgsmeldung	Fertigstellung des Kaufes	-

Zahlungsabschluss melden Dieser Service kann durch Drittanbieter genutzt werden, um Paybest über eine erfolgte Bezahlung zu informieren. In der Praxis kann dies durch eine E-Mail realisiert sein, die PayPal an Paybest versendet.

Eingabedaten

Datum	Verwendungszweck	Personenbezug
Transaktionsnummer	Zuordnung zu PayPal-Bezahlvorgang	-

Ausgabedaten

Datum	Verwendungszweck	Personenbezug
Erfolgsmeldung		-

4FO AG - PotatoSystem

Metadaten-Abfrage Durch diesen Dienst kann der Anbieter Metadaten zu den von ihm angebotenen Dateien abfragen. Der Kauflink enthält auch eine Nummer, durch die auf den Anbieter geschlossen werden kann.

Eingabedaten

Datum	Verwendungszweck	Personenbezug
Produktnummer	Zuordnung zu Datensatz	-

Ausgabedaten

Datum	Verwendungszweck	Personenbezug
Interpret	Anzeige in Webseite	-
Liedtitel	Anzeige in Webseite	-
Name d. Albums	Anzeige in Webseite	-
Kauflink	Weiterleitung zum PotatoSystem	Anbieter

Account-Erstellung Falls ein Käufer am Provisionssystem teilnehmen möchte, muss er einen Account erzeugen.

Eingabedaten

Datum	Verwendungszweck	Personenbezug
Username	Selbstgewählt, zur Identifizierung	Käufer
E-Mail-Adresse	Kommunikation zw. Käufer und System	Käufer

Ausgabedaten

Datum	Verwendungszweck	Personenbezug
Erfolgsmeldung		-

Kauf von Dateien Beim Kauf der ausgewählten Dateien wird zur Bezahlung o.g. Bezahlendienst genutzt. Die Weiterverkaufslinks sind nur in den Ausgabedaten enthalten, falls der Käufer einen Account im PotatoSystem hat.

Eingabedaten

Datum	Verwendungszweck	Personenbezug
Warenkorb	Zusammenstellung mehrerer Dateien	Anbieter der Dateien

Ausgabedaten

Datum	Verwendungszweck	Personenbezug
Downloadlinks	Übertragung der Dateien zum Käufer	-
Verkaufslinks	Für den Weiterverkauf durch den Käufer	Käufer

Herunterladen von Dateien Der Käufer kann die durch beim Kauf erhaltenen Downloadlinks die erworbenen Dateien herunterladen.

Eingabedaten

Datum	Verwendungszweck	Personenbezug
HTTP-Anfrage	Download	-

Ausgabedaten

Datum	Verwendungszweck	Personenbezug
Musikdatei	Abschluss des Kaufvorgangs	-

PayPal

Bezahlung Durch diesen Service kann der Kunde die Bezahlung abwickeln, wenn er sich dafür entscheidet, über PayPal statt direkt über Paybest zu bezahlen. Hier davon ausgegangen, dass der Kunde bereits Guthaben auf seinem PayPal-Account hat, mit dem er die Zahlung vornehmen kann. Ist die Zahlung erfolgt, so wird dem Kunden der Erfolg gemeldet, und die 4FO AG erfährt von dem Zahlungseingang auf ihrem PayPal-Account.

Eingabedaten

Datum	Verwendungszweck	Personenbezug
Transaktionsnummer	Zuordnung zu Bezahlvorgang und Empfänger	-
Preis	Abwicklung der Bezahlung	-
E-Mail-Adresse	Dient PayPal als Kundenkennung	Kunde

Ausgabedaten

Datum	Verwendungszweck	Personenbezug
Erfolgsmeldung		-

Anbieter

Herunterladen von Dateien Der Anbieter muss der 4FO AG eine Schnittstelle bereitstellen, über die die Musikdateien übertragen werden können.

Eingabedaten

Datum	Verwendungszweck	Personenbezug
HTTP-Anfrage	Download	-

Ausgabedaten

Datum	Verwendungszweck	Personenbezug
Musikdatei	Zwischenspeicherung auf Proxy im PotatoSystem	-

4.1.5.2 Ablauf

Der Vorgang des Kaufes eines Musikstückes durch den Kunden gliedert sich in sechs Abschnitte, welche im Folgenden kurz beschrieben werden.

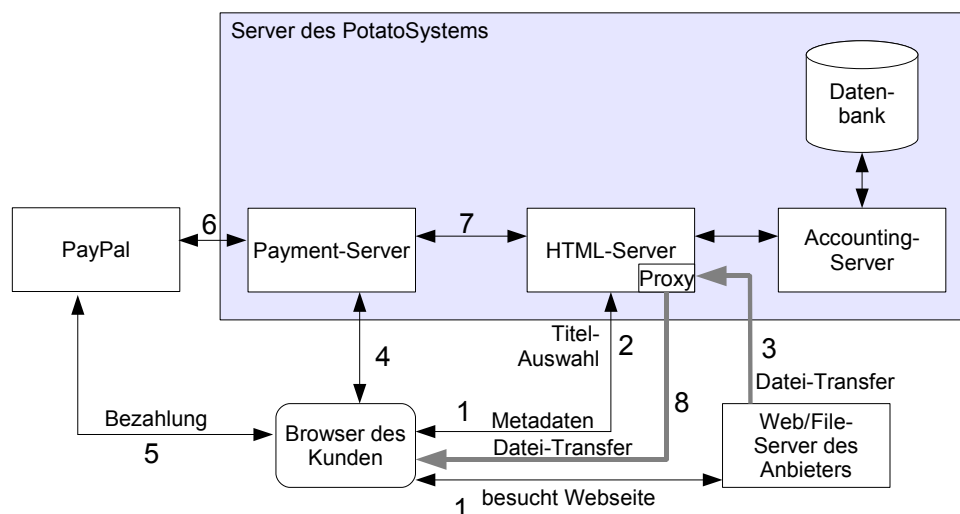


Abbildung 4.2: Schematische Darstellung eines möglichen Ablaufs (beruht auf [NG05])

1. Der Nutzer besucht zunächst die Webseite des Anbieters. Metadaten zu einzelnen Musikdateien wie Liedtitel, Name des Interpreten, etc. sind zwar in die Seite des Anbieters eingebettet, werden aber vom HTML-Server des Potatosystems geliefert (vergleiche Abb. 4.2).

2. Der Nutzer wählt eine oder mehrere Titel aus, die er kaufen möchte. Will er vom Provisionssystem Gebrauch machen, so muss er spätestens jetzt einen PotatoSystem-Account anlegen bzw. sich mit einem bereits existierenden Account anmelden.
3. Die ausgewählten Dateien werden vom File-Server des Anbieters zum Proxy transferiert.
4. Der Nutzer initiiert den Bezahlvorgang für die ausgewählten Titel beim Payment-Server, der ihn an PayPal weiterleitet.
5. Der Nutzer bezahlt bei PayPal.
6. PayPal informiert den Payment-Server des PotatoSystems über die erfolgte Zahlung.
7. Der Payment-Server informiert den HTML-Server, der daraufhin den nächsten Schritt freischaltet.
8. Der Nutzer kann die Dateien vom Proxy herunterladen und frei nutzen. Hat er sich zuvor registriert, so wird ihm zusätzlich ein personalisierter Weiterverkaufslink zur Verfügung gestellt, und auf Wunsch auch Zugang zu den Metadaten, die bereits der Anbieter in 1. verwendete.
9. Verkauft der Nutzer nun seinerseits die Dateien über seine privaten Homepage, so erkennt der Accounting-Server, wer der Weiterverkäufer ist, und berechnet entsprechend die Provision.

Der geschilderte Ablauf ist auch in Abb. 4.3 als UML-Sequenzdiagramm dargestellt, wobei sich der Nutzer dort beim PotatoSystem registriert und die zuletzt erwähnten Weiterverkaufsoptionen nicht modelliert wurden.

4.1.6 Ursprung des Szenarios

Dieses Szenario stellt das real existierende PotatoSystem dar und beruht hauptsächlich auf einem DuD-Artikel [NG05] und der Studie privacy4DRM [BGW05].

Die Akteure und ihre Beziehungen gehen, wie auch der Ablauf in Abschnitt 4.1.5.2 größtenteils aus diesen Quellen hervor, wobei PayPal als konkreter Payment-Drittanbieter gegenüber den Quellen ergänzt wurde. Die Datenflüsse und die Servicebeschreibungen erschließen sich indirekt.

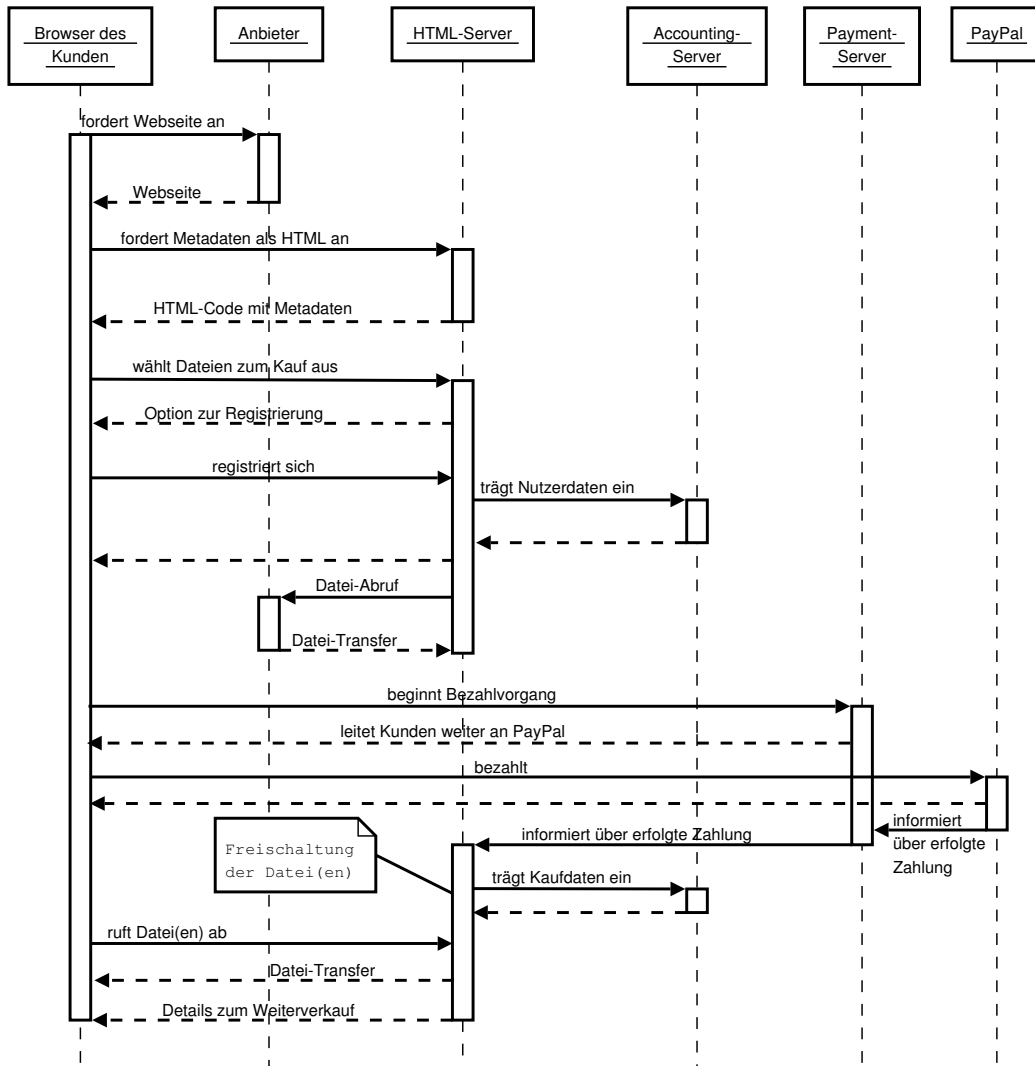


Abbildung 4.3: Ablauf als UML-Sequenzdiagramm

4.2 Hanival: Fortgeschrittenes Datenschutzszenario, Netzservices

In diesem Szenario wird die Bereitstellung eines Pakets aus Internetdienstleistungen, bestehend aus Domain, Webspace und Internetzugang, an einen Endkunden beschrieben. Dies soll aus verschiedenen Gründen (Kosten, Rahmenbedingungen) nicht von einem Unternehmen allein realisiert werden. Deshalb werden zur Bereitstellung einzelner Teile des Pakets mehrere spezialisierte Dienstleistungsanbieter benötigt, deren Dienstleistungen Hanival bündelt. Das Dienstleistungspaket kann jedoch nicht vom Endkunden direkt beauftragt werden. Das Endkundengeschäft übernimmt der Wiederverkäufer, der das Dienstleistungspaket von Hanival einkauft und dem Endkunden zur Verfügung stellt. Die Akteure Hanival, Wiederverkäufer und sowie die Dienstleistungsanbieter verschmelzen durch ihre Zusammenarbeit bei der Bereitstellung der Dienstleistungen zu einer virtuellen Organisation.

Da der Endkunde nur ein Vertragsverhältnis mit dem Wiederverkäufer besitzt, besteht die Besonderheit diese Szenarios in der Verkettung der Dienstleistungsbeziehungen. Hierdurch werden die personenbezogenen Daten des Endkunden, die auch sensible Bankdaten beinhalten, zur Erfüllung von Dienstleistungen bis zu den Dienstleistungsunternehmen weitergegeben. Dies geschieht in der Regel ohne Kenntnis des Endkunden.

Innerhalb dieses allgemeinen Szenarios entsteht insbesondere durch langfristige Verträge und eine Vielzahl von möglichen Abläufen ein sehr komplexes Geflecht aus Kommunikations- und Vertragsbeziehungen. Daher wird zur Vereinfachung lediglich der Vorgang der Beauftragung des Servicepaketes betrachtet. Dieser Vorgang beinhaltet auch die Erstzahlung der Servicegebühr des Endkunden an seinen Vertragspartner, den Wiederverkäufer.

Das in diesem Kapitel vorgestellte Szenario basiert auf dem im Rahmen des EU-Projektes Adaptive Service Grid² entwickelten „Dynamic Supply Chain Scenario for Internet Service Providers“.

4.2.1 Akteure

4.2.1.1 Endkunde

Der Endkunde ist auf das Angebot eines Leistungspaketes des Wiederverkäufers aufmerksam geworden. Dieses Paket-Angebot ist mit einer bestimmten Mindestvertragslaufzeit versehen. Es besteht aus Internetzugang und einer vom Endkunden wählbaren Internet-Domain mit dazugehörigem Webspace.

²EU-Projektnummer FP6 - 004617

Aufgrund eines attraktiven Paketpreises oder sonstiger Präferenzen des Endkunden für den Wiederverkäufer möchte er dieses Paket beim Wiederverkäufer über dessen Webseite beauftragen. Der Endkunde tritt nur mit dem Wiederverkäufer in Kontakt und hat deshalb bis auf wenige Ausnahmen keine Kenntnis der weiteren Abläufe und der beteiligten Akteure.

4.2.1.2 Wiederverkäufer

Der Wiederverkäufer kauft ein Leistungspaket von Hanival ein und verkauft es weiter an einen Endkunden. Der Kauf des Paketes ist über eine vom Wiederverkäufer betriebene Webseite möglich. Auf Grund einer direkten Gewinnerzielungsabsicht durch einen Preisaufschlag auf die von Hanival eingekauften Dienstleistungen oder der Kundenbindung möchte der Wiederverkäufer als alleiniger Vertragspartner vor dem Endkunden auftreten. Somit zahlt der Endkunde die Gebühr für das Paket direkt an den Wiederverkäufer, der als Zwischenkäufer eine Gebühr an Hanival zu zahlen hat.

4.2.1.3 Hanival

Das Unternehmen Hanival³ ist ein Internet Service Provider (ISP). Das bedeutet, es bietet ein bestimmtes Spektrum von Internetdienstleistungen an. Diese Dienstleistungen kann Hanival zum Teil selbst erbringen (Webpace) oder muss sie bei anderen Dienstleistungsanbietern einkaufen (Registrierung einer Domain, Internetzugang, Zahlungsdienstleistungen). Die Dienstleistungen bündelt Hanival zu Dienstleistungspaketen. Diese verkauft Hanival jedoch nicht an Endkunden direkt, sondern an gewerbliche Wiederverkäufer, die wiederum die Pakete an Endkunden verkaufen, beziehungsweise selbst nutzen.

Nach Abschluss eines Rahmenvertrages über standardisierte Dienstleistungspakete (Registrierung einer Domain, Webpace und Internetzugang) stellt Hanival dem Wiederverkäufer eine Schnittstelle für die Beauftragung der Pakete zur Verfügung. Darüber hinaus ermöglicht Hanival mit seiner technischen Infrastruktur dem Wiederverkäufer die Zahlungsdurchführung des Endkunden bei einem Zahlungsdienstleister zu beauftragen.

4.2.1.4 Dienstleistungsanbieter

Registrierungsstelle (Reg.) Die Registrierungsstelle ist eine Organisation, welche die Top-Level-Domains verwaltet. Insbesondere für die einzelnen

³<http://www.hanival.com>

Ländern zugeordneten Domains wurden Registrierungsstellen angelegt. Beispielsweise existiert für „.de“-Domains die DENIC⁴ und für „.at“-Domains die NIC.AT⁵. Üblicherweise können Personen bei der Registrierungsstelle nicht direkt eine Domain auf ihren Namen eintragen lassen. Hierfür müssen sie die Dienstleistung eines Registrars in Anspruch nehmen. Dieser hat im Vorfeld einen Rahmenvertrag mit der Registrierungsstelle geschlossen. Im hier beschriebenen Szenario wird aus Gründen der Vereinfachung angenommen, dass Hanival ein solcher Registrar ist.

Die Registrierungsstelle bietet als Dienstleistung (teilweise gegen Gebühr) die Abfrage des aktuellen Registrierungszustandes einer Domain, die Registrierung einer Domain, die Löschung einer Domain und die Änderung der Domaindaten (Domaininhaber, technischer und administrativer Ansprechpartner, etc.) an.

Hanival Webpace (Ha-Wsp) Dieser Dienstleistungsanbieter stellt Webpace mit Hilfe einer Infrastruktur aus administrierten Webservern und Datenverbindungen bereit. Der Endkunde bekommt Zugriff auf den Server, so dass er eigene Inhalte, bspw. html-Seiten, hochladen kann. Die Registrierungsstelle kann vom Endkunden oder einer von ihm beauftragten Person angewiesen werden, die Domain auf einen solchen, an das Internet angebotenen Webserver zu leiten. Hierdurch sind die hochgeladenen Inhalte über das Internet unter der Domain des Endkunden abrufbar.

Hanival Webpace ist in diesem Szenario eine Organisationseinheit von Hanival und somit formal mit Hanival identisch. Er bietet Hanival die Bereitstellung von Webpace als interne Dienstleistung an.

Internetzugangsanbieter (IZA) Die Dienstleistung des Internetzugangsanbieters ist die Bereitstellung eines Breitbandzugangs an einer bestimmten geografischen Adresse für private oder gewerbliche Kunden. Der Zugang zum Endkunden wird über eine Funk- oder Kabelverbindung realisiert, in Deutschland typischerweise über die Telefonleitung per DSL. Die Bereitstellung einer DSL-Leitung und deren Anbindung an das Internet über ein Backbone kann über ein Geflecht von Leistungsbeziehungen erfolgen, das für dieses Szenario jedoch keine Beachtung findet.

Der Internetzugangsanbieter bietet an, im Vorfeld eine Auskunft über die voraussichtliche Umsetzbarkeit eines Internetzugangs für eine spezielle geografische Adresse einzuholen. Dies ist notwendig, da er die Bereitstellung des Zuganges nicht für alle Adressen garantieren kann.

⁴<http://www.denic.de>

⁵<http://www.nic.at>

Zahlungsdienstleister (ZDL) Es existiert eine große Anzahl von Zahlungsdienstleistern auf dem deutschen und internationalen Markt, die anbieten, eine Zahlung zwischen zwei Parteien abzuwickeln. Hierbei reicht die Bandbreite vom klassischen Kreditkartenanbieter bis zum Micropayment. Ein immer noch in der Praxis weit verbreitetes Zahlungsverfahren ist das Lastschriftverfahren in seiner speziellen Ausprägung des Einzugsermächtigungsverfahrens. Es bietet für den Verkäufer den Vorteil, dass hiermit auch langfristige Zahlungsbeziehungen, wie sie in Dauerschuldverhältnissen üblich sind, mit geringem Aufwand ermöglicht werden. Für den Käufer gilt es zwischen der Unkompliziertheit der Preisgabe seiner Bankdaten und Sicherheitsbedenken darüber, was mit diesen Daten geschieht abzuwägen.

Damit das Lastschriftverfahren zur Anwendung kommen kann, müssen sowohl der Zahlungsempfänger als auch der Zahlungspflichtige ein Konto bei beliebigen Banken besitzen. Es kann davon ausgegangen werden, dass jede Bank an das Lastschriftabkommen (LSA) gebunden ist. Der Ablauf des Lastschriftverfahrens lässt sich wie folgt zusammenfassen. Der Zahlungsempfänger (Wiederverkäufer) erhält vom Zahlungspflichtigen (Endkunde) dessen Kontodaten und Ermächtigung des Lastschrifteinzuges über den vereinbarten Betrag. Diese Daten gibt der Zahlungsempfänger an seinen Zahlungsdienstleister (in den meisten Fällen eine Bank) weiter. Dieser setzt sich mit der Bank des Zahlungspflichtigen in Verbindung und veranlasst die Zahlung vom angegebenen Konto des Zahlungspflichtigen auf das Konto des Zahlungsempfängers. Zur Finanzierung seiner Dienstleistung erhebt der Zahlungsdienstleister vom Zahlungsempfänger eine Gebühr.

Obgleich lediglich ein Vertrag zwischen dem Zahlungsempfänger und seinem Zahlungsdienstleister besteht, kann der Zahlungsempfänger Hanival beauftragen, die Lastschrift technisch an den Zahlungsdienstleister zu übermitteln.

4.2.2 Beziehungen der Akteure

Zur besseren Veranschaulichung sind die für dieses Szenario relevanten Beziehungen zwischen den beteiligten Akteuren in Abbildung 4.4 zusammengefasst.

Hierbei sind die einzelnen Beziehungen definiert als Vertrag:

1. über die Bereitstellung des Servicepaketes und die Zahlung der Gebühr zwischen Endkunde und Wiederverkäufer.
2. zwischen dem Endkunden und seiner Hausbank über die Führung eines Girokontos.

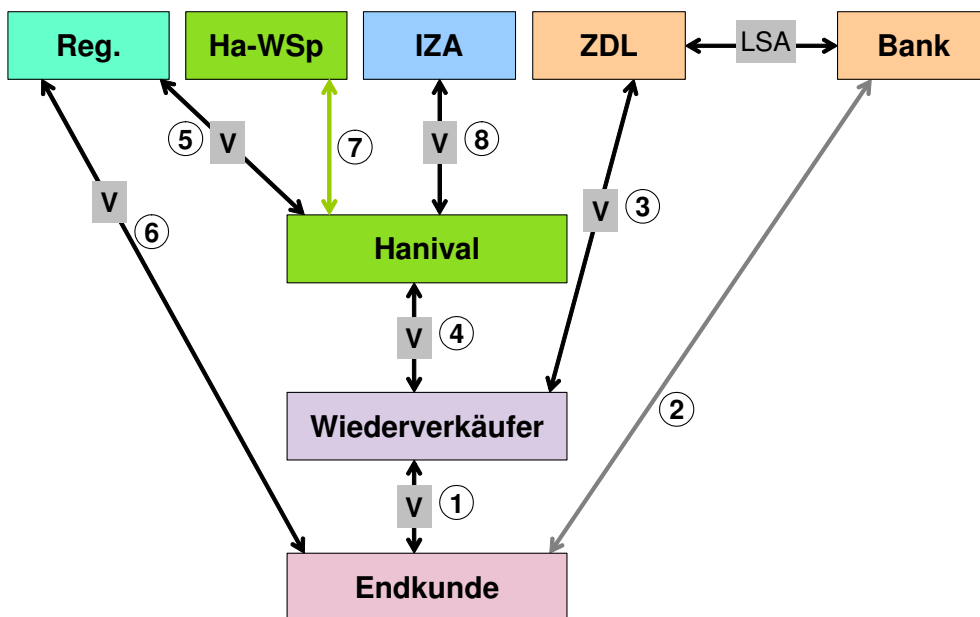


Abbildung 4.4: Beziehungen der Akteure im Hanival-Szenario

3. des Wiederverkäufers mit seinem Zahlungsdienstleister über die Führung eines Kontos und die Erteilung von Lastschriftinzügen.
4. zwischen Wiederverkäufer und Hanival über die Bereitstellung des Servicepaketes und die Weiterleitung der Erteilung von Lastschriftinzügen.
5. von Hanival mit der Registrierungsstelle, wodurch Hanival als Registrar auftreten kann.
6. des Endkunden mit der Registrierungsstelle, der den Endkunden als Inhaber seiner Domain ausweist.
7. interner Art, zwischen Hanival und seiner Organisationseinheit Hanival Webspace über die Bereitstellung von Webspace.
8. über die Bereitstellung eines Internetzugangs am Wohnort des Endkunden zwischen Hanival und dem Internetzugangsanbieter.

4.2.3 Datenflüsse zwischen den Akteuren

Zur Veranschaulichung sind die in diesem Szenario relevanten Datenflüsse, speziell die Weitergabe der Kundendaten, in Abbildung 4.5 zusammengefasst. Es können die folgenden fünf Datenflüsse identifiziert werden:

1. Der Endkunde teilt dem Wiederverkäufer seine Kontaktdaten (Kundenname, Kundenadresse, Telefonnummer) und seine Wünsche über die Ausgestaltung des von ihm bestellten Paketes (Domainname, Größe des Webspace, DSL-Geschwindigkeit) mit. Darüber hinaus übermittelt er dem Wiederverkäufer seine Bankdaten (Kontonummer, Bankleitzahl, Name der Bank), damit dieser einen Lastschriftauftrag über die Paketgebühr erteilen kann.
2. Die vom Kunden erhaltenen Daten gibt der Wiederverkäufer an Hanival weiter, zur Erfüllung des Kundenauftrages.
3. Die für eine Registrierung einer Web-Domain nötigen Daten des Kunden (Domainname, Kundenname, Kundenadresse) werden von Hanival an die Registrierungsstelle übermittelt.
4. Hanival-Webspace erhält von Hanival die Größe des vom Kunden gewünschten Webspace um diesen bereitzustellen.
5. Hanival übermittelt dem Internet-Zugangsanbieter den Kundennamen und die Kundenadresse, damit dieser den Internetzugang für den Kunden bereitstellen kann.
6. Der Zahlungsdienstleister erhält von Hanival die Kundenkontodaten (Kundenname, Kontonummer, Bankleitzahl, Name der Bank) zur Durchführung des Lastschriftauftrages.

4.2.4 Verantwortlichkeit

Wie die Beschreibung der Datenflüsse zwischen den Akteuren gezeigt hat, werden in diesem Szenario personenbezogene Daten der Endkunden nicht nur von deren Vertragspartner, dem Wiederverkäufer, sondern auch von weiteren Stellen, nämlich Hanival, der Registrierungsstelle, dem Internetzugangsanbieter und dem Zahlungsdienstleister verwendet. Da keine besonderen vertraglichen Vereinbarungen existieren, sind die genannten Stellen auch jeweils für die von ihnen durchgeführte Datenverarbeitung verantwortlich. Keine eigenständige verantwortliche Stelle ist hingegen Hanival Webspace, weil es sich bei diesem lediglich um eine Organisationseinheit von Hanival handelt. Verantwortlich für die von Hanival Webspace durchgeführte Datenverarbeitung ist damit Hanival.

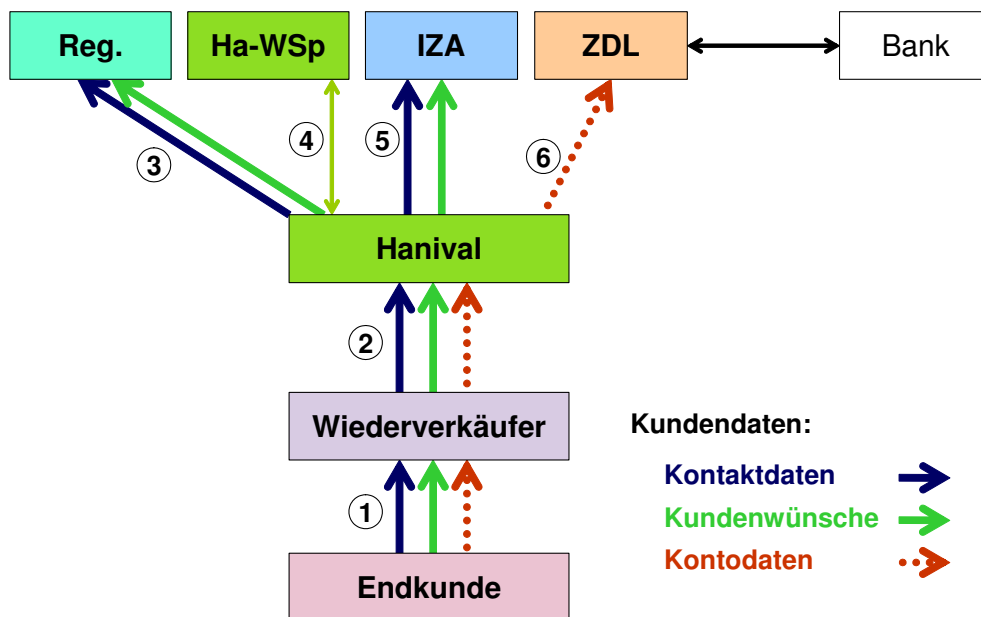


Abbildung 4.5: Datenflüsse im Hanival-Szenario

4.2.5 Service-orientierte Architektur

In diesem Abschnitt wird eine mögliche Service-orientierte Architektur (SOA) für dieses Szenario beschrieben.

Hierin besitzen alle Akteure eine eigene Infrastruktur zum Betreiben ihrer Services. Diese Infrastrukturen sind an ein öffentliches Netzwerk angebunden, so dass Aufrufen von Services anderer Infrastrukturen und Akteure möglich ist. Es ist anzumerken, dass im hier vorgestellten Detaillierungsgrad des Szenarios sicherheitsrelevante Aspekte, wie Vertraulichkeit, Integrität oder Authentizität, nicht betrachtet werden. Diese Sicherheitsfunktionalitäten können von den Infrastrukturen geleistet werden.

4.2.5.1 Services

Für dieses Szenario wurden die folgenden Services identifiziert, die auf den Infrastrukturen der jeweiligen Akteure zur Verfügung stehen. Die Services sind unter Angabe ihrer Input- und Outputdaten in Abbildung 4.6 zusammengefasst.

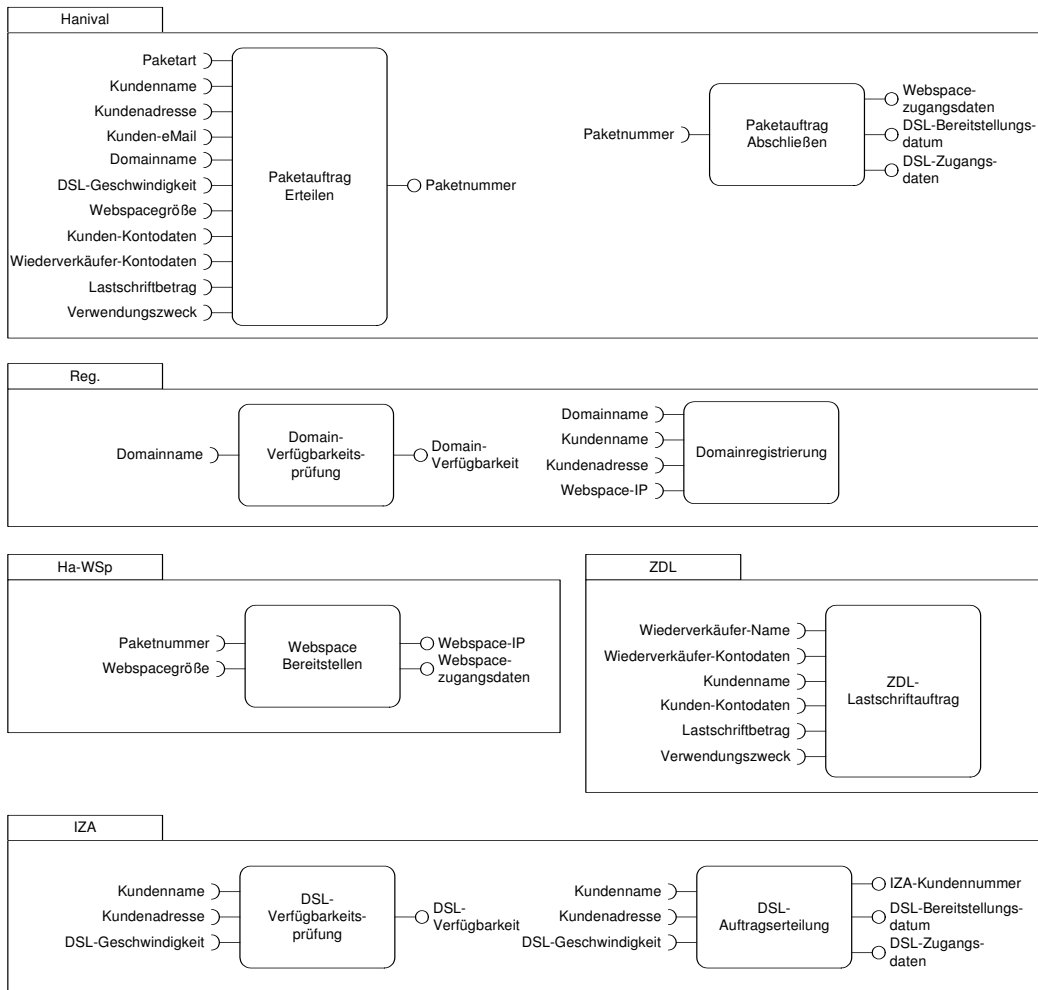


Abbildung 4.6: Relevante Services der Akteure im Hanival-Szenario

Hanival

PaketauftragErteilen Dies ist der zentrale Service, mit dem der Wiederverkäufer ein Servicepaket bei Hanival bestellen kann. Hierfür sind seine Daten sowie die Daten des Kunden notwendig. Nach dem Aufruf beginnt der Service bei den einzelnen Dienstleistungsanbietern über deren Services zu ermitteln, ob sie die vom Kunden gewünschte Konfiguration des Servicepaketes erbringen können. Ist dies der Fall, wird der Lastschriftauftrag an den ZDL weiter gegeben.

Eingabedaten

Datum	Zweck	Betroffener	Personenbezug	Beispiel
Kundenname	Auftragsverwaltung, Weitergabe an Reg., IZA und ZDL	Endkunde	Endkunde	Max Müller
Kundenadresse	Auftragsverwaltung, Weitergabe an Reg., IZA und ZDL	Endkunde	Endkunde	Postweg 2, 56072 Koblenz
Kunden-E-Mail	Auftragsverwaltung, Weitergabe an Reg.	Endkunde	Endkunde	mmueller@md-e.com
Domainname	Auftragsverwaltung, Weitergabe an Reg.	Endkunde	Endkunde	mmueller.de
DSL-Geschwindigkeit	Auftragsverwaltung, Weitergabe an IZA	Endkunde	Endkunde	2000 Mbit
Webespacegröße	Auftragsverwaltung, Weitergabe an Ha-WSp	Endkunde	Endkunde	2 GByte
Kunden-Kontodaten	Weitergabe an ZDL	Endkunde	Endkunde	K-Nr.: 37628, BLZ: 48028926, USW direct-Bank
Wiederverkäufer-Kontodaten	Weitergabe an ZDL	Wiederverkäufer	nein	K-Nr.: 48587, BLZ: 43892754, DWN-Bank
Lastschriftbetrag	Weitergabe an ZDL	Wiederverkäufer	Endkunde	29 Euro
Verwendungszweck	Durchführung des Lastschriftauftrags	Wiederverkäufer	nein	Einrichtungsgebühr Web-Paket

Ausgabedaten

Datum	Zweck	Betroffener	Personenbezug	Beispiel
Paketnummer		Hanival	nein	2007298303

PaketauftragAbschließen Falls die Zahlung beim Wiederverkäufer eingegangen ist, kann er durch Aufruf dieses Services Hanival anweisen, die Dienstleistungen der Anbieter verbindlich zu bestellen.

Eingabedaten

Datum	Zweck	Betroffener	Personenbezug	Beispiel
Paketnummer	Zuordnung zu erteiltem Paketauftrag	Hanival	nein	2007298303

Ausgabedaten

Datum	Zweck	Betroffener	Personenbezug	Beispiel
Webspacezugangsdaten		Ha-WSp	nein	User: mmeuller, PW: asdf1234
DSL-Bereitstellungsdatum		IZA	nein	01.02.2003
DSL-Zugangsdaten		IZA	nein	User: mueller, PW: jklmQ

Reg.

Domain-Verfügbarkeitsprüfung Hiermit kann ermittelt werden, ob eine angegebene Domain noch verfügbar und somit auf eine beliebige Person bei der Registrierungsstelle registrierbar ist.

Eingabedaten

Datum	Zweck	Betroffener	Personenbezug	Beispiel
Domainname	Prüfung der Domain	Endkunde	Endkunde	mmueller.de

Ausgabedaten

Datum	Zweck	Betroffener	Personenbezug	Beispiel
Domain-Verfügbarkeit		Reg.	nein	verfügbar

Domainregistrierung Dieser Service steht nur Registraren zur Verfügung. Unter Angabe des Domainnamens, administrativer Daten und den Daten der Person auf welche, die Domain zu registrieren ist, kann eine Domain verbindlich registriert werden.

Eingabedaten

Datum	Zweck	Betroffener	Personenbezug	Beispiel
Domainname	Registrierung der Domain	Endkunde	Endkunde	mmueller.de
Kundenname	Registrierung der Domain	Endkunde	Endkunde	Max Müller
Kundenadresse	Registrierung der Domain	Endkunde	Endkunde	Postweg 2, 56072 Koblenz
Webpace-IP	Verknüpfung der Domain mit dem Webpace	Ha-WSp	nein	131.38.29.104

Ha-Wsp

WebpaceBereitstellen Über diesen Service kann Hanival seine Abteilung Hanival-Webpace anweisen Webpace einer angebenene Größe über einen Server bereitzustellen. Der Service gibt die Zugriffsdaten an Hanival zurück.

Eingabedaten

Datum	Zweck	Betroffener	Personenbezug	Beispiel
Paketnummer	Verwaltung des Webpace	Hanival	nein	2007298303
Webpacegröße	Einrichtung des Webpace	Endkunde	Endkunde	2 GByte

Ausgabedaten

Datum	Zweck	Betroffener	Personenbezug	Beispiel
Webpace-IP		Ha-WSp	nein	131.38.29.104
Webpacezugangsdaten		Ha-WSp	nein	User: mmeuller, PW: asdf1234

ZDL

ZDL-Lastschriftauftrag Hierüber bietet der ZDL einem Unternehmen an, einen Lastschriftauftrag entgegenzunehmen und mit Hilfe der an diesem Auftrag beteiligten Banken durchzuführen.

Eingabedaten

Datum	Zweck	Betroffener	Personenbezug	Beispiel
Wiederverkäufer-Name	Durchführung des Lastschriftauftrags	Wiederverkäufer	nein	IS-Tel GmbH
Wiederverkäufer-Kontodaten	Durchführung des Lastschriftauftrags	Wiederverkäufer	nein	K-Nr.: 48587, BLZ: 43892754, DWN-Bank
Kundenname	Durchführung des Lastschriftauftrags	Endkunde	Endkunde	Max Müller
Kunden-Kontodaten	Durchführung des Lastschriftauftrags	Endkunde	Endkunde	K-Nr.: 37628, BLZ: 48028926, USW directbank
Lastschriftbetrag	Durchführung des Lastschriftauftrags	Wiederverkäufer	nein	29 Euro
Verwendungszweck	Durchführung des Lastschriftauftrags	Wiederverkäufer	nein	Einrichtungsgelühr Web-Paket

IZA

DSL-Verfügbarkeitsprüfung Mit Hilfe dieses Services kann Hanival feststellen, ob der IZA an der vom Kunden angegebene Adresse eine DSL-Leitung bereitstellen kann.

Eingabedaten

Datum	Zweck	Betroffener	Personenbezug	Beispiel
Kundenname	DSL-Verfügbarkeitsprüfung	Endkunde	Endkunde	Max Müller
Kundenadresse	DSL-Verfügbarkeitsprüfung	Endkunde	Endkunde	Postweg 2, 56072 Koblenz
DSL-Geschwindigkeit	DSL-Verfügbarkeitsprüfung	Endkunde	Endkunde	2000 Mbit

Ausgabedaten

Datum	Zweck	Betroffener	Personenbezug	Beispiel
DSL-Verfügbarkeit		IZA	nein	verfügbar

DSL-Auftragserteilung Dieser Service dient Hanival dazu, den Auftrag für die Bereitstellung eines DSL-Zugangs für einen Kunden an einer bestimmten Adresse verbindlich zu erteilen.

Eingabedaten

Datum	Zweck	Betroffener	Personenbezug	Beispiel
Kundenname	DSL-Zugang freischalten	Endkunde	Endkunde	Max Müller
Kundenadresse	DSL-Zugang freischalten	Endkunde	Endkunde	Postweg 2, 56072 Koblenz
DSL-Geschwindigkeit	DSL-Zugang freischalten	Endkunde	Endkunde	2000 Mbit

Ausgabedaten

Datum	Zweck	Betroffener	Personenbezug	Beispiel
IZA-Kundennummer		IZA	nein	26599
DSL-Bereitstellungsdatum		IZA	nein	01.02.2003
DSL-Zugangsdaten		IZA	nein	User: mueller, PW: jklmQ

4.2.5.2 Ablauf

Der Vorgang der Beauftragung eines Servicepaketes gliedert sich in fünf Phasen, welche im Folgenden beschrieben werden.

1. Der Endkunde wählt auf den Seiten des Wiederverkäufers ein Servicepaket, bestehend aus Domain, Webspace und DSL-Internetzugang. Dieses bestellt er unter Angabe seiner Kundendaten (Name, Kontaktdaten, etc.), Kontodaten und seiner speziellen Kundenwünsche über die Ausgestaltung des Servicepaketes (Domainname, Größe des Webspace, DSL-Geschwindigkeit) beim Wiederverkäufer über dessen Webseite. Da dieser Vorgang ausschließlich über die Webseite des Wiederverkäufers abgewickelt wird, sind keine Services involviert.
2. Der Wiederverkäufer beauftragt Hanival mit der Bereitstellung des Servicepaketes, unter Angabe der Kundendaten und Kundenwünsche. Darüber hinaus teilt der Wiederverkäufer Hanival die Kontodaten des Kunden mit, um die Buchung des Paketpreises vom Kundenkonto auf das Konto des Wiederverkäufers vorzunehmen. Dieser Schritt erfolgt durch den Aufruf des Services `PaketauftragErteilen` vom Wiederverkäufer.

3. Hanival holt auf Basis der Kundendaten und Kundenwünsche die Angebote der Dienstleistungsanbieter Registrierungsstelle (Service: Domain-Verfügbarkeitsprüfung) und Internetzugangsanbieter (Service: DSL-Verfügbarkeitsprüfung) ein. Können diese die vom Endkunden gewünschte Dienstleistung (Domain noch verfügbar, DSL-Zugang am Wohnort des Endkunden möglich) erbringen, so stellt Hanival den Webspaces bereit (Service: Webspacesbereitstellung) und fährt mit den nächsten Schritten fort. Ist die Bereitstellung der Dienste aus irgendeinem Grund nicht möglich, bricht Hanival den Vorgang ab, und meldet dies dem Wiederverkäufer, welcher wiederum den Kunden über den Abbruch des Auftrages informiert.
4. Hanival weist den Zahlungsdienstleister an, die Paketgebühr vom Kundenkonto auf das Konto des Wiederverkäufers zu überweisen. Dies geschieht durch den Aufruf des Services Lastschriftauftrag.
5. Sobald die Zahlung des Endkunden auf dem Konto des Wiederverkäufers eingegangen ist, benachrichtigt dieser Hanival durch Aufruf des Services PaketauftragAbschließen. Hierdurch erteilt Hanival die Aufträge an die Registrierungsstelle (Service Domainregistrierung) und den Internetzugangsanbieter (Service DSL-Auftragserteilung). Der Endkunde erhält vom Wiederverkäufer eine Auftragsbestätigung und seine Zugangsdaten für Webspaces und DSL.

Das Zusammenwirken der an diesem Ablauf beteiligten Services ist in Form eines Sequenzdiagramms in Abbildung 4.7 dargestellt. Hierbei sind den Serviceaufrufen die entsprechenden Phasen zugeordnet.

4.2.6 Ursprung des Szenarios

Dieses Szenario basiert in der in diesem Kapitel beschriebenen Form zu großen Teilen auf einem Arbeitsbericht [SMS⁺06] des von der Europäischen Union geförderten Projektes Adaptive Services Grid (ASG)⁶.

Insbesondere der Aufbau der VO (vgl. Abbildung 4.4) lehnt sich sehr stark an das ASG-Szenario an. Auch die Beschreibung der Akteure Hanival, Zahlungsdienstleister und Registrierungsstelle orientiert sich an dieser Vorlage. Hanival selbst ist ein reales Unternehmen⁷, dessen geschäftliche Tätigkeit dieses Szenario prinzipiell beinhaltet. Die Akteure Hanival-Webspaces und Internetzugangsanbieter sind zur Vervollständigung dieses Szenarios konstruiert worden.

⁶Fördernummer: FP6-IST-004617, <http://www.asg-platform.org>

⁷<http://www.hanival.net/>

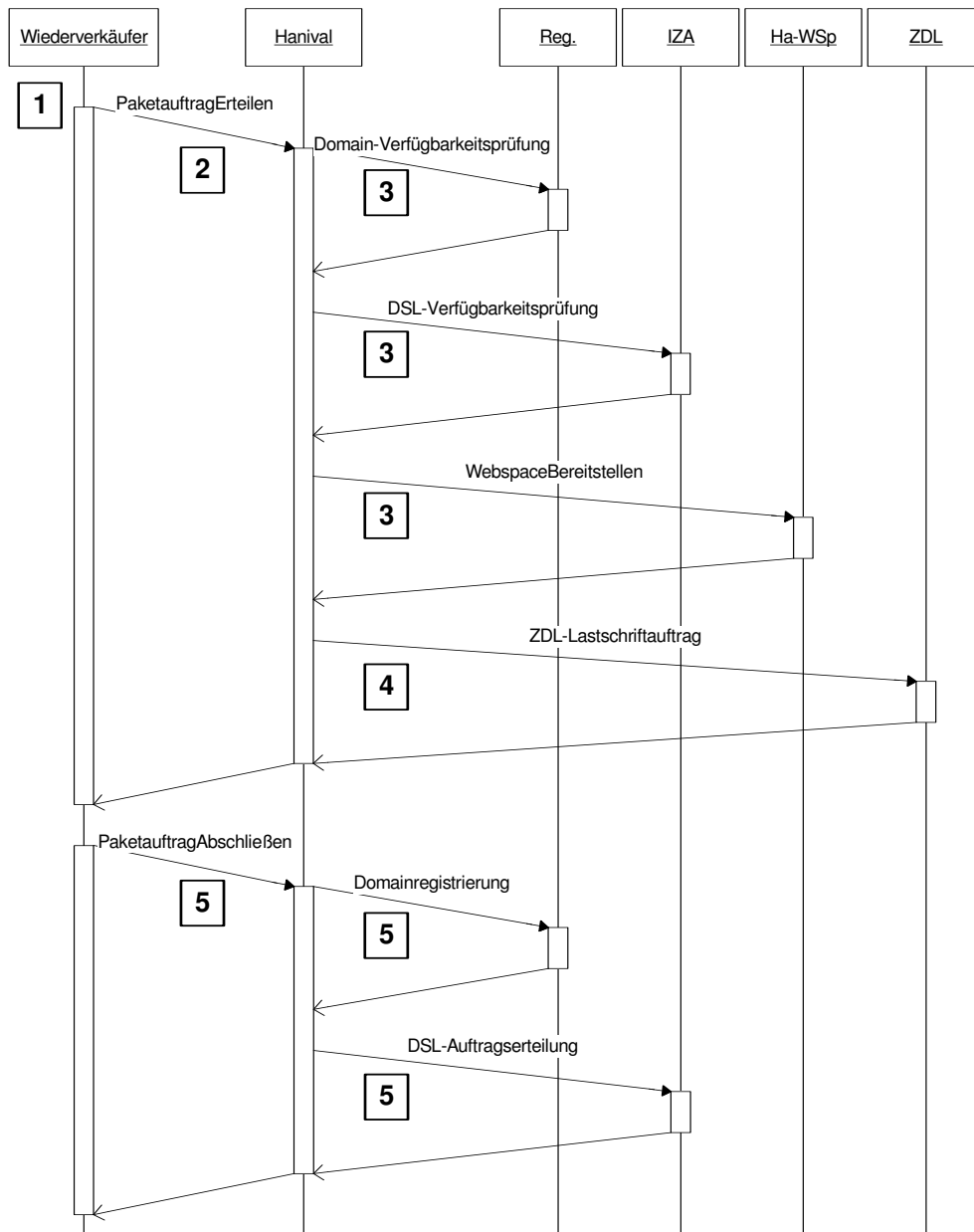


Abbildung 4.7: Ablauf des Hanival-Szenarios als Sequenzdiagramm

Die hier beschriebenen vertraglichen Beziehungen sind für dieses Szenario weitgehend konstruiert worden. Eine Ausnahme bilden die Beziehungen zwischen Hanival und Registrierungsstelle bzw. Zahlungsdienstleister. Ihre Beschreibung basiert auf allgemein zugänglichen Vorschriften und Regelungen zu Domainregistrierung und zum Einzugsermächtigungsverfahren.

Die in diesem Szenario vorgestellte SOA orientiert sich am ASG-Szenario. Die Anzahl der Services und deren Komplexität wurde jedoch reduziert; für die nicht im Ursprungsszenario berücksichtigten Akteure wurden die jeweiligen Services konstruiert.

4.3 Amazon Mechanical Turk: Länderübergreifendes Datenschutzszenario, Verantwortlichkeitsproblematik und Einbezug privater Endanbieter

Amazon bietet verschiedene Web Services an: neben einer öffentlichen, frei zugänglichen Schnittstelle für den Produktkatalog existieren auch einige kostenpflichtige Dienstleistungen, die mit dem Versandhandel nichts zu tun haben⁸, und die auf Unternehmen als Kunden abzielen; so kann man z.B. Rechenleistung oder Speicherplatz mieten.

Unter dem Namen „Amazon Mechanical Turk“ (AMT) bietet Amazon auch einen Dienst an, der (etwas humoristisch) als „Artificial Artificial Intelligence“ bezeichnet wird⁹:

- Aufgaben, die klassischerweise nicht oder nur schlecht von Computern gelöst werden können (z.B. „Beschreibe, was auf diesem Foto zu sehen ist“ oder „Übertrage dieses gesprochene Interview in einen geschriebenen Text“), für Menschen jedoch trivial oder zumindest einfach sind, werden aus eben diesem Grund auch nicht durch Computer bearbeitet, sondern an menschliche Arbeiter weitergereicht. Amazon bezeichnet diese Aufgaben als HITs („Human Intelligence Task“).
- Pro erledigtem HIT bekommen die Arbeiter vom Auftraggeber einen (zumeist sehr geringen) Geldbetrag.

⁸Für einen Überblick über alle angebotenen Web Services siehe <http://aws.amazon.com/>.

⁹Eine detaillierte Beschreibung sowie eine Erläuterung zur Herkunft des Namens finden sich unter <http://www.mturk.com/mturk/help?helpPage=whatIs>.

- Ein Arbeiter kann in speziellen Tests beweisen, dass er die nötige Qualifikation für bestimmte Aufgaben hat. Zudem kann er sich durch das erfolgreiche Bearbeiten von HITs eine Reputation aufbauen und dadurch auch anspruchsvollere HITs bekommen.
- Aus der Sicht des Auftraggebers gestaltet sich der Auftrag sehr einfach: Er erstellt zunächst eine allgemeine Beschreibung der Aufgabe, die Amazon benutzt, um für Arbeiter zu werben. Danach kann er wie in einem „normalen“ Web Service-Aufruf die Eingabedaten (also z.B. Fotos) an Amazon senden und bekommt nach einiger Zeit das Ergebnis zurückgeliefert.
- Aus Abrechnungsgründen können zur Zeit nur in den USA sesshafte Unternehmen Aufträge erteilen, die Arbeiter jedoch können weltweit an jedem Ort arbeiten, an dem sie Zugang zum Internet haben.

Schon kurz nach dem Start des Mechanical Turk wurde das Übersetzungsunternehmen „von Kempelen“ gegründet, das seine Dienstleistungen fast vollständig auf AMT aufbaut¹⁰:

- Das Übersetzen von Texten und das Überführen von gesprochenen in geschriebene bzw. von geschriebenen in gesprochene Texte wird nicht von Angestellten von von Kempelen erledigt, sondern von AMT-Arbeitern.
- AMT-Arbeiter werden in verschiedene Qualifikationsstufen unterteilt, wobei Arbeiter höherer Stufen die Ergebnisse von Arbeitern niedriger Stufen kontrollieren, bevor sie an den Auftraggeber zurückgehen.

Zu Amazon und von Kempelen kommt in diesem Szenario ein Software-Hersteller (im Folgenden „Zettasoft“ genannt) hinzu, der seinen Sitz in den USA hat und seine Produkte auch in vielen Ländern vertreibt, in denen andere Sprachen gesprochen werden. Support-Anfragen von Kunden, die auf Englisch gestellt werden, können direkt durch das eigene Personal beantwortet werden. Zusätzlich will Zettasoft aber auch Anfragen beantworten, die in anderen Sprachen gestellt werden; mit der Übersetzung der nicht-englischsprachigen Anfragen wird von Kempelen beauftragt.

¹⁰vgl. hierzu auch <http://www.vonkempelen.com/>

4.3.1 Akteure

4.3.1.1 Amazon

Amazon macht die HITs von von Kempelen auf einer speziellen Webseite publik, welche von AMT-Arbeitern frequentiert wird¹¹. Werden die HITs angenommen, so setzt Amazon die Eingabedaten, die von Kempelen beim Aufruf des AMT Web Services übergeben hat, in ein „benutzerfreundliches“ Format um, das von den Arbeitern leicht bearbeitet werden kann (z.B. eine Webseite, die neben dem fremdsprachigen Text ein Eingabefeld für die Übersetzung enthält). Die Ergebnisse der HITs wiederum sendet Amazon als Klartext an von Kempelen.

Wie die HITs geht auch die Bezahlung nur mittelbar von von Kempelen über Amazon an die Arbeiter. Einen Teil des vom Auftraggeber bezahlten Geldes behält Amazon als Provision.

4.3.1.2 AMT-Arbeiter

Die Arbeiter bearbeiten die von Amazon vergebenen HITs. Die Bezahlung ist hierbei so gering, dass praktisch niemand durch das Arbeiten für AMT ernsthaft Geld verdienen oder gar seinen Lebensunterhalt finanzieren kann; stattdessen gibt es viele Personen, die die HITs aus Spaß und zum Zeitvertreib bearbeiten.

4.3.1.3 von Kempelen

von Kempelen fertigt u.a. Übersetzungen als Auftragsarbeiten an. Hierfür muss von Kempelen kein Stammpersonal einstellen (das Fixkosten verursacht), sondern kann bei Bedarf auf die AMT-Arbeiter zugreifen und bezahlt diese nur für die erbrachte Leistung. Durch die große Menge von Arbeitern können auch große Mengen von Aufträgen zeitnah bearbeitet werden. Die niedrigen Löhne führen überdies dazu, dass von Kempelen seine Dienstleistungen wesentlich preiswerter anbieten kann als seine Konkurrenten. Schließlich profitiert es als junges Unternehmen auch maßgeblich vom Medienrummel, der um die Amazon Web Services gemacht wird, und von der Werbung, die Amazon selbst mit ihm als Kunden macht.

4.3.1.4 Zettasoft

Zettasoft hat zwar seinen Firmensitz in den USA, will für seine internationalen Kunden aber auch Support-Anfragen in anderen Sprachen als Englisch

¹¹vgl. <http://www.mturk.com/mturk/findhits?match=false>

beantworten. Hierdurch kann es sich von Konkurrenten abheben, die diesen Service nicht anbieten bzw. sich auch gegen größere Unternehmen behaupten, die Ableger in mehreren Ländern haben.

4.3.1.5 Kunde

Der Kunde hat ein Produkt von Zettasoft gekauft. Bei der Verwendung der Software treten Probleme auf, so dass der Kunde sich an Zettasoft wendet. Da seine Englischkenntnisse nicht ausreichen, um das Problem zu beschreiben, formuliert er die Anfrage in seiner Muttersprache (z.B. Deutsch), und erwartet möglichst schnell eine ebenfalls deutschsprachige Antwort.

4.3.1.6 Variante

In der bislang geschilderten Grundkonstellation dieses Szenarios werden an höchstens zwei Stellen durch Serviceaufrufe Landesgrenzen übertreten, da die drei beteiligten Unternehmen sich alle in den USA befinden. Denkbar wäre jedoch auch, dass die Unternehmen ihren Sitz in unterschiedlichen Ländern haben; dies gilt vor allem für Zettasoft, aber auch für AMT und von Kempelen (z.B. in der Gestalt von Tochterfirmen). Im Rahmen der rechtlichen Szenarienanalyse wird deshalb neben der Grundkonstellation auch noch eine Variante untersucht: Diese weicht insoweit vom Ausgangsszenario ab, als sich der Sitz von Zettasoft nicht in den USA, sondern in Deutschland befindet.

Führt man sich im Übrigen beispielsweise eine Konstellation vor Augen, in der Zettasoft sich in Asien befindet, von Kempelen in Europa und AMT nach wie vor in den USA, so sind damit für die verschiedenen Akteure ganz unterschiedliche Rechtslagen relevant. Die Konsequenzen dieser unterschiedlichen rechtlichen Situationen für deren Zusammenarbeit bzw. für die Datenschutzrechte des Kunden sind u.U. schwer zu überblicken.

4.3.2 Beziehungen der Akteure

In Abb. 4.8 ist dargestellt, welche Akteure zueinander Beziehungen haben. Welcher Art diese Beziehungen sind, wird im Folgenden erläutert:

1. Der Kunde hat mit Zettasoft einen Support-Vertrag, der Zettasoft verpflichtet, auch Anfragen zu beantworten, die in einigen anderen Sprachen als Englisch gestellt wurden.
2. von Kempelen wird von Zettasoft pro geleistete Übersetzung bezahlt und sichert seinerseits eine gewisse Qualität der Übersetzung zu.

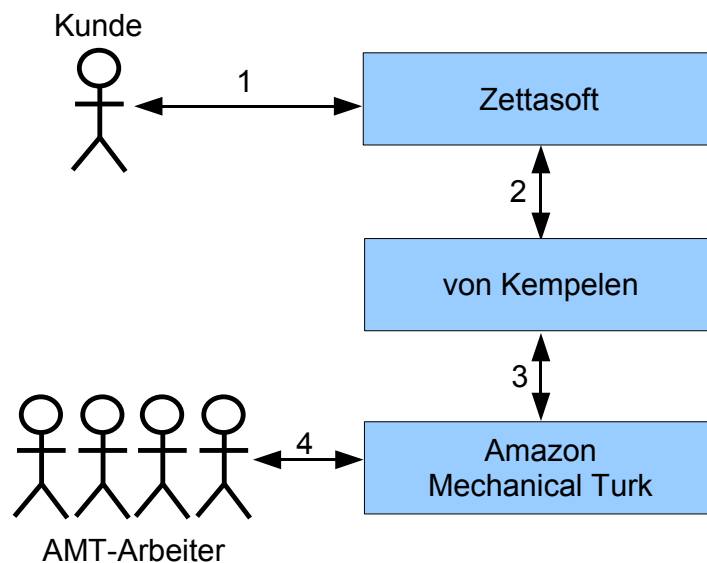


Abbildung 4.8: Beziehungen der Akteure im AMT-Szenario

3. von Kempelen baut seine Dienstleistungen zu einem Großteil auf AMT auf. Da die AMT-Arbeiter nicht direkt durch von Kempelen bezahlt werden, wird der Lohn mittelbar über AMT entrichtet, wobei Amazon einen Anteil davon einbehält. Im Gegenzug entbindet AMT von Kempelen von der Verpflichtung, geeignete Arbeiter zu finden und die HITs zu verwalten.
4. Die Verpflichtungen der Arbeiter gegenüber AMT sind nur in geringem Maße vertraglich abgesichert. Da Amazon solche Verpflichtungen angesichts der großen Zahl der Arbeiter auch nur schlecht durchsetzen könnte, ist das Arbeiter-AMT-Verhältnis unmittelbarer: Ein Arbeiter wird nur dann für seine Arbeit bezahlt, wenn der Auftraggeber (im konkreten Fall von Kempelen) mit dem Ergebnis zufrieden ist. Bei konstant schlechter Leistung muss der Arbeiter überdies mit einer schlechten Bewertung im AMT-eigenen Reputationssystem rechnen.

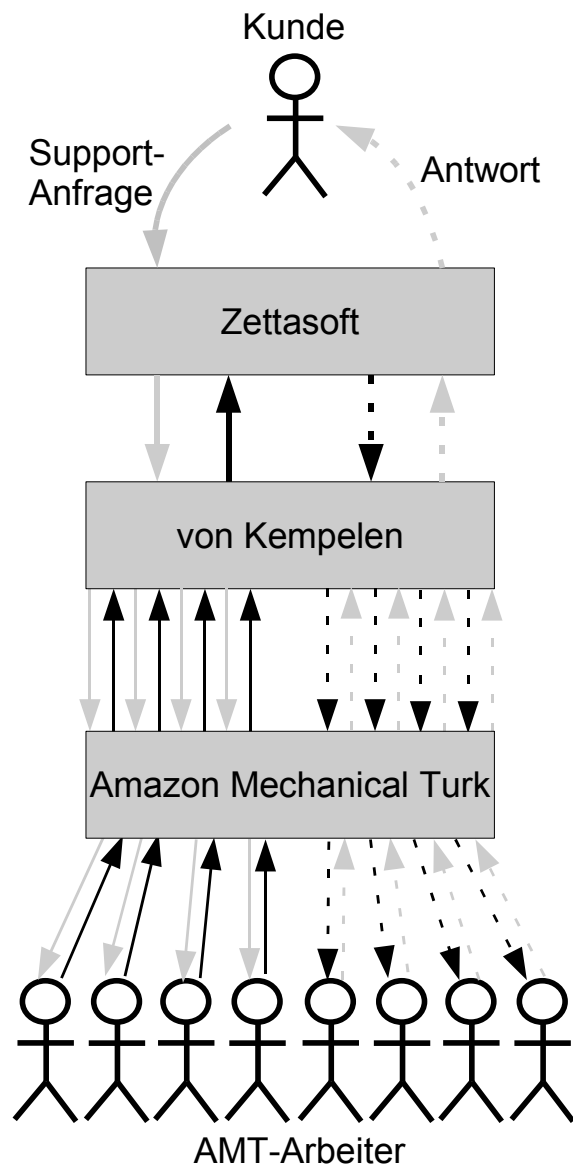
4.3.3 Datenflüsse zwischen den Akteuren

Welche Daten zwischen welchen Akteuren fließen, wird aus Abb. 4.9 ersichtlich. Zwischen Zettasoft, von Kempelen, AMT und den AMT-Arbeitern werden nur, wie in der Grafik verzeichnet, die Anfrage des Kunden und die Antwort von Zettasoft in jeweils zwei Sprachen kommuniziert.

Bei den Datenflüssen zwischen Kunde und Zettasoft muss jedoch differenziert werden: Um sich zu authentifizieren, muss der Kunde eine Kundennummer angeben, sowie eine E-Mail-Adresse, um die Antwort erhalten zu können. Diese Informationen werden vom eigentlichen Anfragetext getrennt erhoben und nicht mit an von Kempelen übertragen.

4.3.4 Verantwortlichkeit

Wie die Beschreibung der Datenflüsse zwischen den Akteuren gezeigt hat, werden in diesem Szenario personenbezogene Daten der Kunden nicht nur von deren Vertragspartner Zettasoft, sondern auch von weiteren Stellen, nämlich von Kempelen, Amazon Mechanical Turk (AMT) und den jeweils involvierten AMT-Arbeitern verwendet. Die beteiligten Stellen haben durch entsprechende vertragliche Regelungen eine Auftragsdatenverarbeitung im Sinne des § 11 BDSG vereinbart. Konkret handelt es sich bei Zettasoft um den Auftraggeber und bei den anderen beteiligten Stellen um Auftragnehmer bzw. um Unterauftragnehmer. Die Besonderheit dieser konkreten Konstellation besteht darin, dass Zettasoft als Auftraggeber für jegliche Verarbeitung personenbezogener Daten in diesem Szenario verantwortlich ist. Anders als in den beiden vorangegangenen Szenarien gibt es in diesem Szenario also nur eine verantwortliche Stelle, die sowohl für ihre eigene Datenverarbeitung als auch für die durch die (Unter)Auftragnehmer erfolgte Verwendung personenbezogener Daten die Verantwortung trägt. Die Auftragnehmer verpflichten sich im Gegenzug vertraglich dazu, personenbezogene Daten nur im Rahmen der durch Zettasoft als Auftraggeber erfolgten Weisungen zu verwenden. Auf das rechtliche Konstrukt der Auftragsdatenverarbeitung und die hiermit einhergehenden Besonderheiten wird in der rechtlichen Szenarienanalyse ausführlich eingegangen.



Datenflüsse	Sprache d. Kunden	Englisch
Support-Anfrage		
Antwort auf Anfrage		

Abbildung 4.9: Schematische Darstellung der Datenflüsse

4.3.5 Service-orientierte Architektur

Im Folgenden wird das Szenario als Service-orientierte Architektur (SOA) betrachtet.

4.3.5.1 Services

Zettasoft

Anfrageannahme Zwar wird der Service der Annahme von Supportanfragen nur manuell über eine Webseite in Anspruch genommen, jedoch kann er durchaus als Service im Sinne einer SOA gesehen werden.

Eingabedaten

Datum	Verwendungszweck	Personenbezug
Kundennummer	Authentifizierung des Kunden	Kunde
E-Mail-Adresse	Benötigt für die Antwort	Kunde
Sprachauswahl	Benötigt für automatisierte Übersetzung	-
Anfragetext	Beschreibung des Problems, das gelöst werden soll	<i>Kunde</i> ¹²

Ausgabedaten

Datum	Verwendungszweck	Personenbezug
Erfolgsmeldung		-

Rückmeldedienst Da die übersetzten Texte erst mit einiger Verzögerung bei Zettasoft eintreffen, muss eine Möglichkeit bestehen, sie ihm zuzustellen; der Rückmeldedienst erfüllt diesen Zweck.

Eingabedaten

Datum	Verwendungszweck	Personenbezug
von Kempelen-Auftragsnummer	Zuordnung des übersetzten Textes zum Auftrag	-
Übersetzter Text		<i>Kunde</i> ¹²

Ausgabedaten

Datum	Verwendungszweck	Personenbezug
Erfolgsmeldung		-

¹²Je nachdem, was der Kunde in seiner Anfrage geschrieben hat, kann der Personenbezug hier von „nicht vorhanden“ bis zu „eindeutig personenbeziehbar“ reichen.

von Kempelen

Auftragsannahme Über diesen Dienst können die Kunden Übersetzungsaufträge an von Kempelen übergeben. Da die Annahme des Auftrags zur Übersetzung und die Rückgabe des Resultats voneinander zeitlich entkoppelt sind, wird das Resultat nicht direkt, sondern erst mit Hilfe von Zettasofts Rückmeldedienst übermittelt.

Eingabedaten

Datum	Verwendungszweck	Personenbezug
Ursprungssprache	Sprache, die der Text im Moment hat	-
Zielsprache	Sprache, in die übersetzt werden soll	-
Text	zu übersetzender Text	<i>Kunde</i> ¹²

Ausgabedaten

Datum	Verwendungszweck	Personenbezug
von Kempelen-Auftragsnummer	Zuordnung des zu übersetzenden Textes zum Auftrag	-

Rückmeldedienst Analog zum Rückmeldedienst von Zettasoft kann AMT über diesen Dienst die Ergebnisse der HITs an von Kempelen liefern. Über einen solchen Dienst könnten beliebige Ergebnisse von bearbeiteten HITs zurückgeliefert werden; hier wird jedoch nur der Fall der Übersetzung-HITs betrachtet.

Eingabedaten

Datum	Verwendungszweck	Personenbezug
AMT-Auftragsnummer	Zuordnung des Resultats zum ursprünglichen HIT	-
Übersetzter Text		<i>Kunde</i> ¹²
Bewertung der vorigen Übersetzung	Trifft nur zu, falls ein bereits übersetzter Text korrigiert werden sollte	-

AMT

HIT-Beschreibung erzeugen Dieser Dienst wird genutzt, um die generelle Aufgabenbeschreibung inkl. geforderter Qualifikation bei AMT einzustellen. Konkret zu bearbeitende Daten werden nicht übermittelt.

Eingabedaten

Datum	Verwendungszweck	Personenbezug
Aufgabenbeschreibung	Arbeiter können erkennen, ob sie an diesem HIT Interesse haben	-
Mindestanforderung	Diese Qualifikation müssen Arbeiter erfüllen, die den HIT übernehmen wollen	-

Ausgabedaten

Datum	Verwendungszweck	Personenbezug
HIT-Beschreibungs-ID	Eindeutige Nummer, über die die HIT-Beschreibung im weiteren Verlauf identifiziert wird	-

Daten für konkreten HIT übertragen Ein zu bearbeitender Datensatz wird übermittelt; je nach Aufgabenstellung des HIT kann dies nur ein zu übersetzender Text sein oder ein Paar aus Original und Übersetzung, wobei letztere bewertet und ggf. korrigiert werden soll. Bevor dieser Dienst aufgerufen wird, muss bereits der vorangegangene genutzt worden sein.

Eingabedaten

Datum	Verwendungszweck	Personenbezug
HIT-Beschreibungs-ID	Beschreibung, auf die sich dieser Datensatz bezieht	-
Zu übersetzende Daten	Nur der Originaltext oder Original und Übersetzung zur Bewertung/Korrektur	<i>Kunde</i> ¹²

Ausgabedaten

Datum	Verwendungszweck	Personenbezug
AMT-Auftragsnummer	Ermöglicht spätere Zuordnung des Resultats zu den Eingabedaten	-

4.3.5.2 Ablauf¹³

Der Vorgang der Bearbeitung einer Support-Anfrage gliedert sich in 11 Abschnitte, welche im Folgenden kurz beschrieben werden.

1. Der Kunde will sich mit seiner Support-Anfrage an Zettasoft wenden. Auf der Web-Seite von Zettasoft wird ihm die Möglichkeit geboten, seine Anfrage auch in anderen Sprachen als Englisch zu formulieren. Er entscheidet sich, in seiner Muttersprache (für das Beispiel sei diese Deutsch) zu schreiben, trägt den Text sowie seine Kundennummer und

¹³vgl. hierzu auch Abb. 4.9

E-Mail-Adresse in ein Formular auf der erwähnten Web-Seite ein und wählt Deutsch als Anfrage-Sprache aus.

2. Der Server von Zettasoft, auf dem die Anfrage eingeht, erkennt, dass es sich um einen fremdsprachigen Text handelt, welcher nicht durch das Stammpersonal beantwortet werden kann. Er übergibt den reinen Anfrage-Text (ohne Kundennummer und E-Mail-Adresse) direkt an von Kempelen mit dem Auftrag, ihn ins Englische zu übersetzen.
3. Um die Übersetzung leisten zu können, hat von Kempelen zuvor Qualifikationstests an AMT übergeben, anhand derer AMT-Arbeiter ihre Eignung für Übersetzungen zwischen verschiedenen Sprachen zeigen können. von Kempelen erzeugt nun zunächst bei Amazon einen HIT, der die Übersetzung der Support-Anfrage verlangt.
4. Amazon macht die neue Aufgabe auf seiner „Mechanical Turk“-Web-Seite bekannt. Nur Arbeiter, die mindestens die niedrigste Qualifikationsstufe erreicht haben, dürfen diesen HIT annehmen.
5. Ein AMT-Arbeiter, dem Deutsch-Englisch-Übersetzungen leicht fallen, nimmt den HIT an: Amazon zeigt ihm den Originaltext an, worauf er eine Übersetzung eintippt und diese an Amazon sendet.
6. Amazon reicht das Resultat des HITs an von Kempelen weiter. Diese erzeugen nun einen neuen HIT, in dem ein Arbeiter einer höheren Qualifikationsstufe die Qualität der vorliegenden Übersetzung prüfen und Fehler gegebenenfalls korrigieren soll.
7. Der neue HIT wird wiederum von Amazon angeboten und durch einen Arbeiter erledigt. Dieser iterative Prozess des Korrigierens wird mehrmals wiederholt, bis der Text schließlich von mehreren erfahrenen AMT-Arbeitern für korrekt befunden wird¹⁴.
8. von Kempelen sendet die nun englischsprachige Anfrage zurück an Zettasoft.
9. Das Fachpersonal von Zettasoft liest die Anfrage und verfasst eine (ebenfalls englischsprachige) Antwort. Diese Antwort wird wiederum an von Kempelen übertragen, mit dem Auftrag, sie ins Deutsche zu übersetzen.

¹⁴Die Anzahl der Arbeitern in Abbildung 4.9, die an diesem Prozess beteiligt sind, wurde hierbei willkürlich auf vier festgelegt.

10. Die Punkte 3 bis 7 werden nochmals durchlaufen, mit dem Unterschied, dass nun vom Englischen ins Deutsche übersetzt wird.
11. von Kempelen übermittelt die deutschsprachige Antwort auf die Support-Anfrage weiter an Zettasoft. Dort wird der übersetzte Text wieder mit der Kundennummer und der E-Mail-Adresse des Kunden zusammengeführt und diesem anschließend als Antwort per E-Mail zugesendet.

4.3.6 Ursprung des Szenarios

Dieses Szenario beruht primär auf den offiziellen Webseiten der realen Unternehmen Amazon Mechanical Turk und von Kempelen, insbesondere sind deren Beschreibungen in der Einleitung aus diesen Quellen hergeleitet.

Von Kempelen, AMT und die AMT-Arbeiter existieren wirklich, Zettasoft und deren Kunden sind hingegen fiktional. Die Beziehungen zwischen den von Kempelen und AMT sowie zwischen AMT und den Arbeitern wurden originalgetreu beschrieben, soweit dies auf Basis öffentlich zugänglicher Informationen möglich war.

Der in diesem Szenario beschriebene Ablauf wurde zwar konstruiert, ist aber auf der Grundlage der realen Akteure realistisch. Insbesondere existieren die Services von von Kempelen und AMT, wie sie in Abschnitt 4.3.5.1 beschrieben sind, wirklich, nur ihre konkrete Funktionsweise und die Schnittstellenbeschreibungen wurden konstruiert.

4.4 PSB – Entwicklung von Produktionsstraßen: Basisszenario für Betriebs- und Geschäftsgeheimnisse

Das PSB Szenario besteht aus zwei Teilszenarien, die zeigen, dass die im Rahmen dieser Untersuchung unternommenen Betrachtungen nicht nur auf Datenschutz, sondern auch für die Überprüfung und Überwachung der Einhaltung von Datennutzungsrechten anwendbar sind. In beiden Szenarien wird die Firma PSB (aus Vertraulichkeitsgründen wurden diese Szenarien anonymisiert) betrachtet, die Produktionsstraßen entwickelt, beim Kunden aufbaut und wartet.

Das erste Teilszenario betrachtet eine virtuelle Organisation, die zum Zweck der Weiter- beziehungsweise Neuentwicklung von Produktionsstraßen zwischen dem PSB, Zulieferern und Ingenieurbüros gebildet wird. Der Zulieferer produziert Bauteile für die Produktionsstraßen, die von dem PSB

gebaut werden. Diese Bauteile besitzen eine große Anzahl an spezifischen Eigenschaften, die zum Geschäftsgeheimnis des Zulieferers gehören. Für die Entwicklung und Produktion der Produktionsstraßen werden teilweise Informationen über diese Eigenschaften benötigt. Einzelne Entwicklungsaufgaben lässt der PSB durch externe Ingenieurbüros lösen. Hierfür müssen Eigenschaftsbeschreibungen von Bauteilen, die verwendet werden sollen, an die Ingenieurbüros weitergegeben werden, die kein direktes Vertragsverhältnis mit dem Zulieferer haben. In diesem Teilszenario spielt die Weitergabe von vertraulichen Daten und die damit verbundene Einschränkung auf die notwendigen Informationen eine Rolle (Datensparsamkeit).

4.4.1 Akteure

4.4.1.1 PSB

Das Kerngeschäft des PSB ist die Herstellung von Produktionsstraßen. Viele der Bauteile, die für die Herstellung benötigt werden, bezieht der PSB über Zulieferer. Teils handelt es sich dabei um hoch entwickelte Bauteile mit speziellen Beschaffenheiten. Um Entwicklungskosten niedrig zu halten, werden möglichst viele Bauteile in zukünftigen Versionen der Produktionsstraßen, sowie in Neuentwicklungen, weiter verwendet. Teilaufgaben der Entwicklung vergibt der PSB an externe Ingenieurbüros, die bestimmte Expertisen aufweisen. Für die Einbindung der vorhandenen Bauteile benötigen diese Ingenieurbüros die Beschreibung einiger der speziellen Beschaffenheiten der Bauteile. Der PSB leitet zu diesem Zweck Teile der Spezifikation an die Ingenieurbüros weiter.

4.4.1.2 Zulieferer

Der Zulieferer produziert Bauteile für Produktionsstraßen und liefert diese an Produktionsstraßenhersteller wie den PSB. Viele der Bauteile haben bestimmte Beschaffenheiten, die Firmengeheimnis des Zulieferers sind und einen Wettbewerbsvorteil darstellen. Für die Verwendung der Bauteile in ihren Produktionsstraßen brauchen die Hersteller jedoch die genaue Spezifikation. Zu diesem Zweck teilt der Zulieferer den Herstellern die Spezifikation der Komponenten mit. Im Gegenzug verpflichten sich die Hersteller die Informationen vertraulich zu behandeln und nur weiterzugeben, wenn diese für die Entwicklungsarbeit unbedingt benötigt werden.

4.4.1.3 Ingenieurbüro

Das Ingenieurbüro hat in einem bestimmten Bereich der Produktionsstraßenentwicklung eine Expertise. Daher wird es zur Erfüllung diverser Entwicklungsaufgaben von Produktionsstraßenherstellern beauftragt. Sollen existierende Komponenten wieder verwendet werden, muss das Ingenieurbüro alle relevanten Beschaffenheiten dieser Komponenten berücksichtigen.

4.4.1.4 Kunde

Der Kunde des PSB, bei dem die Produktionsstraße betrieben wird.

4.4.2 Beziehungen der Akteure

In Abbildung 4.10 sind die einzelnen Beziehungen der Akteure untereinander hervorgehoben:

1. Der PSB und der Zulieferer haben einen Vertrag über die Lieferung von Bauteilen, sowie die Bereitstellung von vertraulichen Informationen. Im Gegenzug verpflichtet sich der PSB die Informationen vertraulich zu behandeln und nur nötige Teile bekannt zu geben.
2. Der PSB und das Ingenieurbüro haben einen Vertrag über die Entwicklung neuer Bauteile unter Wiederverwendung existierender Bauteile. Für die Wiederverwendung der Bauteile verpflichtet sich der PSB dem Ingenieurbüro alle relevanten Informationen zur Verfügung zu stellen.

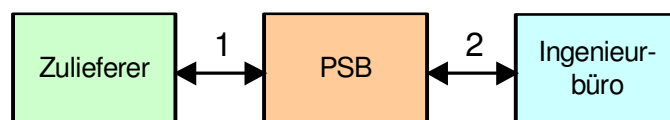


Abbildung 4.10: Beziehungen der Akteure

4.4.3 Datenflüsse zwischen den Akteuren

Abbildung 4.11 gibt eine Übersicht über die Datenflüsse zwischen den Akteuren:

1. Zwischen dem Zulieferer und dem PSB werden Informationen bezüglich der Spezifikation von Bauteilen ausgetauscht.

2. Zwischen dem PSB und dem Ingenieurbüro werden Informationen, die benötigt werden für die Entwicklung von Produktionsstraßen, ausgetauscht. Hierzu gehören auch Informationen aus der Spezifikation von zugelieferten Bauteilen.

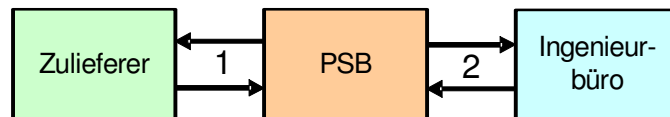


Abbildung 4.11: Schematische Darstellung der Datenflüsse

4.4.4 Verantwortlichkeit

In diesem Teilszenario werden keine personenbezogenen Daten, sondern solche, die Betriebs- und Geschäftsgeheimnisse enthalten, verarbeitet. Verantwortliche Stellen im Sinne des Datenschutzrechts gibt es in diesem Szenario folglich nicht. Sowohl PSB als auch das Ingenieurbüro trifft jedoch die Verantwortlichkeit, durch entsprechende technische und organisatorische Maßnahmen zu verhindern, dass Dritte Kenntnis von den Betriebs- und Geschäftsgeheimnissen erlangen (können). Die Verpflichtung hierzu wird durch sog. Non-Disclosure-Agreements begründet. Verantwortliche Stellen in diesem Sinne sind somit PSB und das Ingenieurbüro.

4.4.5 Service-orientierte Architektur

In diesem Abschnitt wird eine mögliche Service-orientierte Architektur (SOA) für dieses Szenario beschrieben.

4.4.5.1 Die Dienste innerhalb der virtuellen Organisation

Innerhalb dieses Szenarios werden von den einzelnen Akteuren verschiedene Dienstleistungen angeboten. Im Folgenden wird deren Funktionalität sowie deren Eingabe- und Ausgabedaten kurz erläutert:

PSB

Weiterentwicklungsdienst: Die Weiterentwicklung von Produktionsstraßen ist im vorgestellten Szenario die zentrale Dienstleistung. Von dieser

Dienstleistung gehen alle weiteren Aktionen aus. Die Eingabedaten für diese Dienstleistung sind der Konstruktionsplan der existierende Produktionsstraße, Beschreibung aller Bauteile, die in der existierenden Produktionsstraße verbaut wurden, sowie die natürlich-sprachlichen Anforderungen, die die Verbesserungswünsche beschreiben. Das Ergebnis dieser Dienstleistung ist der Konstruktionsplan für eine weiterentwickelte Produktionsstraße, die dann beim Kunden gebaut wird, sowie die Beschreibung aller Bauteile, die für die weiterentwickelte Produktionsstraße gebraucht werden.

Eingabedaten

Name	Zweck	Betroffener	Urheber
Konstruktionsplan	Weiterentwicklung	PSB und Kunde	PSB
Bauteilbeschreibungen	Weiterentwicklung	Hersteller der Bauteile (z. B. Zulieferer)	PSB oder Hersteller der Bauteile
Anforderungsliste	Weiterentwicklung	PSB und Kunde	PSB oder Kunde als Auftraggeber

Ausgabedaten

Name	Zweck	Betroffener	Urheber
Konstruktionsplan	./.	PSB und Kunde	PSB
Bauteilbeschreibungen	./.	Hersteller der Bauteile (z. B. Zulieferer)	PSB

Informationsdienst: Werden bei der Weiterentwicklung Informationen über Komponenten gebraucht, die wieder verwendet werden sollen, dann muss das Ingenieurbüro diese bei dem PSB anfordern. Dieser Dienst erhält als Eingabe den Namen des Zulieferers, die Produktnummer der Komponente und eine Beschreibung der benötigten Informationen. Als Ergebnis liefert dieser Dienst diese Information, falls der Zulieferer mit der Weitergabe einverstanden ist.

Eingabedaten

Name	Zweck	Betroffener	Urheber
Name des Zulieferers	./.	Zulieferer	./.
Produktnummer	Identifikation der Komponente	./.	./.
Informationsbeschreibung	Identifikation der Informationen	PSB und Ingenieurbüro	Ingenieurbüro

Ausgabedaten

Name	Zweck	Betroffener	Urheber
Bauteilbeschreibungen	./.	Hersteller der Bauteile	PSB oder Hersteller der Bauteile

Ingenieurbüro

Entwicklungsdienst: Für die Entwicklung neuer Komponenten, stellt das Ingenieurbüro eine Dienstleistung zur Verfügung. Als Eingabe erhält diese Dienstleistung eine natürlich-sprachliche Beschreibung der zu entwickelnden Komponente. Die Ausgabe dieses Dienstes ist der Konstruktionsplan für die neue Komponente und eine Beschreibung aller Bauteile, die für die entwickelte Komponente gebraucht werden.

Eingabedaten

Name	Zweck	Betroffener	Urheber
Komponentenbeschreibung	Entwicklung	PSB und Kunde	PSB oder Kunde als Auftraggeber

Ausgabedaten

Name	Zweck	Betroffener	Urheber
Konstruktionsplan	./.	PSB, Ingenieurbüro und Kunde	Ingenieurbüro
Bauteilbeschreibung	./.	Hersteller der Bauteile (z. B. Zulieferer)	Ingenieurbüro

Zulieferer

Informationsdienst: Die für ihren Informationsdienst benötigten Informationen erhält der PSB wiederum vom Zulieferer. Hierfür übermittelt der PSB die Produktnummer der Komponente, die Beschreibung der benötigten Informationen und den Namen des Ingenieurbüros, das die Informationen

braucht, an den Dienst. Als Ergebnis liefert dieser Dienst die Informationen, mit deren Weitergabe der Zulieferer einverstanden ist.

Eingabedaten

Name	Zweck	Betroffener	Urheber
Name des Ingenieurbüros	./.	Ingenieurbüro	./.
Produktnummer	Identifikation der Komponente	./.	./.
Informationsbeschreibung	Identifikation der Informationen	PSB und Ingenieurbüro	Ingenieurbüro

Ausgabedaten

Name	Zweck	Betroffener	Urheber
Bauteilbeschreibungen	./.	Zulieferer	Zulieferer

4.4.5.2 Ablauf innerhalb der virtuellen Organisation

Im Folgenden wird exemplarisch ein Durchlauf durch den Arbeitsprozess der virtuellen Organisation gezeigt (siehe Abbildung 4.12). Auch wenn der PSB die Spezifikation der Kugellager im Vorfeld erhält, werden im Folgenden die Informationsflüsse zwischen dem PSB und dem Zulieferer explizit aufgezeigt, indem diese als zusätzliche Nachfrage modelliert werden (3. und 4.).

1. Der PSB beabsichtigt die Weiterentwicklung einer Produktionsstraße, die bei mehreren Kunden im Einsatz ist. Eine Komponente des Produktionsstraße, die in der aktuellen Version Schwachstellen aufgezeigt hat und weiterentwickelt werden soll, ist eine bestimmte Achse. Diese Achse wird von Kugellagern, die über einen Zulieferer bezogen werden, gelagert. Mit der Entwicklung der neuen besseren Achse beauftragt der PSB ein externes Ingenieurbüro. Bei der Auftragserteilung teilt der PSB dem Ingenieurbüro die genaue Spezifikation der alten Achse mit.
2. Das Ingenieurbüro entwickelt eine neue Achse, die in Eigenschaften von der alten Version abweicht, die für den Einsatz der Achse mit den verwendeten Kugellagern relevant sind. Um zu überprüfen, ob das neue Design der Achse eventuell an die Kugellager angepasst werden muss benötigt das Ingenieurbüro spezifische Daten über das Kugellager und fragt diese bei dem PSB an.
3. Der PSB fordert bei dem Zulieferer die Spezifikation der Kugellager an, um diese an das Ingenieurbüro weiterzureichen.

4. Der Zulieferer teilt daraufhin dem PSB die Spezifikation der Kugellager mit. Dabei wird auch festgelegt, welche Teile der Spezifikation die PSB an das Ingenieurbüro weitergeben darf.
5. Der PSB reicht die benötigten Informationen an das Ingenieurbüro weiter.
6. Als Ergebnis liefert das Ingenieurbüro den Entwurf einer neuen Achse, die kompatibel mit den verwandten Kugellagern ist.

4.4.6 Ursprung des Szenarios

Dieses Szenario basiert auf Informationen über Geschäftsprozesse und Datenflüsse zweier großer europäischer Unternehmen im Bereich des Maschinenbaus. Besonders die Aufgabenverteilung unter den beteiligten Betrieben, die Geschäftsprozesse und Datenflüsse der VO spiegeln die tatsächlichen Gegebenheiten wieder. Die hier beschriebenen vertraglichen Beziehungen sind für dieses Szenario weitgehend konstruiert worden.

4.5 PSB – Wartung von Produktionsstraßen: Fortgeschrittenes Szenario für Betriebs- und Geschäftsgeheimnisse

Das zweite Teilszenario beschreibt eine virtuelle Organisation, die sich zur technischen Überwachung von Produktionsstraßen, die sich bei Kunden im Einsatz befinden, bildet. Die Überwachung erfolgt dabei durch die Erfassung und Auswertung von Multimediadaten während des Betriebs der Produktionsstraße. Für die Erfassung der Multimediadaten hat der PSB einen Vertrag mit einem externen Datendienstleister, der die Daten direkt beim Kunden erfasst und in seinen Datenbanken speichert. Durch vertragliche Gegebenheiten mit dem Unternehmen hat nicht der PSB sondern der Datendienstleister die Rechte an den Multimediadaten. Im Vertrag zwischen dem PSB und diesem Unternehmen wird geregelt zu welchem Zweck der PSB die Daten an wenn weitergeben darf. Die Analyse wird ebenfalls von einem externen Dienstleister durchgeführt. Da es im Interesse des Kunden des PSB ist, dass keine Informationen über Probleme an den von ihr genutzten Produktionsstraßen weitergegeben werden, müssen die Multimediadaten vor der Weitergabe an

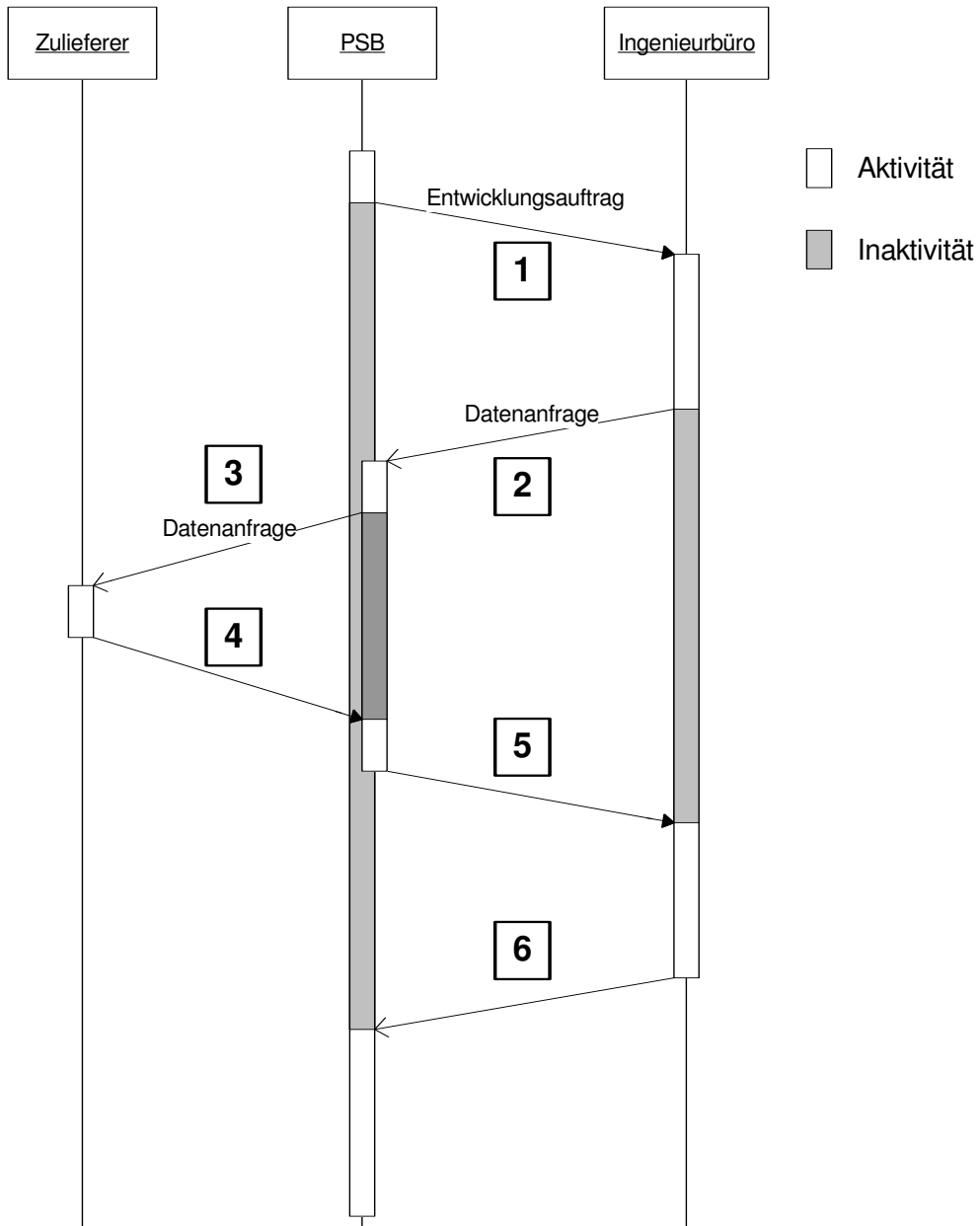


Abbildung 4.12: Sequenzdiagramm der Abläufe

den Analysten anonymisiert werden. In diesem Teilszenario spielt die Weitergabe von Daten, die nicht Eigentum von dem PSB sind, und die Anonymisierung von Daten, die vertrauliche Informationen über Vertragspartner des PSB enthalten, eine entscheidende Rolle.

4.5.1 Akteure

4.5.1.1 PSB

Ein zentrales Geschäftsfeld des PSB ist die langfristige Vermietung von Produktionsstraßen an seine Kunden. Dabei bleiben die Produktionsstraßen Eigentum des PSB und der PSB übernimmt die Wartung und Kontrolle der Produktionsstraßen. Ein Teil der Kontrolle geschieht durch Überwachung der Produktionsstraße während des Betriebes. Hierbei werden verschiedene Multimediatdaten für eine spätere Analyse erfasst.

4.5.1.2 Warenproduzent

Der Warenproduzent setzt die gemieteten Produktionsstraßen ein. In seinem Interesse ist die Geheimhaltung der zur Laufzeit der Produktionsstraße erfassten Daten, um Rückschlüsse über Probleme durch Außenstehende zu vermeiden. Dieses Interesse ist vertraglich mit dem PSB vereinbart.

4.5.1.3 Datendienstleister

Im Auftrag des PSB erfasst der Datendienstleister verschiedene Multimediatdaten (z.B. Mitschnitte der Betriebsgeräusche, Bilder, usw.) während des Betriebs der Produktionsstraße. Die Daten werden dann in Datenbanken des Datendienstleisters gespeichert und auf Abruf dem PSB zur Verfügung gestellt. Auf Grund von Vertragsstrukturen ist der Datendienstleister der Eigentümer der Daten.

4.5.1.4 Datenanalyst

Der Datenanalyst analysiert die Multimediatdaten auf Anzeichen von bevorstehenden Schäden, Materialermüdungen usw. Hierfür erhält er die Daten vom PSB.

4.5.2 Beziehungen der Akteure

In Abbildung 4.13 sind die einzelnen Beziehungen der Akteure innerhalb der virtuellen Organisation untereinander hervorgehoben:

1. Der PSB und der Warenproduzent haben einen Vertrag über die Wartung der gemieteten Produktionsstraßen. In diesem Vertrag ist enthalten, dass das Erfassen und Speichern der Daten, die für die Wartung benötigt werden, durch den Datendienstleister geschieht. Des Weiteren ist geregelt, dass Informationen über den Einsatz und Probleme von Produktionsstraßen nicht weitergegeben werden dürfen, außer es ist nicht erkennbar, dass es sich um eine Produktionsstraße handelt, die bei dem Warenproduzent im Einsatz ist.
2. Der Datendienstleister hat einen Vertrag mit dem PSB zur Erfassung, Speicherung und Bereitstellung der für die Überwachung der Produktionsstraßen nötigen Multimediadaten. Der Datendienstleister besitzt nach diesem Vertrag die Eigentumsrechte an den erfassten Multimediadaten. Auf Basis dieser Eigentumsrechte regelt der Vertrag die Weitergabe der Daten durch den PSB zu Analysezwecken.
3. Der Datendienstleister erfasst im Auftrag des PSB Multimediadaten bei dem Warenproduzenten. Diese Daten speichert er in Datenbanken und stellt sie der PSB auf Anfrage zur Verfügung.
4. Der Datenanalyst hat einen Vertrag mit dem PSB über die Analyse und Auswertung von Multimediadaten, die für die Wartung und Überwachung der Produktionsstraßen gesammelt werden.

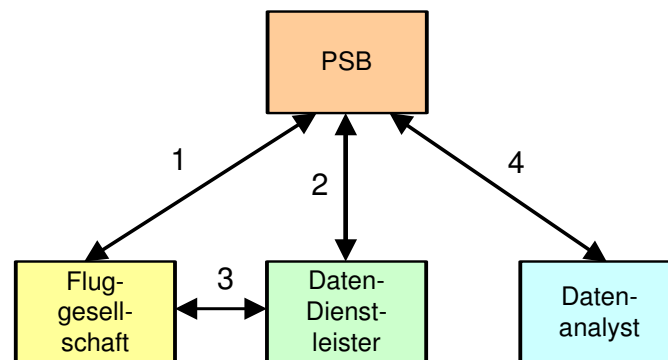


Abbildung 4.13: Beziehungen der Akteure

4.5.3 Datenflüsse zwischen den Akteuren

Abbildung 4.14 stellt die Datenflüsse und Abläufe innerhalb der virtuellen Organisation dar:

1. Der Datendienstleister erfasst die Daten beim Warenproduzenten. Die erfassten Daten werden in der Datenbank des Datendienstleisters gespeichert.
2. Zur Überprüfung und Auswertung von Daten fordert der PSB Daten beim Datendienstleister an.
3. Der Datendienstleister übermittelt diese Daten an den PSB.
4. Der PSB leitet die Multimediadaten anonymisiert an den Datenanalytisten weiter, damit dieser die Daten analysieren und auswerten kann.
5. Das Ergebnis der Analyse wird an den PSB zurück übermittelt.

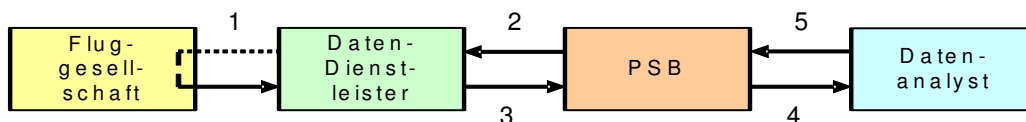


Abbildung 4.14: Schematische Darstellung der Datenflüsse

4.5.4 Verantwortlichkeit

Auch in diesem Teilszenario werden keine personenbezogenen Daten, sondern solche, die u. U. Rückschlüsse auf Probleme beim Betrieb einer Produktionsstraße geben können, verarbeitet. Somit gibt es auch in diesem Szenario keine verantwortlichen Stellen im Sinne des Datenschutzrechts. PSB und den Datendienstleister haben sich jedoch gegenüber dem Warenproduzenten vertraglich dazu verpflichtet, keine Multimediadaten weiterzugeben - ausgenommen sind insoweit nur Daten, denen sich nicht entnehmen lässt, dass es sich eine Produktionsstraße handelt, die bei diesem Warenproduzent im Einsatz ist. Auch hier besteht also wieder die Verpflichtung, technische und organisatorische Maßnahmen zu treffen, die verhindern, dass Dritte Kenntnis von den Daten erlangen können. Zudem trifft PSB auch die Verpflichtung, die Daten - bevor sie an den Datenanalytisten weitergegeben - dergestalt zu anonymisieren, dass nicht mehr erkennbar ist, bei welchem Warenproduzenten die konkrete Produktionsstraße im Einsatz ist. Verantwortliche Stellen in dem eben geschilderten Sinne sind damit PSB und der Datendienstleister.

4.5.5 Service-orientierte Architektur

In diesem Abschnitt wird eine mögliche Service-orientierte Architektur (SOA) für dieses Szenario beschrieben.

4.5.5.1 Die Dienste innerhalb der virtuellen Organisation

Innerhalb dieses Szenarios werden von den einzelnen Akteuren verschiedene Dienstleistungen angeboten. Im Folgenden wird deren Funktionalität sowie deren Eingabe- und Ausgabedaten kurz erläutert:

PSB

Problemanalysedienst: Dieser Dienst bietet den Warenproduzenten eine Schnittstelle, um Probleme mit einer Produktionsstraße zu melden. Hierfür werden von dem aufrufenden Warenproduzenten eine Problembeschreibung, die Identifikationsnummer der betroffenen Produktionsstraße und der Zeitpunkt, zu dem das Problem aufgetreten ist, gemeldet.

Eingabedaten

Name	Zweck	Betroffener	Urheber
Problembeschreibung	Identifikation des Problems	PSB und Warenproduzent	Warenproduzent
Identifikationsnummer	Identifikation der Produktionsstraße	Warenproduzent	./.
Zeitpunkt	Identifikation des Problems	./.	./.

Ausgabedaten

Name	Zweck	Betroffener	Urheber
Untersuchungsbericht	./.	Warenproduzent und PSB	PSB

Datendienstleister

Datenzugriffsdienst: Der Datenzugriffsdienst ermöglicht dem PSB den Zugriff auf die Daten, die beim Datendienstleister gespeichert werden. Als Eingabe erhält dieser Dienst die Identifikationsnummer der Produktionsstraße sowie der Zeitpunkt, an beziehungsweise ab dem das Problem aufgetreten ist. Als Ergebnis liefert dieser Dienst die Multimediadaten, die ab diesem Zeitpunkt an der betroffenen Produktionsstraße aufgenommen wurden.

Eingabedaten

Name	Zweck	Betroffener	Urheber
Identifikationsnummer	Identifikation der Produktionsstraße	Warenproduzent	./.
Zeitpunkt	Identifikation des Problems	./.	./.

Ausgabedaten

Name	Zweck	Betroffener	Urheber
Multimediatdaten	./.	der Warenproduzent	der Datendienstleister

Datenanalytst

Analysedienst: Dieser Dienst wertet die Multimediatdaten aus. Hierfür erhält der Dienst als Eingabe die Multimediatdaten und liefert als Ergebnis einen Bericht an gefundenen Auffälligkeiten.

Eingabedaten

Name	Zweck	Betroffener	Urheber
Multimediatdaten	Analyse des Problems	PSB und Warenproduzent	Datendienstleister

Ausgabedaten

Name	Zweck	Betroffener	Urheber
Liste von Auffälligkeiten	./.	PSB und Warenproduzent	Datenanalytst

4.5.5.2 Ablauf innerhalb der virtuellen Organisation

Im Folgenden wird exemplarisch ein Durchlauf durch den Arbeitsprozess der virtuellen Organisation gezeigt (siehe Abbildung 4.15):

1. Während des Einsatzes der Produktionsstraßen, erfasst der Datendienstleister die Multimediatdaten beim Warenproduzenten und speichert diese in seiner Datenbank.
2. Der Warenproduzent teilt dem PSB mit, dass es Probleme mit einer der Produktionsstraßen gibt, die bei dem Warenproduzenten im Einsatz sind. Hierfür wird die Identifikationsnummer der betroffenen Produktionsstraße sowie der Zeitpunkt, wann das Problem aufgetreten ist, dem PSB mitgeteilt.

3. Der PSB fordert die entsprechenden Multimediadaten vom Datendienstleister an.
4. Der Datendienstleister ruft die Daten aus seiner Datenbank ab und überträgt diese an den PSB zu Analyse Zwecken.
5. Nachdem der PSB die Daten intern anonymisiert hat, werden Teile der Daten an den externe Multimediaanalysten weitergegeben.
6. Der Multimediaanalyst arbeitet die Daten dahingehend auf, dass diese vom PSB weiterverwendet werden können, und überträgt die Daten zurück an den PSB.
7. Nach der Evaluation der aufgearbeiteten Daten und der Identifikation des Problems teilt der PSB das Ergebnis und die nächsten Schritte dem Warenproduzenten mit.

4.5.6 Ursprung des Szenarios

Dieses Szenario basiert auf Informationen über Geschäftsprozesse und Datenflüsse zweier großer europäischer Unternehmen im Bereich des Maschinenbaus. Besonders die Aufgabenverteilung unter den beteiligten Betrieben, die Geschäftsprozesse und Datenflüsse der VO spiegeln die tatsächlichen Gegebenheiten wieder. Die hier beschriebenen vertraglichen Beziehungen sind für dieses Szenario weitgehend konstruiert worden.

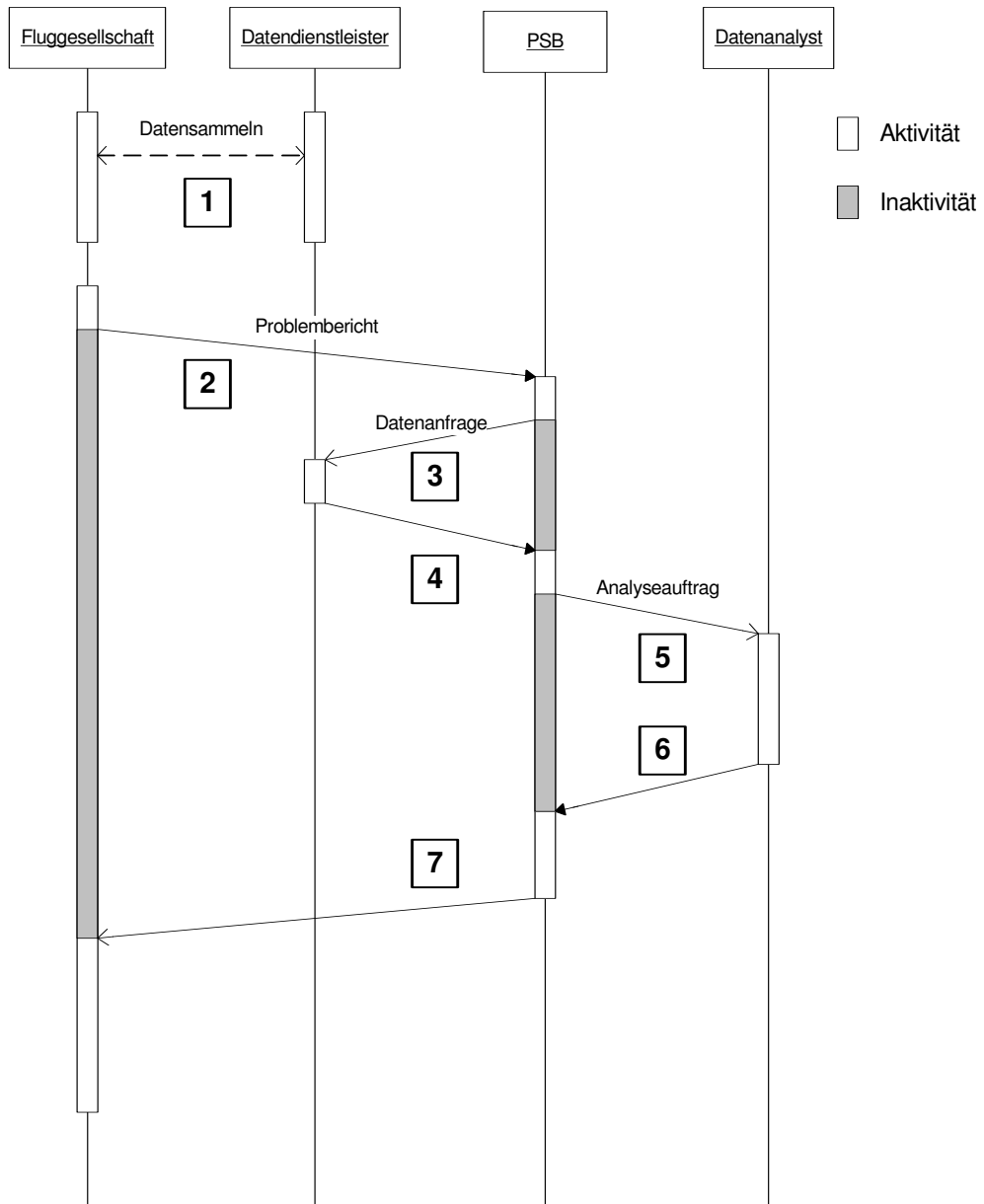


Abbildung 4.15: Sequenzdiagramm der Abläufe

4.6 Rechtliche Analyse der Szenarien

4.6.1 Allgemeine Bemerkungen

Nachfolgend werden die verschiedenen Szenarien in rechtlicher Hinsicht analysiert, wobei es insoweit ganz überwiegend um Fragestellungen aus dem Bereich des Datenschutzrechts geht. Methodische Grundlage der Analyse ist das bereits im Abschnitt 2.3 vorgestellte und erläuterte Prüfungsschema. Insofern ist festzustellen, dass die Prüfungsschritte 1 (Analyse des Datenflusses) und 2 (Anwendbarkeit der Datenschutzgesetze, Beteiligte) zum größten Teil bereits in der jeweiligen Szenarienbeschreibung abgehandelt werden. Im Rahmen der rechtlichen Analyse wird auf diese Prüfungsschritte nur dann (nochmals) eingegangen, wenn insoweit schwierige Fragestellungen zu klären sind (z. B. wenn genauer untersucht werden muss, ob Daten einen Personenbezug aufweisen oder wenn es um Fragestellungen der Auftragsdatenverarbeitung geht). Bei der rechtlichen Analyse der Szenarien werden also im Allgemeinen nur die Prüfungsschritte 3-5 behandelt und auch insoweit werden immer nur die Punkte angesprochen, die problematisch und damit für die Analyse von besonderem Interesse sind. Stets thematisiert wird indes die Bedeutung der rechtlichen Analyse im Hinblick auf die vier Beherrschbarkeitsfaktoren Zusage, Unterrichtung, Protokollierung und Auskunft.

Bevor die einzelnen Szenarien rechtlich analysiert werden, seien an dieser Stelle aber zunächst einige allgemeine Bemerkungen vorausgeschickt, welche die bereits im Kapitel 2 erfolgten Ausführungen ergänzen:

4.6.1.1 Verantwortlichkeit und Transparenz

Wie schon im Abschnitt „SOA & Datenschutz: Chancen und Risiken“ (2.1.1.4) erwähnt, besteht bei einem organisationsübergreifenden Einsatz Service-orientierter Architekturen angesichts technisch leicht zu bewerkstelligender Verkettungen ein erhöhtes Risiko einer rechtswidrigen Verarbeitung personenbezogener Daten. Diese können insbesondere dazu verwendet werden, detaillierte Profile der jeweils betroffenen Personen zu erstellen. Durch die Beteiligung vieler unterschiedlicher Stellen wird zudem schnell ein hohes Maß an Komplexität bei der Verarbeitung personenbezogener Daten erreicht. Insofern besteht die Gefahr, dass die betroffenen Personen nicht mehr überblicken können, welche Stellen welche Daten über sie verarbeiten. Sofern dies der Fall ist, wird den Betroffenen hierdurch aber die Ausübung ihrer Rechte auf Auskunft, Berichtigung, Löschung und Sperrung erschwert, wenn nicht sogar (teilweise) unmöglich gemacht¹⁵.

¹⁵Speziell zur datenschutzrechtlichen Auskunftserteilung bei stellenübergreifenden komplexen Datenverarbeitungssystemen vgl. [Wei06]

Wie bereits die eben skizzierte Problematik zeigt, ist es von entscheidender Bedeutung, dass Organisationen, die im Rahmen einer organisationsübergreifenden SOA kooperieren wollen, sich bereits in der Planungsphase mit der Frage der datenschutzrechtlichen Verantwortlichkeit befassen. Denn der Grundsatz, dass ein jegliches rechtlich relevantes Verhalten stets einem (hierfür verantwortlichen) Rechtssubjekt zugerechnet wird, gilt selbstverständlich auch im Datenschutzrecht. Wie bereits ausgeführt, definiert Artikel 2 d) der EG-DatSchRL den für die Verarbeitung Verantwortlichen als die natürliche oder juristische Person, Behörde, Einrichtung oder sonstige Stelle, die allein oder gemeinsam mit anderen über die Zwecke und Mittel der Verarbeitung von personenbezogenen Daten entscheidet. Entsprechend ist nach § 3 Abs. 7 BDSG jede Person oder Stelle verantwortlich, die personenbezogene Daten für sich selbst erhebt, verarbeitet oder nutzt oder dies durch andere im Auftrag vornehmen lässt. Kooperieren mehrere Organisationen im Rahmen einer Service-orientierten Architektur und verarbeiten mehrere dieser Stellen in diesem Zusammenhang personenbezogene Daten, so entscheiden die konkreten vertraglichen Beziehungen zwischen den beteiligten Organisationen darüber, ob lediglich eine oder aber mehrere bzw. sogar alle dieser Stellen für die Datenverarbeitung verantwortlich sind. Konkret bedeutet dies, dass regelmäßig mehrere Stellen verantwortlich im Sinne des Datenschutzrechts sein werden, wenn nicht eine Auftragsdatenverarbeitung vereinbart wird. Insofern kann der Begriff der virtuellen Organisation leicht zu Missverständnissen führen, da er eine (auch) rechtliche „Verschmelzung“ mehrerer Organisationen zu einer diesen übergeordneten Organisationform suggeriert¹⁶. Dies ist jedoch regelmäßig – so auch in den nachfolgenden Szenarien¹⁷ – nicht der Fall, weshalb dann grundsätzlich die einzelnen Organisationen für die jeweils von ihnen durchgeführte Datenverarbeitung verantwortlich sind. Es sei aber nochmals darauf hingewiesen, dass auch in diesen Fällen die Verantwortung für die Datenverarbeitung nur bei einer Stelle liegen kann, wenn von dem Instrument der Auftragsdatenverarbeitung Gebrauch gemacht wird¹⁸.

Sind viele verschiedene Organisationen an einer organisationsübergreifenden SOA beteiligt, so kann die Datenverarbeitung leicht ein Maß an Kom-

¹⁶Tatsächlich kann es in manchen Konstellationen dazu kommen, dass sich die beteiligten Organisationen derart zusammenschließen, dass hierdurch – zumindest vorübergehend – ein neues Rechtssubjekt entsteht. Dies ist aber kein Automatismus, wie es der Begriff der virtuellen Organisation nahelegt, sondern wird im SOA-Kontext eher selten der Fall sein.

¹⁷In diesen geht es jeweils um eine schlichte Kooperation von Unternehmen unter Nutzung von IT, ohne dass hierdurch ein neues Rechtssubjekt geschaffen würde.

¹⁸In diesen Fällen ist nach § 11 Abs. 1 S. 1 BDSG (nur) der Auftraggeber für die Einhaltung der Vorschriften des Bundesdatenschutzgesetzes und anderer Vorschriften über den Datenschutz verantwortlich.

plexität erreichen, welches dazu führt, dass sie für den Betroffenen intransparent wird. Vor diesem Hintergrund ist es von besonderer Bedeutung, dass die jeweils verantwortliche Stelle eine Information und Beauskunftung der betroffenen Personen gemäß den gesetzlichen Vorgaben sicherstellt. Letztlich muss ein Maß an Transparenz hergestellt werden, das den Betroffenen die effektive Wahrnehmung ihrer Rechte gegenüber den verantwortlichen Stellen ermöglicht.

Damit bleibt als kurzes Zwischenfazit festzuhalten, dass auch im Rahmen einer Service-orientierten Architektur jede einzelne Verarbeitung personenbezogener Daten einer Stelle zugerechnet wird, die für den konkreten Verarbeitungsvorgang verantwortlich ist und somit auch das gesetzlich geforderte Maß an Transparenz zu gewährleisten hat. Es wird folglich ein wesentlicher Bestandteil der rechtlichen Analyse der Szenarien sein, zu überprüfen, wie die jeweils für die Verarbeitung verantwortlichen Stellen die Einhaltung der gesetzlichen Informationspflichten und die rechtskonforme Beauskunftung der Betroffenen gewährleisten können.

4.6.1.2 Internationale Bezüge

Innerhalb der Europäischen Union (EU) und des Europäischen Wirtschaftsraums (EWR)¹⁹ ist durch die EU-Datenschutzrichtlinie (RL 95/46/EG – EG-DatSchRL) und die Datenschutzrichtlinie für elektronische Kommunikation (RL 2002/58/EG – EKom-EG-DatSchRL) ein einheitlicher Mindeststandard für die Verarbeitung personenbezogener Daten geschaffen worden. Ähnliches gilt für den Bereich des (sonstigen) Verbraucherschutzrechts, für den durch verschiedene Richtlinien ebenfalls ein europaweit vergleichbares Schutzniveau etabliert worden ist²⁰. Das jeweils gewährleistete Schutzniveau geht aber sowohl im Bereich des Datenschutzes als auch im Bereich des Verbraucherschutzrechts vielfach weit über das Niveau hinaus, welches in außerhalb der EU und des EWR gelegenen Staaten garantiert wird. In der Gesamtschau besteht also ein deutliches Schutzgefälle zwischen den EU/EWR-Staaten und den meisten der sog. Drittstaaten. Bereits im Abschnitt „Grundprinzipien des Datenschutzrechts“ (2.1.1.3) ist darauf hingewiesen worden, dass die Übermittlung personenbezogener Daten in diese Drittstaaten (folgerichtig) nur

¹⁹Zu diesem gehören neben den EU-Mitgliedsstaaten auch noch Island, Liechtenstein und Norwegen.

²⁰Hier seien exemplarisch nur die Richtlinie 93/13/EWG über missbräuchliche Klauseln in Verbraucherverträgen, die Richtlinie 97/7/EG über den Verbraucherschutz bei Vertragsabschlüssen im Fernabsatz und die Richtlinie 2000/31/EG über bestimmte rechtliche Aspekte der Dienste der Informationsgesellschaft, insbesondere des elektronischen Geschäftsverkehrs, im Binnenmarkt (sog. E-Commerce-Richtlinie) genannt.

unter den besonderen Voraussetzungen der §§ 4 b f. BDSG (Artikel 25 f. EG-DatSchRL) zulässig ist. Im SOA Kontext kommt es häufig zu einer die Grenzen des EU/EWR-Raums überschreitenden Datenverarbeitung, weshalb auch diese Problematik im Rahmen der nachfolgenden Szenarienanalyse noch näher dargestellt wird.

Die Szenarienanalyse wird anhand des geltenden deutschen Rechts vorgenommen, allerdings erfolgt wegen der vielfach auftretenden internationalen Bezüge und im Hinblick auf den soeben erwähnten „geschützten Bereich“ innerhalb der EU und des EWR auch stets ein Hinweis auf die jeweils korrespondierenden Vorschriften der EU-Datenschutzrichtlinie.

4.6.1.3 Konsequenzen für die Beherrschbarkeitsfaktoren einer SOA

Im Kapitel „Technischer Rahmen“ sind Zusicherung, Unterrichtung, Protokollierung und Auskunft als wesentliche Beherrschbarkeitsfaktoren einer Service-orientierten Architektur identifiziert worden, die bereits beim Design einer solchen zu berücksichtigen sind. Maßgeblich beeinflusst werden diese Faktoren von den jeweils zu beachtenden rechtlichen Anforderungen. Deshalb ist es ein wichtiger Bestandteil dieser juristischen Szenarienanalyse, stets auf die Konsequenzen der Ergebnisse der jeweiligen rechtlichen Analyse für die einzelnen Beherrschbarkeitsfaktoren hinzuweisen.

Pauschal lässt sich sagen, dass Zusicherungen aus datenschutzrechtlicher Perspektive regelmäßig darin bestehen werden, personenbezogene Daten nur zu den jeweils rechtlich zulässigen Zwecken (z. B. Vertragserfüllung) zu verarbeiten. Die Funktion von Zusicherungen besteht aus datenschutzrechtlicher Sicht also in erster Linie in der Sicherstellung der Einhaltung des Zweckbindungssatzes²¹.

Hinsichtlich des Beherrschbarkeitsfaktors Unterrichtung geht es aus Datenschutzsicht darum zu identifizieren, welche Stellen für die Erfüllung welcher Unterrichtungs-, Benachrichtigungs- oder Informationspflichten verantwortlich sind²².

Außerdem muss beim Design einer organisationsübergreifenden SOA stets bedacht werden, wie eine rechtskonforme Beauskunftung des Betroffenen realisiert werden kann. Macht dieser seinen Auskunftsanspruch geltend, so muss sichergestellt sein, dass ihm eine vollständige Auskunft über die zu seiner

²¹Zu diesem vergleiche die entsprechenden Ausführungen im Abschnitt „Grundprinzipien des Datenschutzrechts“ (2.1.1.3).

²²Im Internet-Umfeld kommt insoweit einer auf einer Website platzierten Datenschutzerklärung, die allgemein verständlich verfasst ist und alle wesentlichen Aspekte der Datenverarbeitung abdeckt, eine wichtige Bedeutung zu.

Person gespeicherten Daten, die Empfänger oder Kategorien von Empfängern und den Zweck der Speicherung erteilt wird.

Zur Erfüllung des Auskunftsanspruchs können dabei die im Rahmen der Protokollierung gespeicherten Informationen verwendet werden. In diesem Zusammenhang ist allerdings zu beachten, dass die Protokollierung personenbezogener Daten aus rechtlicher Sicht nicht unbegrenzt zulässig ist. Da auf rechtliche Fragen der Protokollierung²³ in dieser Untersuchung bislang noch nicht eingegangen worden ist, soll an dieser Stelle ein kurzer Überblick hierüber gegeben werden:

Protokollierung und Recht Aus verfassungsrechtlicher Sicht zählt die Protokollierung zu den verfahrensrechtlichen Vorkehrungen zum Schutz der informationellen Selbstbestimmung. Sie macht die Verwendung personenbezogener Daten sowohl für den Betroffenen als auch für den internen Datenschutzbeauftragten und die zuständige Aufsichtsbehörde nachvollziehbar und damit überhaupt erst kontrollfähig.

Die Protokollierung zählt zu den zentralen technisch-organisatorischen Maßnahmen der Datensicherheit und ist eine Voraussetzung für die Umsetzung nahezu aller der in der Anlage zu § 9 BDSG genannten Maßnahmen [Biz06]. Nach § 4 e Satz 1 Nr. 9 BDSG bildet die allgemeine Beschreibung der Sicherheitsmaßnahmen nach § 9 BDSG einen Bestandteil des (internen) Verfahrensverzeichnis – im Rahmen dieser Beschreibung ist dann auch aufzuführen, für welche Zwecke eine Protokollierung durchgeführt wird. Zu unterscheiden ist zwischen der Protokollierung der Aktivitäten der Administratoren zur Gestaltung eines IT-Systems und der Protokollierung der konkreten Verarbeitung personenbezogener Daten durch die Nutzer des Systems.

Besondere Anforderungen an die Protokollierung stellt das Datenschutzrecht bei automatisierten Abrufverfahren²⁴. Spezielle Regelungen für die Protokollierung treffen außerdem auch Stellen, die geschäftsmäßig personenbezogene Daten an Dritte übermitteln (z. B. Auskunfteien)²⁵.

Auch Protokolldateien können einen Personenbezug aufweisen und etwa zur Kontrolle von Mitarbeitern eingesetzt werden. Folglich ist bei der technischen Auswahl und Gestaltung von Protokollierungsverfahren der Grundsatz der Datenvermeidung- und sparsamkeit zu beachten und insbesondere von den Möglichkeiten der Anonymisierung und Pseudonymisierung Gebrauch zu machen²⁶ (§ 3a BDSG). Darüber hinaus sieht § 31 BDSG eine beson-

²³Ausführlich hierzu [Biz06]

²⁴Einschlägig sind hier § 10 BDSG sowie eine Vielzahl bereichsspezifischer Regelungen (z. B. § 112 Abs. 4 S. 4 TKG).

²⁵§ 29 Abs. 2 S. 3 und 4 BDSG

²⁶Dies allerdings nur, soweit es möglich ist und der Aufwand in einem angemessenen

dere Zweckbindung für personenbezogene Daten vor, die ausschließlich zu Zwecken der Datenschutzkontrolle, der Datensicherung oder zur Sicherstellung des ordnungsgemäßen Betriebes einer Datenverarbeitungsanlage gespeichert werden. Schließlich ist der Betroffene nach erfolgter Protokollierung grundsätzlich gem. §§ 33 Abs. 1 BDSG zu benachrichtigen²⁷. Im Hinblick hierauf ist es sinnvoll, Mitarbeiter und Kunden bereits zu Beginn der jeweiligen Vertragsbeziehung entsprechend zu informieren.

Abschließend sei noch auf einige spezielle Protokollierungsregelungen im Bereich der elektronischen Informations- und Kommunikationsdienste hingewiesen: Gemäß 13 Abs. 2 Nr. 2 TMG ist eine elektronische Einwilligung in die Datenverarbeitung bei Telemediendiensten nur dann wirksam, wenn sie durch die verantwortliche Stelle protokolliert wird²⁸. Des Weiteren darf ein Anbieter von Telemediendiensten – also z. B. der Betreiber einer kommerziellen Website – gem. § 15 Abs. 4 Satz 1 TMG personenbezogene Nutzungsdaten²⁹ über das Ende des Nutzungsvorgangs hinaus (nur) verwenden, soweit sie für Zwecke der Abrechnung mit dem Nutzer erforderlich sind³⁰. Ist dies nicht der Fall, so sind die Daten folglich grundsätzlich unmittelbar nach Ende der Nutzung zu löschen³¹.

4.6.2 PotatoSystem

Bei diesem Szenario³² ist zu unterscheiden zwischen der Datenverarbeitung

- vor Vertragsschluss (relevanter Dienst: Account-Erstellung),
- bei Vertragsschluss (relevante Dienste: Paybest, PayPal und Kauf von Dateien),
- für andere – nicht vertragsrelevante – Zwecke,

Verhältnis zu dem angestrebten Schutzzweck steht.

²⁷Der Ausnahmetatbestand des § 33 Abs. 2 Nr. 2 BDSG wird hier regelmäßig nicht einschlägig sein, da die Benachrichtigung im Regelfall keinen unverhältnismäßigen Aufwand für die verantwortliche Stelle bedeuten wird [Biz06].

²⁸Gleiches gilt gem. § 94 Nr. 2 TKG auch bei Telekommunikationsdiensten.

²⁹Bei den diesen handelt es sich um Angaben darüber, wer welche Telemediendienste innerhalb welchen Zeitraums in Anspruch genommen hat, und damit um Protokolldaten.

³⁰Eine vergleichbare Regelung für Telekommunikations-Verkehrsdaten findet sich in § 96 Abs. 2 TKG.

³¹Dies ist nur dann nicht der Fall, wenn die Daten noch zur Erfüllung bestehender Aufbewahrungsfristen benötigt werden. In einer solchen Konstellation sind sie nach Abschluss der Nutzung durch den Diensteanbieter (lediglich) zu sperren.

³²Eine ausführliche rechtliche Analyse dieses Szenarios findet sich bereits in der Studie *privacy4DRM* [BGW05].

- durch verborgene Schnittstellen und Verkettung verschiedener Funktionen³³.

Während unterschiedliche Stellen für die Verarbeitung personenbezogener Daten verantwortlich sind (Musikanbieter, 4FO AG und Zahlungsmittelanbieter), ist von dieser stets der jeweilige Nutzer des PotatoSystems betroffen. Bei der Datenverarbeitung durch die 4FO AG wird - wie bereits in der technischen Beschreibung des PotatoSystems - auch im Rahmen der rechtlichen Analyse wieder zwischen einer Verarbeitung durch den Payment-, den HTML- und den Accounting-Server differenziert. Zur Klarstellung sei insoweit noch einmal darauf hingewiesen, dass die 4FO AG in allen diesen Fällen verantwortliche Stelle für die Datenverarbeitung ist.

4.6.2.1 Datenverarbeitung vor Vertragsschluss

Surfen des Nutzer auf der Website eines Musik-Anbieters Surft der Nutzer auf der Website eines Musik-Anbieters, so kann dieser über Logfiles und unterschiedliche technische Ansätze Daten wie IP-Adresse, Clickstream oder Cookies erheben³⁴, welche vielfach einen Personenbezug aufweisen werden³⁵. Verantwortliche Stelle ist hier der jeweilige Musikanbieter (Label oder Einzelkünstler), welcher die eben genannten sowie weitere Nutzungsdaten³⁶ unter den Voraussetzungen des § 15 TMG verarbeiten darf. Die 4FO AG kann insoweit durch vertragliche Regelungen dafür sorgen, dass der Musikanbieter sein Angebot datenschutzkonform und für den Nutzer hinreichend transparent ausgestaltet. Die nötige Transparenz kann etwa durch die Veröffentlichung einer umfassenden, verständlich formulierten und leicht auffindbaren Datenschutzerklärung auf der Website hergestellt werden³⁷. Darüber

³³Auf den bei privacy4DRM aus Gründen der Einheitlichkeit der Darstellung der rechtlichen Bewertung verschiedener Systeme mit aufgeführten Prüfungspunkt „Datenverarbeitung bei Rechteüberprüfung zur Nutzung“ wird vorliegend verzichtet. Die via PotatoSystem erworbenen Dateien können nämlich ohne Einschränkungen durch ein Digital Rights Management genutzt werden, weshalb keine Rechteüberprüfung zur Nutzung stattfindet und folglich auch keine (personenbezogenen) Daten verarbeitet werden.

³⁴Ausführliche Ausführungen zu Datenspuren, die bei Nutzung des Internets anfallen, finden sich in [KK00].

³⁵Zum Personenbezug von IP-Adressen vgl. etwa Weichert in [DKWW07, § 3 Rn. 4] und zum Personenbezug von Cookies siehe [Biz03].

³⁶Beispielsweise Metadaten zu verwendetem Browser und Betriebssystem.

³⁷Gem. § 13 Abs. 1 S. 1 TMG hat der Diensteanbieter den Nutzer zu Beginn des Nutzungsvorgangs über Art, Umfang und Zwecke der Verarbeitung personenbezogener Daten sowie über die Übermittlung von Daten in unsichere Drittstaaten zu unterrichten. Dies hat in allgemein verständlicher Form zu erfolgen. Diese Norm kann allerdings durchaus auch dahin gehend ausgelegt werden, dass die in ihr statuierte Unterrichtspflicht durch

hinaus ist dem Nutzer gem. § 13 Abs. 5 TMG auch die Weiterleitung zu einem anderen Diensteanbieter anzuzeigen – dies gilt beispielsweise für den Fall, dass er an die Server des PotatoSystems weitervermittelt wird.

Surfen des Nutzers auf der PotatoSystem-Website Surft der Nutzer lediglich auf der Website des PotatoSystems, ohne angemeldet zu sein oder einen Kauf zu tätigen, so gilt das Gleiche wie beim Surfen auf der Website eines Musikanbieters: Auch die 4FO AG kann die bereits oben genannten Nutzungsdaten erheben, wenn ein Nutzer ihre Seiten abrufen; außerdem wird auch hier wieder in vielen Fällen ein Personenbezug vorliegen. Wie der jeweilige Musikanbieter ist auch die 4FO AG dazu verpflichtet, die Nutzer über die beim Surfen auf der Website erfolgende Datenverarbeitung zu informieren und ihnen die Weitervermittlung zu anderen Diensteanbietern anzuzeigen³⁸.

Erstellung eines Nutzeraccounts (Dienst Accounterstellung) Die (fakultative) Erstellung eines Nutzeraccounts setzt voraus, dass der Nutzer einen Loginnamen, ein Passwort, seine Email-Adresse und das Land, in dem er sich aufhält, angibt. Diese Daten werden in vielen Fällen einen Personenbezug aufweisen³⁹. Für die Datenverarbeitung verantwortlich ist die 4FO AG, über deren Accounting-Server die Daten erhoben werden. Von der Datenverarbeitung betroffen ist der jeweilige (registrierungswillige) Nutzer, der Mitglied der Potato-Community werden und an dem Provisionssystem des PotatoSystems teilnehmen möchte. Bei dem Provisionssystem und der Potato-Community handelt es sich um Bestandteile eines elektronische Informations- und Kommunikationsdienstes, für den die Vorschriften des Telemediengesetzes (TMG) einschlägig sind⁴⁰. Die Zulässigkeit der Datenverarbeitung ergibt sich aus § 14 Abs. 1 TMG, weil alle erhobenen (Bestands)Daten zur Begründung bzw. inhaltlichen Ausgestaltung dieses Telemediendienstes erforderlich sind: Loginname und Passwort werden für eine spätere Anmeldung am System benötigt, die Angabe der Email-Adresse ist Voraussetzung für die Information des Nutzers und eine Kontaktaufnahme zu anderen Mitgliedern der

eine auf der Website abrufbare Datenschutzerklärung alleine (noch) nicht erfüllt wird. Dies ließe sich aus dem Umstand folgern, dass hier die Unterrichtung nicht automatisch erfolgt, sondern der Nutzer die Webseite mit der Datenschutzerklärung bewusst ansteuern und damit selbst aktiv werden muss.

³⁸§ 13 Abs. 1 S. 1, Abs. 5 TMG

³⁹So etwa dann, wenn die Email-Adresse den Vor- und Nachnamen des Nutzers enthält oder in einem öffentlichen Verzeichnis eingetragen ist

⁴⁰Vgl. § 1 Abs. 1 S. 1 TMG. Wie die Anwendungsbereiche von TKG, TMG und BDSG voneinander abzugrenzen sind, ist bereits im Abschnitt „Rechtliches Rahmengerüst“ (2.1.1.2) ausgeführt worden.

Community und die Nennung des Landes ist ebenfalls für die Communityfunktion erforderlich.

4.6.2.2 Datenverarbeitung bei Vertragsschluss

Einleitung des Bezahlvorgangs (Dienst Paybest) Hat der Nutzer ein Musikstück ausgewählt, so wird er von dem HTML-Server des PotatoSystems an dessen Payment-Server weitergeleitet. Zur Bezahlung verwendet das PotatoSystem den Dienst Paybest, welcher verschiedene Zahlungsmöglichkeiten bei unterschiedlichen Zahlungsmittelanbietern (so z. B. PayPal) zur Verfügung stellt. Die 4FO AG übermittelt dabei an den jeweiligen Anbieter keine Daten, die für diesen einen Personenbezug aufweisen. Die vom PotatoSystem selbst verwendete Session-ID dient der späteren Zuordnung von Kunde, Warenkorb und Bezahlung durch den Accounting-Server, weshalb ihre Verwendung nach § 15 Abs. 1 TMG zulässig ist.

Durchführung des Bezahlvorgangs (Zahlungsmittelanbieter) Je nach verwendetem Zahlungsmittel ist vorab eine Registrierung oder – soweit eine solche bereits bei anderer Gelegenheit erfolgt ist – eine Identifizierung durchzuführen. So muss der Kunde etwa bei der Bezahlung via PayPal zumindest seinen Namen und seine Post- und E-Mail-Adresse angeben. Insofern erforderliche personenbezogene Daten werden direkt an den jeweiligen Zahlungsmittelanbieter übermittelt. Verantwortliche Stelle für die Datenverarbeitung ist der jeweilige Zahlungsmittelanbieter. Da die Datenverarbeitung von Anbieter zu Anbieter variiert, würde eine datenschutzrechtliche Bewertung den Rahmen dieser Untersuchung sprengen und kann deshalb an dieser Stelle nicht erfolgen⁴¹.

Weitere Abwicklung des Kaufs (Dienst Kauf von Dateien) Bei Auslieferung der Ware werden eine Produktnummer und die Kundennummer, welche die 4FO AG dem jeweiligen Nutzer zugeordnet hat, zu einer eindeutigen Transaktionsnummer (TAN) zusammengefasst. Diese wird gespeichert und im Klartext in den Dateinamen des gekauften Produkts sowie in Verkaufslinks des Erwerbers, der ja nun im Rahmen des Provisionssystems selbst zum Anbieter wird, eingebracht.

Die in der TAN enthaltene Kundennummer kann über den zentralen Accounting-Server den Registrierungsdaten des jeweiligen Nutzers zugeordnet werden. Sofern die Registrierungsdaten für die 4FO AG einen Personenbezug

⁴¹Aus Sicht des Datenschutzes wäre übrigens eine möglichst weitgehende Etablierung anonymer Zahlungssysteme besonders zu begrüßen [Neu03].

aufweisen, gilt dies deshalb auch für die TAN. Diese dient der Zuordnung im Rahmen des Provisionsmodells des PotatoSystems und ist deshalb strukturell für dieses erforderlich. Sie ist als Nutzungsdatum des Distributionssystems anzusehen, weshalb ihre Verarbeitung gem. § 15 Abs. 1 TMG auch ohne Einwilligung des Nutzers zulässig ist. Allerdings müssen Nutzungsdaten nach Ende der Nutzung und erfolgter Abrechnung gelöscht oder zumindest gesperrt werden (vgl. § 15 Abs. 4 TMG). Hinsichtlich der TAN kann ein Ende der Nutzung jedoch nur dann angenommen werden, wenn der Nutzer einen Inhalt definitiv nicht mehr anbieten will. In einem solchen Falle ist die jeweilige TAN dann auch im PotatoSystem zu löschen.

Im Übrigen erscheint es als möglich, dass nicht nur die 4FO AG, sondern auch Zweiterwerber über die TAN und die in dieser enthaltenen Kundennummer einen Personenbezug herstellen können. Dies ließe sich etwa dadurch bewerkstelligen, dass die Verkaufslinks des ursprünglichen Erwerbers und späteren Anbieters, die ja ebenfalls die TAN und damit auch seine Kundennummer beinhalten, mit weiteren Daten über diesen verkettet werden. Hierzu könnten beispielsweise Daten verwendet werden, die dem Impressum auf dessen Verkaufswebseite entnommen werden können. § 13 Abs. 4 Nr. 3 TMG verpflichtet den Anbieter von Telemediendiensten dazu, durch technische und organisatorische Vorkehrungen sicherzustellen, dass Nutzer Telemedien gegen Kenntnisnahme Dritter geschützt in Anspruch nehmen können. Dies ist in der vorliegenden Konstellation aber wegen der soeben geschilderten Möglichkeit der Herstellung eines Personenbezugs durch Dritte gerade nicht gewährleistet.

4.6.2.3 Datenverarbeitung für andere Zwecke

Der Accounting-Server des PotatoSystems schafft für die 4FO AG die (technische) Möglichkeit der Erstellung umfangreicher Kundenprofile, welche mit Hilfe von einfachen Analysewerkzeugen, aber auch mittels spezieller Data Mining-Methoden ausgewertet werden können. Den Webseiteninformationen der 4FO AG zufolge wird eine solche Auswertung für die Vermittlung von Nutzern im Rahmen der Communityfunktion vorgenommen. Außerdem werden die Daten auch für die eigene Marktforschung der 4FO AG verwendet. In diesem Zusammenhang ist allerdings § 15 Abs. 3 TMG zu beachten, wonach die Erstellung von Nutzungsprofilen nur bei Verwendung von Pseudonymen erlaubt ist, und auch dies nur dann, wenn der Nutzer dem nicht widerspricht. Auf dieses Widerspruchsrecht hat der Diensteanbieter den Nutzer explizit hinzuweisen. Außerdem dürfen Nutzungsprofile nicht mit Daten über den Träger des Pseudonyms zusammengeführt werden. Dies hat der Dienstean-

bietet durch technische und organisatorische Vorkehrungen sicherzustellen⁴².

Des Weiteren bietet die 4FO AG die Möglichkeit eines sog. User-Matchings an: Diese Funktionalität ermöglicht es registrierten Mitgliedern, sich die Loginnamen anderer Mitglieder anzeigen zu lassen, die ähnliche Stücke gekauft haben. Im Anschluss hieran kann eine Liste eingesehen werden, die die Musikstücke enthält, die diese Personen erworben haben. Hierbei handelt es sich jedoch um eine optionale Möglichkeit, die der einzelne Nutzer für sich wählen kann. Aus Sicht des Datenschutzrechts liegt hier folglich eine Einwilligungslösung vor, welche als Opt-In-Verfahren auszugestalten ist.

4.6.2.4 Verborgene Schnittstellen und Verkettung von Funktionen

Baut ein Nutzer eine Verbindung zu einem Server des Potato-Systems auf, so werden jedes Mal Informationen über den verwendeten Browser, das eingesetzte Betriebssystem, die Sprache und das Herkunftsland übermittelt. Des Weiteren können Cookies für das Bezahlssystem Paybest aktiviert werden. Schließlich kann das PotatoSystem nur dann genutzt werden, wenn JavaScript und Popup-Windows aktiviert werden. Hierbei handelt es sich um Mechanismen, die sicherheitsrelevante Schwachstellen enthalten können, durch die es zu Schäden auf dem Rechner des Nutzers kommen kann. Hierüber sowie über mögliche Gegenmaßnahmen ist der Nutzer umfassend aufzuklären. Zudem sollte gegebenenfalls zu einer Deaktivierung dieser Mechanismen nach Beendigung der Nutzung des PotatoSystems geraten werden.

4.6.2.5 Zusicherung, Unterrichtung, Protokollierung und Auskunft

Zuzusichern ist hier durch die jeweilige Daten verarbeitende Stelle – Musikanbieter, 4FO bzw. Zahlungsmittelanbieter –, dass personenbezogene Daten ausschließlich zu den oben genannten (zulässigen) Zwecken wie z. B. Begründung und inhaltliche Ausgestaltung des Vertragsverhältnisses zur Nutzung des PotatoSystems verarbeitet werden. Wie oben ausführlich geschildert, ist der Nutzer nach Maßgabe des § 13 Abs. 1 Satz 1 TMG zu unterrichten. Ihm ist zudem die Weiterleitung zu einem anderen Diensteanbieter gem. § 13 Abs. 5 TMG anzuzeigen.

In den Logdateien der Webserver der verschiedenen verantwortlichen Stellen werden die Nutzungsdaten i. S. d. § 15 Abs. 1 TMG protokolliert. Insoweit ist noch einmal auf § 15 Abs. 4 TMG hinzuweisen: Nach dieser Vorschrift sind die Nutzungsdaten unmittelbar nach Ende der Nutzung zu löschen, wenn sie

⁴²§ 13 Abs. 4 Nr. 6 TMG

nicht für Abrechnungszwecke benötigt werden. Hinsichtlich der Beauskunftung des Nutzers ist § 13 Abs. 7 TMG einschlägig, wonach der Diensteanbieter den Nutzer nach Maßgabe des § 34 BDSG auf Verlangen Auskunft über die zu seiner Person oder zu seinem Pseudonym gespeicherten Daten zu erteilen hat. Diese Auskunft kann auch elektronisch erteilt werden, wenn der Nutzer hiermit einverstanden ist.

4.6.3 Hanival

In diesem Szenario werden Daten durch die folgenden Unternehmen bzw. Personen verarbeitet:

- Wiederverkäufer (relevanter Dienst: PaketauftragErteilen),
- Hanival (inkl. Organisationseinheit Webspaces; verschiedene relevante Dienste),
- Registrierungsstelle (relevante Dienste: Domain-Verfügbarkeitsprüfung und -registrierung),
- Internetzugangsanbieter (relevante Dienste: DSL-Verfügbarkeitsprüfung und -Auftragserteilung) und Zahlungsdienstleister

Bei der nachfolgenden rechtlichen Analyse wird die Anwendbarkeit deutschen Rechts unterstellt. In dieser Konstellation ist es aber grundsätzlich möglich, dass eine oder mehrere der für die Datenverarbeitung verantwortlichen Stellen außerhalb der EU und des EWR angesiedelt sind und dort auch die Verarbeitung personenbezogener Daten stattfindet. Auf die aus solchen internationalen Bezügen resultierenden spezifischen rechtlichen Probleme soll an dieser Stelle allerdings (noch) nicht näher eingegangen werden. Ausführungen zu dieser Thematik werden vielmehr erst in dem nachfolgenden Szenario Amazon Mechanical Turk erfolgen.

4.6.3.1 Verarbeitung der Daten durch die beteiligten Stellen

Auch in diesem Szenario werden (personenbezogene) Daten nicht nur von dem Vertragspartner des Kunden, dem Wiederverkäufer, sondern auch von anderen Stellen, nämlich Hanival und den verschiedenen Dienstleistungsanbietern, verarbeitet. Die datenschutzrechtliche Bewertung hängt wiederum davon ab, wie die vertraglichen Beziehungen zwischen den verschiedenen Beteiligten ausgestaltet sind. Nachfolgend wird davon ausgegangen, dass innerhalb dieses Szenarios keine Auftragsdatenverarbeitung vereinbart worden ist

und damit nicht nur der Wiederverkäufer, sondern auch Hanival und die verschiedenen Dienstleistungsunternehmen verantwortliche Stellen im Sinne des § 3 Abs. 7 BDSG (Artikel 2 d) EG-DatSchRL) sind⁴³. Für diese Annahme spricht, dass es nicht im Interesse von Hanival liegt, für die Datenverarbeitung eines – auch aus wirtschaftlichen Gründen - selbständigen Datenverarbeiters die Verantwortung für die Ordnungsmäßigkeit seiner Datenverarbeitung zu übernehmen. Aus Vereinfachungsgründen wird unterstellt, dass für die jeweilige Datenverarbeitung auch keine Einwilligung der betroffenen Kunden eingeholt wird. Eine solche Annahme entspricht der Erfahrung, dass Datenverarbeitende Stellen in der Regel eine gesonderte Interaktion über die datenschutzrechtliche Konformität eher zu vermeiden suchen, um den Nutzer ihrer Webseite nicht abzuschrecken. Die Zulässigkeit der Datenverarbeitung ist also auch innerhalb dieses Szenarios an den einschlägigen gesetzlichen Erlaubnistatbeständen des Datenschutzrechts zu messen.

Zulässigkeit der Datenverarbeitung Möchte ein Kunde mit dem Wiederverkäufer einen Vertrag über die Erbringung eines Paketes an ISP-Dienstleistungen abschließen, so gibt er auf dessen Website seine Kontaktdaten (Name, Adresse und Email-Adresse), seine Bankdaten und seine Wünsche hinsichtlich Domainname, Webpace und DSL-Geschwindigkeit in ein Formular ein. Der Wiederverkäufer übermittelt sämtliche dieser Daten an Hanival, woraufhin Hanival seinerseits die für die Erbringung der einzelnen Dienstleistungen benötigten Daten an das jeweilige Dienstleistungsunternehmen weiterleitet. Betrachtet man die Datenflüsse in diesem Szenario, so ist festzustellen, dass nicht nur der Wiederverkäufer und Hanival, sondern auch alle beteiligten Dienstleistungsunternehmen personenbezogene Daten verarbeiten. Wie bereits erwähnt, ist zwischen den Beteiligten keine Auftragsdatenverarbeitung vereinbart worden, weshalb jede der beteiligten Organisationen verantwortliche Stelle im Sinne des Datenschutzrechts ist.

Bei den in Rede stehenden personenbezogenen Daten des Kunden handelt es sich um sogenannte Inhaltsdaten⁴⁴, so dass hinsichtlich ihrer Verarbeitung die Regelungen des Bundesdatenschutzgesetzes zur Anwendung kommen. Da keine Einwilligung des Kunden eingeholt wird, muss sich jede der beteiligten Stellen bei der Verarbeitung von personenbezogenen Daten auf einen gesetzlichen Erlaubnistatbestand stützen können. Insoweit ist von Bedeutung, zu welchen Zwecken die Daten jeweils verarbeitet werden:

⁴³Etwas anderes gilt nur für Hanival Webpace, da es sich hierbei lediglich um eine unselbständige Organisationseinheit von Hanival handelt, weshalb Hanival für die von Hanival Webpace vorgenommene Datenverarbeitung verantwortlich ist.

⁴⁴Gleiches galt auch schon für die im Szenario Amazon Mechanical Turk verarbeiteten Kundendaten. Im Übrigen sind auch hier wieder die Vorschriften des Telemediengesetzes zu beachten, wenn der Kunde auf der Website des Wiederverkäufers surft.

Der Wiederverkäufer verarbeitet die Daten zur Erfüllung seines ISP-Vertrages mit dem Kunden. Zwischen der Registrierungsstelle und dem Kunden als (künftigem) Domaininhaber kommt es ebenfalls zum Abschluss eines Vertrags (über die Registrierung einer Internet-Domain)⁴⁵, zu dessen Erfüllung die Registrierungsstelle die Daten des Kunden verarbeitet. Hingegen besteht kein Vertragsverhältnis des Kunden mit Hanival, dem Internetzugangsanbieter und dem vom Wiederverkäufer eingeschalteten Zahlungsdienstleister. Diese verarbeiten die personenbezogenen Daten des Kunden, um ihre vertraglichen Verpflichtungen gegenüber dem Wiederverkäufer bzw. untereinander zu erfüllen.

Folglich lässt sich die Datenverarbeitung durch den Wiederverkäufer und die Registrierungsstelle auf § 28 Abs. 1 Satz 1 Nr. 1 BDSG stützen. Hinsichtlich der Datenverarbeitung durch Hanival, den Internetzugangsanbieter und den Zahlungsdienstleister kommt als Erlaubnistatbestand hingegen § 28 Abs. 1 Satz 1 Nr. 2 BDSG in Betracht. Jedenfalls wenn der Kunde bei Abschluss des Vertrages mit dem Wiederverkäufer über die Mitwirkung dieser Stellen informiert wird, ist die Datenverarbeitung durch sie zulässig, weil sie zur Vertragserfüllung gegenüber dem Wiederverkäufer erforderlich ist und kein Grund zu der Annahme besteht, dass ein überwiegendes schutzwürdiges Interesse des Kunden an dem Ausschluss der Verarbeitung besteht. Dieser hat ja schließlich selbst ein Interesse daran, dass die genannten Stellen, über deren Einschaltung er auch informiert worden ist, an der Erfüllung seines Vertrags mit dem Wiederverkäufer mitwirken.

Da stets nur die für die Erreichung des konkret verfolgten (zulässigen) Zwecks erforderlichen Daten übermittelt werden, sind die im Szenario beschriebenen Datenverarbeitungsvorgänge aus datenschutzrechtlicher Sicht zulässig. Im Übrigen ist auch hier wieder wegen der Vielzahl der Daten verarbeitenden Stellen ein besonderes Augenmerk auf die Gewährleistung des gesetzlich vorgeschriebenen Maßes an Transparenz zu richten.

Sonderfall: Abbruch des Bestellvorgangs Ist die Bereitstellung eines der in dem durch den Wiederverkäufer (bzw. Hanival) angebotenen ISP-Paket enthaltenen Dienste nicht möglich, so bricht Hanival den Bestellvorgang ab. Hierüber wird der Wiederverkäufer informiert, welcher seinerseits den Kunden über den Abbruch unterrichtet. Kommt es zu einem solchen Abbruch, so muss sichergestellt sein, dass die personenbezogenen Daten

⁴⁵Dies gilt jedenfalls bei der Vergabe von .de-Domains durch die DENIC (vgl. die FAQs der DENIC für Domainanmelder, abrufbar unter <http://www.denic.de/de/faqs/domainanmelder/index.html>). Der Registrierungsvertrag kommt durch Bestätigung oder Durchführung der Registrierung seitens DENIC zustande.

des Kunden unverzüglich von allen verantwortlichen Stellen gelöscht werden. Nach § 35 Abs. 2 Satz 2 Nr. 1 BDSG sind nämlich personenbezogene Daten zu löschen, wenn ihre Speicherung unzulässig ist⁴⁶. Dies ist im Falle eines Abbruchs des Bestellvorgangs der Fall, da die Rechtsgrundlage für die Speicherung der Daten durch den Abbruch entfällt. Allerdings bleibt es dem Kunden unbenommen, zu einem späteren Zeitpunkt einen erneuten Bestellvorgang einzuleiten und dem Wiederverkäufer – und damit auch den anderen Stellen – erneut seine Daten mitzuteilen.

Zusicherung, Unterrichtung, Protokollierung und Auskunft In diesem Szenario ist durch jede der Daten verarbeitenden Stellen – Wiederverkäufer, Hanival, Registrierungsstelle, Internetzugangsanbieter und Zahlungsdienstleister – zuzusichern, dass personenbezogene Daten ausschließlich zur Erfüllung des Vertrags des Endkunden mit dem Wiederverkäufer bzw. zur Erfüllung des Vertrags des Kunden mit der Registrierungsstelle verarbeitet werden. Der Kunde ist bei der Erhebung seiner personenbezogenen Daten durch den Wiederverkäufer gem. § 4 Abs. 3 BDSG über dessen Identität, die Zweckbestimmung der Erhebung, Verarbeitung und Nutzung sowie die Kategorien von Empfängern zu unterrichten. Die Unterrichtung sollte dabei auf der Webseite, auf der der Kunde seine Daten in ein Formular eingibt, erfolgen. Werden seine Daten erstmals von einer der anderen Daten verarbeitenden Stellen gespeichert, so hat diese den Kunden gem. § 33 Abs. 1 Satz 1 BDSG zu benachrichtigen. Diese Benachrichtigungspflicht entfällt allerdings dann, wenn der Wiederverkäufer auf der Webseite nicht nur über die Kategorien von Empfängern unterrichtet hat, sondern alle Empfänger auch schon namentlich genannt hat [DKWW07, § 4 Rn. 14].

Hinsichtlich der beim Surfen des Nutzers auf der Website des Wiederverkäufers anfallenden Nutzungsdaten gilt abermals § 15 Abs. 4 Satz 1 TMG, wonach diese in der Logdatei des Webservers protokollierten Daten grundsätzlich unmittelbar nach Ende der Nutzung zu löschen sind. Bezüglich der im vorliegenden Szenario im Vordergrund stehenden Inhaltsdaten sollten die verschiedenen verantwortlichen Stellen jeweils dafür Sorge tragen, dass alle Datenflüsse protokolliert werden, die für die vollständige Beauskunftung von Kunden benötigt werden. Macht der Kunde seinen Auskunftsanspruch gem. § 34 BDSG geltend, so ist jede der verantwortlichen Stellen hinsichtlich der von ihr durchgeführten Datenverarbeitung zur Beauskunftung des Betroffe-

⁴⁶Hinsichtlich der Nutzungsdaten nach TMG, die beim Surfen in der Beziehung Client-Server angefallen sind, gilt hier wiederum § 15 Abs. 4, wonach Nutzungsdaten nach Ende des Nutzungsvorgangs zu löschen sind, wenn sie nicht für Abrechnungszwecke benötigt werden.

nen verpflichtet. Insoweit könnte in Betracht gezogen werden, dem Kunden einen zentralen Auskunftsservice zur Verfügung zu stellen, den er auf der Website seines Vertragspartners (des Wiederverkäufers) aufrufen kann und der ihm als Ergebnis eine umfassende Beauskunftung durch alle in den Bestellvorgang involvierten verantwortlichen Stellen liefert.

4.6.4 Amazon Mechanical Turk

In diesem Szenario werden Daten zum Zwecke der Übersetzung einer Supportanfrage durch die folgenden Unternehmen bzw. Personen verarbeitet:

- Zettasoft (relevante Dienste: Anfrageannahme und Auftragsannahme),
- von Kempelen (relevanter Dienst: Auftragsannahme),
- Amazon Mechanical Turk (relevanter Dienst: Datenübertragung HIT)
- und die Amazon Mechanical Turk (AMT)-Arbeiter

Bei der nachfolgenden rechtlichen Analyse wird die Anwendbarkeit deutschen Rechts unterstellt. In dieser Konstellation ist es aber grundsätzlich möglich, dass eine oder mehrere der für die Datenverarbeitung verantwortlichen Stellen außerhalb der EU und des EWR angesiedelt sind und dort auch die Verarbeitung personenbezogener Daten stattfindet. Auf die aus solchen internationalen Bezügen resultierenden spezifischen rechtlichen Probleme soll an dieser Stelle allerdings (noch) nicht näher eingegangen werden. Ausführungen zu dieser Thematik werden vielmehr erst in dem nachfolgenden Szenario Amazon Mechanical Turk erfolgen.

4.6.4.1 Analyse des Szenarios unter Zugrundelegung deutschen Rechts

Im vorliegenden Szenario werden (personenbezogene) Daten nicht nur von dem Vertragspartner des Kunden, Zettasoft, sondern auch von den Unternehmen von Kempelen und Amazon Mechanical Turk sowie von verschiedenen AMT-Arbeitern verarbeitet. Die datenschutzrechtliche Bewertung wird dabei maßgeblich davon bestimmt, wie die vertraglichen Beziehungen zwischen den verschiedenen Beteiligten ausgestaltet sind. So ist grundsätzlich eine vertragliche Ausgestaltung möglich, welche dazu führt, dass mehrere oder sogar alle von ihnen als verantwortliche Stelle i. S. d. § 3 Abs. 7 BDSG (Artikel 2 d) EG-DatSchRL) anzusehen sind (hierzu vgl. die bereits behandelten Szenarien). In diesem Szenario hat allerdings Zettasoft als Vertragspartner

des Kunden mit allen anderen beteiligten Stellen eine Auftragsdatenverarbeitung – direkt bzw. im Wege einer Unterauftragsverarbeitung – vereinbart, weshalb die Verantwortung für jegliche im Rahmen des Szenarios stattfindende Datenverarbeitung alleine bei Zettasoft liegt, wohingegen die anderen beteiligten Stellen personenbezogene Daten nur entsprechend den Weisungen von Zettasoft bzw. des jeweiligen Unterauftraggebers verarbeiten dürfen (§ 11 BDSG, Artikel 17 EG-DatSchRL).

Im Übrigen sei vorab schon darauf hingewiesen, dass das Datenschutzrecht dann nicht anwendbar ist, wenn Daten von natürlichen Personen ausschließlich für persönliche oder familiäre Tätigkeiten verwendet werden⁴⁷. Eine solche – rein private – Verwendung personenbezogener Daten unterliegt also keinen rechtlichen Restriktionen und ist folglich uneingeschränkt zulässig.

Da die AMT-Arbeiter für ihre Übersetzungstätigkeit nur eine geringe Vergütung erhalten, könnte man zu dem Schluss kommen, dass sie diese Tätigkeit und die mit ihr verbundene Datenverarbeitung lediglich zu privaten Zwecken – quasi als eine Art Hobby – vornehmen. Allerdings kann nicht ausgeschlossen werden, dass zumindest einige der AMT-Arbeiter auch aus kommerziellen Interessen heraus handeln, weshalb auch bei der Datenverarbeitung durch die AMT-Arbeiter stets von einer Anwendbarkeit des Datenschutzrechts ausgegangen werden muss.

Erhebung der Kundendaten (Dienst Anfrageannahme) Will ein Kunde seine Rechte aus dem Supportvertrag mit Zettasoft geltend machen und eine Supportanfrage stellen, so gibt er auf der entsprechenden Webseite des Unternehmens seine Kundennummer, seine Email-Adresse, die gewünschte Sprache sowie den Anfragetext in ein Formular ein. Zettasoft kann die Kundennummer dem jeweiligen Vertragspartner zuordnen, weshalb die genannten Daten für das Unternehmen einen Personenbezug aufweisen und folglich dem Regime des Datenschutzrechts unterfallen. Da der jeweilige Kunde die Daten zwecks Wahrnehmung seiner Rechte aus dem Supportvertrag angibt und Zettasoft hierzu ein spezielles Formular auf seiner Website anbietet, liegt auch ein Beschaffen von Daten über den Betroffenen und damit ein Erheben i. S. d. § 3 Abs. 3 BDSG (Artikel 2 b) EG-DatSchRL) vor. Bei der Mitteilung der genannten Daten handelt es sich um einen Kommunikationsvorgang mit individuellem Inhalt und damit um sog. Inhaltsdaten, weshalb die Regelungen des Bundesdatenschutzgesetzes zur Anwendung kommen⁴⁸.

⁴⁷§ 1 Abs. 2 Nr. 3 BDSG (Artikel 3 Abs. 2 EG-DatSchRL)

⁴⁸Surft der Kunde auf der Website von Zettasoft, so sind daneben natürlich auch wieder die Vorschriften des Telemediengesetzes zu beachten. Insoweit wird auf das vorangegan-

Weil die Datenerhebung für die Erfüllung der Pflichten aus dem Supportvertrag zwischen Zettasoft und dem jeweiligen Kunden erforderlich ist, ist sie nach § 28 Abs. 1 Satz 1 Nr. 1 BDSG (Artikel 7 b) EG-DatSchRL) zulässig.

Zettasoft ist als verantwortliche Stelle gem. § 4 Abs. 3 BDSG (Artikel 10 EG-DatSchRL) nicht nur dazu verpflichtet, den Kunden über seine Identität und die Zweckbestimmung der Datenverarbeitung zu unterrichten, sondern ihm auch die Kategorien von Empfängern – also Personen oder Stellen, die seine Daten erhalten – mitzuteilen. Dies gilt nicht nur für die Übermittlung⁴⁹ von Daten an Dritte, sondern auch für ihre Weitergabe an Auftragnehmer [DKWW07, § 4 Rn. 13]. Die Unterrichtungspflicht besteht allerdings nur dann, wenn der Betroffene nach den Umständen des Einzelfalles nicht mit der Weitergabe an weitere Stellen rechnen muss. Dies ist im vorliegenden Szenario der Fall, da der Kunde zunächst einmal davon ausgehen kann, dass seine Support-Anfrage ausschließlich von den Mitarbeitern von Zettasoft bearbeitet wird. Folglich ist der jeweilige Kunde über die Einschaltung der Unternehmen von Kempelen und Amazon Mechanical Turk sowie mehrerer AMT-Mitarbeiter zu unterrichten. Auch wenn dies bereits bei Abschluss des Supportvertrages geschehen ist, hat eine Unterrichtung auch auf der Internetpräsenz der Zettasoft zu erfolgen⁵⁰. Entsprechende Informationen sollten dabei auf der Webseite bereitgestellt werden, über die der Kunde das bei der Anfrage verwendete Eingabeformular aufrufen kann.

Weitergabe der Daten an von Kempelen (Dienst Auftragsannahme) Zettasoft gibt nur den Text der Supportanfrage, die Information über die gewählte Sprache und eine Referenznummer zur Zuordnung der Anfrage, hingegen nicht die Kundennummer und die Email-Adresse an von Kempelen weiter. Es handelt sich hierbei also um eine Pseudonymisierung⁵¹ der Daten mit dem Ergebnis, dass der betroffene Kunde nach dem Entfernen von Kundennummer und Email-Adresse von von Kempelen, Amazon und den AMT-Arbeitern grundsätzlich nicht mehr bestimmt werden kann, da ledig-

gene Szenario „Modell PotatoSystem“ verwiesen. Im Übrigen vgl. zur Abgrenzung des Anwendungsbereichs von TKG, TMG und BDSG bereits den Abschnitt „Rechtliches Rahmengerüst“ (2.1.1.2).

⁴⁹Dieser Begriff findet sich zwar in dem hier einschlägigen § 4 Abs. 3 S. 1 Nr. 3 BDSG, ist aber als Redaktionsversehen anzusehen [GS05, § 4 Rn. 33].

⁵⁰Zwar entfällt die Unterrichtungspflicht des § 4 Abs. 3 BDSG, wenn der Betroffene bereits auf andere Weise Kenntnis erlangt hat. Erforderlich ist insoweit aber ein enger zeitlicher Zusammenhang zwischen dem Zugang der Informationen und der Erhebung der Daten, weil die verantwortliche Stelle nur dann davon ausgehen kann, dass dem Betroffenen die Informationen auch tatsächlich (noch) bewusst sind [Sim06, § 4 Rn. 40]. Hiervon kann aber in der vorliegenden Konstellation nicht ausgegangen werden.

⁵¹Der Begriff des Pseudonymisierens wird in § 3 Abs. 6a BDSG legaldefiniert.

lich Zettasoft über die Zuordnungsregel (Referenznummer - Kunde) verfügt. Dies ist allerdings nicht immer der Fall: Gibt der Kunde in seiner Supportanfrage Informationen über sich preis, die Rückschlüsse auf seine Person zulassen, so kann schon der Anfragetext für sich betrachtet einen Personenbezug aufweisen⁵². Da Kundennummer und Email-Adresse automatisch vom Anfragetext abgetrennt werden und somit keine Überprüfung durch einen Menschen erfolgt, muss damit stets vom Vorhandensein eines Personenbezugs ausgegangen werden. Folglich ist nicht nur die Erhebung, sondern auch die Weitergabe der Daten an von Kempelen an den einschlägigen Vorschriften des Datenschutzrechts zu messen⁵³. Da diese Weitergabe – wie auch schon die Erhebung der Daten – der Zweckbestimmung des Supportvertrages dient, ist auch sie nach § 28 Abs. 1 Satz 1 Nr. 1 BDSG (Artikel 7 b) EG-DatSchRL) zulässig.

Verarbeitung der Daten durch die verschiedenen Auftragnehmer

Wie bereits erwähnt, ist der Auftraggeber für die Einhaltung der datenschutzrechtlichen Bestimmungen verantwortlich, wenn personenbezogene Daten im Auftrag durch andere Stellen erhoben, verarbeitet oder genutzt werden. Hingegen darf der Auftragnehmer die Daten nur im Rahmen der Weisungen des Auftraggebers verarbeiten.

Voraussetzung hierfür ist allerdings, dass tatsächlich ein Auftragsverhältnis i. S. d. § 11 BDSG (Art. 17 EG-DatSchRL) vorliegt⁵⁴. Insoweit müssen zwischen Zettasoft einerseits und von Kempelen, Amazon Mechanical Turk und den AMT-Arbeitern⁵⁵ andererseits vertragliche Regelungen getroffen werden, die so ausgestaltet sind, dass Letztere bei der Datenverarbeitung lediglich eine Hilfs- und Unterstützungsfunktion haben. Zudem ist jeder (Unter)Auftrag gem. § 11 Abs. 2 Satz 2 BDSG (vgl. auch Artikel 17 Abs. 4 EG-DatSchRL) schriftlich zu erteilen. Hierbei müssen die Datenerhebung, -verarbeitung oder -nutzung, die technischen und organisatorischen Maßnah-

⁵²Nicht näher berücksichtigt wird vorliegend der Umstand, dass die Supportanfrage auch Informationen über andere Personen enthalten kann, durch die diese in manchen Fällen (ebenfalls) bestimmt werden können.

⁵³Gleiches gilt im Übrigen auch für die Verwendung der Daten durch anderen beteiligten Stellen.

⁵⁴Das der Auftragsverarbeitung zugrunde liegende Rechtsverhältnis muss kein Auftrag im Sinne von § 662 BGB sein, vielmehr wird es sich häufig um einen Dienst-, Werk- oder Geschäftsbesorgungsvertrag bzw. um Gestaltungen im Rahmen bereits bestehender Geschäftsbeziehungen handeln [GS05, § 11 Rn. 6].

⁵⁵Nicht nötig wäre eine Beauftragung der AMT-Arbeiter hingegen, wenn diese Angestellte von AMT oder von Kempelen wären und Telearbeit erbringen würden. Arbeitnehmer sind nämlich nicht als eigenständige Daten verarbeitende Stelle, sondern als Teil des jeweiligen Unternehmens anzusehen.

men und etwaige Unterauftragsverhältnisse festgelegt werden. Im vorliegenden Szenario müssten also von Kempelen, Amazon Mechanical Turk und die an einer Übersetzung beteiligten AMT-Arbeiter – direkt von Zettasoft bzw. im Wege eines Unterauftrags – schriftlich beauftragt werden. Hinsichtlich der AMT-Arbeiter besteht insoweit das Problem, dass zunächst einmal nicht feststeht, welche Arbeiter überhaupt an Übersetzungen mitwirken werden. Ein praktikable – wenn auch mit einigem Aufwand verbundene – Lösung könnte hier darin liegen, dass alle Arbeiter, die den Qualifikationstest von von Kempelen bestanden haben und somit als Übersetzer zum Einsatz kommen können und wollen, durch das Übersetzungsunternehmen im Wege eines Unterauftrags beauftragt werden⁵⁶. Alternativ könnten diese Arbeiter (auf Vermittlung von von Kempelen hin) auch direkt durch Zettasoft beauftragt werden.

Generell trifft jeden Auftraggeber die Pflicht, den Auftragnehmer unter besonderer Berücksichtigung der Eignung der von ihm getroffenen technischen und organisatorischen Maßnahmen sorgfältig auszusuchen⁵⁷. Zudem hat der Auftraggeber sich von der Einhaltung der beim Auftragnehmer getroffenen technischen und organisatorischen Maßnahmen zu überzeugen⁵⁸. Auch dies könnte im Hinblick auf die hohe Zahl von AMT-Arbeitern, die als Übersetzer in Betracht kommen, problematisch sein. Allerdings muss die Überprüfung der technischen und organisatorischen Maßnahmen nicht unbedingt „vor Ort“ erfolgen, sondern es können im konkreten Einzelfall auch weniger aufwändige Maßnahmen zur Erfüllung dieser Pflicht ausreichen [Sim06, § 11 Rn. 45 f.]. So würde es im vorliegenden Szenario wohl genügen, wenn die AMT-Arbeiter vertraglich dazu verpflichtet würden, eine aktuelle Virenssoftware und eine Firewall zu verwenden sowie regelmäßig aktuelle Updates ihres Betriebssystems zu installieren. Dies erscheint deshalb als ausreichend, weil die Arbeiter im Rahmen ihrer Übersetzungstätigkeit lediglich eine Webseite mit dem zu übersetzenden Text und einem Formular abrufen und dieses nach Eingabe des übersetzten Textes an Amazon Mechanical Turk zurücksenden. Im Übrigen kann in dieser und ähnlichen Konstellationen die Verwendung von Application Service Providing (ASP) sinnvoll sein, da der Auftraggeber

⁵⁶Allerdings zeigt dieses Beispiel, dass das Instrument der Auftragsdatenverarbeitung zwar relativ problemlos in virtuellen Organisationen mit festen Beteiligten eingesetzt werden kann, aber dann an seine Grenzen stößt, wenn im Vorhinein noch nicht absehbar ist, welche Organisationen oder Personen Daten verarbeiten werden. In solchen Fällen wird es vielfach nicht praktikabel sein, mit allen potentiellen Mitwirkenden eine schriftliche Vereinbarung abzuschließen.

⁵⁷§ 11 Abs. 2 S. 1 BDSG (Artikel 17 Abs. 2 EG-DatSchRL 1. Hs)

⁵⁸§ 11 Abs. 2 S. 4 BDSG (Artikel 17 Abs. 2 2. Hs. EG-DatSchRL) Es reicht nicht, wenn der Auftraggeber dies nur zu Beginn der Auftragsdatenverarbeitung tut, erforderlich ist vielmehr eine fortlaufende Überprüfung.

dann überwiegend selbst dafür sorgen kann, dass die erforderlichen technischen und organisatorischen Maßnahmen getroffen werden.

4.6.4.2 Zusicherung, Unterrichtung, Protokollierung und Auskunft

Es ist bereits mehrfach darauf hingewiesen worden, dass bei der Auftragsdatenverarbeitung nur der Auftraggeber für die Datenverarbeitung verantwortlich ist, wohingegen Auftragnehmer Daten lediglich im Rahmen seiner Weisungen verarbeiten dürfen. Folglich müssen Zusicherungen, die der Auftraggeber hinsichtlich der Datenverarbeitung gemacht hat, stets auch von den Auftragnehmern eingehalten werden. Konkret besteht die Zusicherung im vorliegenden Szenario darin, dass die Daten der Kunden nur zur Erfüllung des Supportvertrages und insbesondere zur Übersetzung der Supportanfrage und -antwort verwendet werden. Werden personenbezogene Daten eines Kunden erstmalig bei einem der Auftragnehmer gespeichert, so ist der betroffene Kunde hiervon gem. § 33 Abs. 1 Satz 1 BDSG (Artikel 11 EG-DatSchRL) zu benachrichtigen. Die Benachrichtigungspflicht trifft wiederum den Auftraggeber als verantwortliche Stelle [DKWW07, § 33 Rn. 10], im vorliegenden Szenario also Zettasoft. Hat die verantwortliche Stelle allerdings im Rahmen ihrer Unterrichtungspflicht gemäß § 4 Abs. 3 BDSG nicht nur die Kategorien der Empfänger, sondern auch schon die jeweilige Stelle oder Person benannt, so entfällt die entsprechende Benachrichtigungspflicht nach § 33 BDSG [DKWW07, § 4 Rn. 14]. Vorliegend können allerdings die konkret zum Einsatz kommenden AMT-Arbeiter vorab (noch) nicht benannt werden, weshalb der jeweilige Kunde jedenfalls dann benachrichtigt werden muss, wenn die tatsächlich involvierten AMT-Arbeiter die Daten erstmals speichern. Die Benachrichtigung muss unverzüglich – also gem. § 121 BGB ohne schuldhaftes Zögern – erfolgen, wobei allerdings betriebliche Erfordernisse berücksichtigt werden können [GS05, § 33 Rn. 15]. Insoweit wäre es im vorliegenden Szenario wohl ausreichend, wenn der Kunde erst nach Abschluss der Übersetzung von Supportanfrage und -antwort über die Speicherung bei den beteiligten AMT-Arbeitern benachrichtigt würde⁵⁹.

Hinsichtlich der beim Surfen des Nutzers auf der Website von Zettasoft anfallenden Nutzungsdaten gilt wiederum § 15 Abs. 4 Satz 1 TMG, wonach diese in der Logdatei des Webservers protokollierten Daten grundsätzlich

⁵⁹Voraussetzung hierfür wäre natürlich eine zeitnahe Bearbeitung und Beantwortung der Supportanfrage. Innerhalb welches Zeitraums eine Benachrichtigung in gesammelter Form erfolgen muss, ist in der Literatur übrigens umstritten: Während [GS05, § 33 Rn. 15] eine Benachrichtigung zum Monatsende für ausreichend halten, ist [Sim06, § 33 Rn. 41] der Ansicht, dass die Benachrichtigung innerhalb weniger Tage zu erfolgen hat.

unmittelbar nach Ende der Nutzung zu löschen sind. Bezüglich der im vorliegenden Szenario im Vordergrund stehenden Inhaltsdaten sollte Zettasoft als verantwortliche Stelle dafür Sorge tragen, dass alle Datenflüsse protokolliert werden, die für die vollständige Beauskunftung von Kunden benötigt werden. § 11 Abs. 1 Satz 2 BDSG stellt klar, dass Zettasoft als Auftraggeber auch für die Wahrung der Rechte des Betroffenen auf Auskunft, Berichtigung, Löschung, Sperrung oder Schadensersatz verantwortlich ist. Macht im vorliegenden Szenario ein Kunde also seinen Auskunftsanspruch geltend, so ist Zettasoft für die richtige und vollständige Beauskunftung verantwortlich.

4.6.4.3 Berücksichtigung der internationalen Bezüge des Szenarios

Nach dem vorliegenden Szenario hält sich der die Supportanfrage stellende Kunde in der Bundesrepublik Deutschland auf. Hingegen befindet sich der Sitz von Zettasoft, von Kempelen und Amazon Mechanical Turk in den USA, wo auch die von diesen Stellen jeweils vorgenommene Datenverarbeitung stattfindet⁶⁰. Die AMT-Arbeiter schließlich können sich an jedem Ort befinden, an dem ein Internetzugang zur Verfügung steht. Da es hier um die Übersetzung einer in deutscher Sprache gestellten Supportanfrage geht, wird aber davon ausgegangen, dass sich zumindest einer der vier involvierten AMT-Arbeiter in der Bundesrepublik Deutschland aufhält. Damit „wandert“ die Supportanfrage zunächst aus Deutschland und dem Bereich der Europäischen Union bzw. des Europäischen Wirtschaftsraumes hinaus in die Vereinigten Staaten von Amerika und danach wieder zurück nach Deutschland bzw. weiter in andere Staaten, in denen sich die einzelnen AMT-Arbeiter befinden. Auch wenn im vorigen Satz nur ein Teil des Gesamtprozesses der Übersetzung von Supportanfrage und -antwort beschrieben worden ist, dürfte hierdurch bereits deutlich geworden sein, wie leicht und oft es im Zeitalter von SOA und Internet zu einer grenzüberschreitenden Weitergabe personenbezogener Daten kommen kann. Dies hat natürlich auch Konsequenzen für das jeweils anwendbare nationale Recht und das durch dieses gewährleistete Datenschutzniveau.

Unterschiedliches Schutzniveau (EU/EWR – Drittstaaten) Während man mit guten Gründen vertreten kann, dass das Ausfüllen und Absenden des Supportformulars durch den Kunden eine Datenerhebung darstellt,

⁶⁰Etwas anderes gilt nach der hier vertretenen Ansicht nur für die Erhebung der Daten durch Zettasoft (hierzu sogleich).

die nach deutschem Recht zu beurteilen ist⁶¹, richtet sich die weitere Datenverarbeitung durch Zettasoft, von Kempelen und Amazon Mechanical Turk nach US-amerikanischem Recht, weil sie auf dem Hoheitsgebiet der USA und gerade nicht in Deutschland stattfindet (vgl. § 1 Abs. 5 S. 2 BDSG).

Insoweit ist an dieser Stelle noch einmal darauf hinzuweisen, dass innerhalb der Europäischen Union und des Europäischen Wirtschaftsraums durch die EU-Datenschutzrichtlinien 95/46/EG und 2002/58/EG ein einheitlicher Mindeststandard für die Verarbeitung personenbezogener Daten geschaffen worden ist. Das hierdurch gewährleistete Datenschutzniveau ist dabei deutlich höher als das, welches in den meisten anderen Staaten (so auch in den Vereinigten Staaten von Amerika) durch die jeweils anwendbaren nationalen Gesetze garantiert wird. Werden personenbezogene Daten von einer in Europa belegenen Daten verarbeitenden Stelle in einen sog. unsicheren Drittstaat (z. B. die USA) übermittelt, so ist dies nach § 4b f. BDSG (Artikel 25 f. EG-DatSchRL) nur unter bestimmten Voraussetzungen zulässig, welche das Vorliegen eines angemessenen Datenschutzniveaus sicherstellen sollen. Vorliegend übersendet der betroffene Kunde seine Daten selbst an Zettasoft, weshalb die genannten Vorschriften nicht einschlägig sind. Besonders wichtig ist in diesem Zusammenhang, dass dem Kunden überhaupt bewusst ist, dass seine Daten in einem Drittstaat unter den Bedingungen eines niedrigeren Schutzniveaus verarbeitet werden. Er kann sein Recht auf informationelle Selbstbestimmung nur dann sinnvoll ausüben, wenn er auch entsprechend über die Datenverarbeitungsbedingungen informiert worden ist. Sofern eine (umfassend informierte) Person dazu bereit ist, das in einem unsicheren Drittstaat bestehende erhöhte Risiko eines Missbrauchs ihrer personenbezogenen Daten in Kauf zu nehmen, bleibt es ihr natürlich unbenommen, ihre Daten einer dort belegenen Stelle zur Verfügung zu stellen. Eine andere Person, die dieses Risiko nicht eingehen möchte, kann die Übersendung personenbezogener Daten hingegen davon abhängig machen, dass die in dem Drittstaat belegene Stelle ihr vertraglich zusichert, sich Einschränkungen bei der Verarbeitung ihrer personenbezogenen Daten zu unterwerfen⁶². Sollte die jeweilige Stelle IT-Produkte oder Verfahren verwenden, die von einer unabhängigen

⁶¹Dies deshalb, weil Zettasoft durch die Gestaltung der Formularseite darüber bestimmt, in welcher Weise der in Deutschland belegene Rechner des Kunden eingesetzt wird (vgl. Art. 4 Nr. 1 c) EG-DatSchRL).

⁶²Beispielsweise könnte sich ein US-Unternehmen gegenüber dem Kunden freiwillig zur Einhaltung der sog. Safe Harbor-Prinzipien oder der EU-Standardvertragsklauseln verpflichten. Hierzu jeweils ausführlich [Sim06, § 4b Rn. 70 ff.] (Safe Harbor) und [Sim06, § 4c Rn. 50 ff.] (Standardvertragsklauseln).

Stelle als datenschutzkonform zertifiziert⁶³ worden sind, könnte die betroffene Person auch dies bei ihrer Entscheidungsfindung berücksichtigen.

Auswirkungen auf die rechtliche Analyse des Szenarios Auf die Datenverarbeitung durch Zettasoft, von Kempelen und Amazon Mechanical Turk findet weder deutsches noch EU-, sondern US-amerikanisches Datenschutzrecht Anwendung, weshalb eine Auftragsdatenverarbeitung im Sinne des § 11 BDSG (Artikel 17 EG-DatSchRL) ausscheidet. Gleiches gilt auch für AMT-Arbeiter, die sich weder in Deutschland noch in der Europäischen Union bzw. im Europäischen Wirtschaftsraum aufhalten. Folglich wäre hier nun eigentlich unter Berücksichtigung des einschlägigen US-amerikanischen Datenschutzrechts zu prüfen, wie die genannten Stellen eine rechtskonforme Datenverarbeitung sicherstellen können. Eine solche Prüfung muss an dieser Stelle aber deshalb unterbleiben, weil sie den Rahmen dieser Untersuchung sprengen würde. Pauschal lässt sich allerdings sagen, dass die in den USA angesiedelten Stellen angesichts des geringeren Schutzniveaus der dortigen Datenschutzregeln insgesamt wesentlich leichter datenschutzkonform agieren können als dies bei Anwendbarkeit des deutschen bzw. europäischen Rechts der Fall wäre. Im Übrigen sei noch einmal darauf hingewiesen, dass sich ein dem deutschen bzw. europäischen vergleichbares Schutzniveau in einer solchen Konstellation dadurch erzielen lässt, dass die Daten verarbeitende Stelle ihren Kunden entsprechende vertragliche Zusicherungen macht.

Sofern ein AMT-Arbeiter sich in Deutschland aufhält, kommt hinsichtlich der durch ihn vorgenommenen Datenverarbeitung hingegen wieder deutsches Recht zur Anwendung. Sofern der Arbeiter mit der Datenverarbeitung beauftragt wird, ist nicht er verantwortliche Stelle im Sinne des BDSG, sondern der jeweilige Auftraggeber. Der Arbeiter ist folglich nicht für die Rechtmäßigkeit der Datenverarbeitung, sondern nach § 11 i. V. m. § 9 (Artikel 17 EG-DatSchRL) lediglich für die Gewährleistung eines ausreichenden Maßes an Datensicherheit verantwortlich⁶⁴.

4.6.4.4 Analyse der Variante des Szenarios

Die Variante zu diesem Szenario unterscheidet sich von der Grundkonstellation lediglich dadurch, dass sich der Sitz von Zettasoft bzw. der Niederlassung, in der die Kundendaten verarbeitet werden, in Deutschland befindet. Der

⁶³Vgl. bereits die diesbezüglichen Ausführungen im Abschnitt „Vorab: Datenschutz als Akzeptanz- und Wettbewerbsfaktor“ (2.1.1.1).

⁶⁴Wird dem AMT-Arbeiter allerdings bekannt, dass die Datenverarbeitung gegen das BDSG verstößt, so hat er eine qualifizierte Remonstrationspflicht gegenüber dem Auftraggeber entsprechend § 11 Abs. 3 S. 2 BDSG.

Sitz von von Kempelen und Amazon Mechanical Turk befindet sich hingegen wiederum in den USA. Diese Variante ist rechtlich wie folgt zu bewerten:

Wie § 3 Abs. 8 S. 3 BDSG zeigt, werden von § 11 BDSG nur Auftragnehmer erfasst, die im Geltungsbereich des Bundesdatenschutzgesetzes bzw. der EG-DatSchRL tätig werden. Stellen in Ländern, die außerhalb von Deutschland und der Europäischen Union (bzw. des EWR) gelegen sind, sind hingegen immer Dritte i. S. d. § 3 Abs. 8 S. 2 BDSG. Folglich stellt auch jede zum Zwecke der Auftragsdatenverarbeitung vorgenommene Weitergabe personenbezogener Daten an solche Stellen stets eine unter dem Verbot mit Erlaubnisvorbehalt stehende Datenübermittlung dar [GS05, § 11 Rn. 16.]. Eine solche Übermittlung bedarf also zum einen einer Rechtsgrundlage, darüber hinaus ist sie aber nach § 4b f. BDSG auch nur unter bestimmten (zusätzlichen) Voraussetzungen zulässig, die ein angemessenes Datenschutzniveau sicherstellen sollen.

Vorliegend steht als Rechtsgrundlage § 28 Abs. 1 S. 1 Nr. 1 BDSG zur Verfügung, da die Weitergabe der personenbezogenen Daten der Zweckbestimmung des Supportvertrages dient. Um den Voraussetzungen der § 4b f. BDSG gerecht zu werden, könnten Zettasoft und die jeweiligen Auftragnehmer insbesondere die von der EG-Kommission auf Grundlage des Artikel 26 Abs. 4 EG-DatSchRL entwickelten Standardvertragsklauseln für die Übermittlung personenbezogener Daten an Auftragsverarbeiter in Drittländern vom 27. Dezember 2001⁶⁵ verwenden. Werden diese der Datenübermittlung (unverändert) zugrunde gelegt, so ist ein angemessenes Datenschutzniveau i. S. d. § 4b f. BDSG gewährleistet. Es bedarf dann auch keiner Genehmigung der Datenübermittlung durch die jeweils zuständige Aufsichtsbehörde, sondern diese ist lediglich zu informieren [DKWW07, § 4c Rn. 18]. Wird ein Unterauftragnehmer eingeschaltet, so sind die aus den Standardvertragsklauseln resultierenden Pflichten des den Unterauftrag erteilenden Auftragnehmers auf den Unterauftragnehmer „weiterzuleiten“. Dies kann entweder dadurch geschehen, dass Zettasoft als Auftraggeber auch mit dem Unterauftragnehmer die Geltung der Standardvertragsklauseln vereinbart oder indem dieser dem Vertrag zwischen Zettasoft und dem den Unterauftrag erteilenden Auftragnehmer beitrifft⁶⁶.

Sofern sich AMT-Arbeiter in Deutschland aufhalten, kann schließlich zwischen ihnen und Zettasoft ohne weiteres eine Auftragsdatenverarbeitung gem. § 11 BDSG (Artikel 17 EG-DatSchRL) vereinbart werden.

⁶⁵Diese Standardvertragsklauseln sind abrufbar unter http://eur-lex.europa.eu/LexUriServ/site/de/oj/2002/l_006/l_00620020110de00520062.pdf.

⁶⁶Hierzu siehe den Tätigkeitsbericht des Berliner Datenschutzbeauftragten für das Jahr 2003, Punkt 4.7.2, abrufbar unter <http://www.datenschutz-berlin.de/jahresbe/index.htm>.

4.6.5 PSB – Entwicklung und Wartung von Produktionsstraßen

4.6.5.1 Allgemeine Bemerkungen

Die Besonderheit dieses Szenarios besteht darin, dass von den beteiligten Stellen keine personenbezogenen Daten verarbeitet werden. Stattdessen fließen zwischen ihnen Daten, deren Geheimhaltung für eines der beteiligten Unternehmen von großer Bedeutung ist. Im ersten Teilszenario geht es um technische Spezifikationen von Zulieferteilen (und damit um Betriebsgeheimnisse⁶⁷), die dem an der Entwicklung einer Produktionsstraße beteiligten Ingenieurbüro durch den Hersteller zur Verfügung gestellt werden, welcher sie wiederum vom Zulieferer selbst erhalten hat. Im zweiten Teilszenario wird hingegen der technische Betrieb von Produktionsstraßen mittels einer Erfassung und Auswertung von Multimediadaten überwacht. Diese werden von einem Datendienstleister erfasst und von einem Datenanalysten ausgewertet. Hier hat der die Produktionsstraße nutzende Warenproduzent ein Interesse an der Geheimhaltung der erfassten Multimediadaten, da diese es Außenstehenden ermöglichen können, Rückschlüsse auf bei dem Betrieb der Produktionsstraße auftretende Probleme zu ziehen. In beiden Teilszenarien hat also jeweils ein Unternehmen ein großes Interesse daran, dass bestimmte Daten vertraulich behandelt und verarbeitet werden. Aus diesem Grunde werden zwischen den Beteiligten auch jeweils vertragliche Geheimhaltungspflichten (sog. non-disclosure agreements) vereinbart⁶⁸. Vergleicht man nun das vorliegende Szenario mit den Szenarien 1-3, so ist festzustellen, dass es in allen vier Szenarien um den Schutz sensibler Daten geht: Dabei handelt es sich zum einen um personenbezogene Daten von Nutzern bzw. Kunden und zum anderen um Daten, die Betriebs- oder Geschäftsgeheimnisse eines Unternehmens beinhalten. Die Konsequenzen, die aus technischer Sicht aus der besonderen Schutzbedürftigkeit der jeweiligen Daten zu ziehen sind, sind dabei die gleichen: Personenbezogene und unternehmensbezogene Daten können nämlich durch die gleichen Schutzmaßnahmen (z. B. Verschlüsselung) vor Kenntnisnahme und Missbrauch durch Unbefugte geschützt werden.

⁶⁷Zu den rechtlichen Rahmenbedingungen des Schutzes von Betriebs- und Geschäftsgeheimnissen vgl. bereits den Abschnitt „Schutz von Betriebs- und Geschäftsgeheimnissen“ (2.1.2).

⁶⁸Auf diesbezügliche rechtliche Fragestellungen soll an dieser Stelle aber nicht eingegangen werden, weil hierdurch der Rahmen dieser Untersuchung gesprengt werden würde.

4.6.5.2 Datenschutz durch Prozessmanagement

Bereits im Abschnitt „Vorab: Datenschutz als Akzeptanz- und Wettbewerbsfaktor“ (2.1.1.1) ist erwähnt worden, dass eine der vier Säulen eines modernen Datenschutzes in der Gewährleistung eines Prozessmanagements in den Daten verarbeitenden Stellen besteht [Biz07]. Die Erfüllung der Anforderungen des Datenschutzes stellt insoweit eine Aufgabe von Compliance und Riskmanagement dar. Dabei bedeutet Riskmanagement für eine von der modernen Informationstechnik abhängige Stelle aber nicht zuletzt auch, dass sie ein funktionierendes Sicherheits- und Datenschutzmanagement zu installieren hat. Dieses aber dient dem Schutz der Unternehmenswerte, zu denen sowohl Betriebs- und Geschäftsgeheimnisse als auch die personenbezogenen Daten von Mitarbeitern und Kunden zählen. Folglich dient derselbe Prozess, nämlich die Installierung eines Sicherheits- und Datenschutzmanagements, sowohl dem Schutz der Betriebs- und Geschäftsgeheimnisse als auch dem der personenbezogenen Daten.

4.6.5.3 Zusicherung, Unterrichtung, Protokollierung und Auskunft

In diesem Szenario wird von den Unternehmen, die mit vertraulichen Daten anderer Unternehmen arbeiten, zugesichert, dass diese Daten nicht an Dritte weitergegeben werden. Da es nicht um die Verarbeitung personenbezogener Daten geht, spielen die datenschutzrechtlichen Unterrichtungspflichten und Auskunftsansprüche hier keine Rolle. Eine (revisionssichere) Protokollierung kann dokumentieren, dass vertrauliche Daten tatsächlich nicht an weitere Stellen weitergegeben worden sind.

4.6.5.4 Fazit

Sowohl bei personenbezogenen Daten als auch bei Informationen, die Betriebs- und Geschäftsgeheimnisse beinhalten, handelt es sich um besonders schutzbedürftige Daten, die vor Kenntnisnahme und Missbrauch durch Dritte zu schützen sind. Ein Unternehmen kann dies hinsichtlich beider Arten von Daten durch die Installierung eines Sicherheits- und Datenschutzmanagements und konkret durch den Einsatz technisch identischer Schutzmaßnahmen sicherstellen.

Kapitel 5

Anforderungen und Lösungsvorschläge

In diesem Kapitel werden Anforderungen spezifiziert, denen eine aus Datenschutzsicht beherrschbare SOA genügen sollte. Grundlage hierfür sind insbesondere die in Kapitel 3 aufgezeigten Probleme aktueller Implementierungen der Beherrschbarkeitsfaktoren und die Ergebnisse der Szenarienanalyse (Kapitel 4). Die Anforderungen sind nach den Beherrschbarkeitsfaktoren gegliedert. Darüber hinaus werden für die einzelnen Anforderungen erste Lösungsansätze vorgestellt. Diese geben einen Anhaltspunkt, welche aktuell vorhandenen oder noch zukünftig zu entwickelnden Technologien und Methoden einzusetzen sind, um den vorliegenden Anforderungen zu entsprechen.

5.1 Methodik der Gestaltungsvorschläge

Zu den folgenden Gestaltungsvorschlägen dieses Kapitels gibt es drei Einflussquellen. Die erste Quelle bilden die rechtlichen Kriterien aus Kapitel 2. Diese sind eingegangen in die strukturierte Beschreibung der Anwendungsszenarien in Kapitel 4. Und zwar sind die verantwortlichen Stellen die beteiligten Services, während das jeweilige Datum, der zugehörige Verwendungszweck und der Personenbezug dann in den Tabellen ausgewiesen sind, die den einzelnen Verarbeitungsschritten zugeordnet sind. Die zweite Quelle bilden die technischen Kriterien, die in Kapitel 3 entwickelt wurden. Sie sind in den Analysefragen zu den Zusicherungen und zur Unterrichtung (Abschnitt 3.3.3), sowie zu der Protokollierung und Auskunft (3.4.3) zusammengefasst. Die dritte Quelle bilden die Analysen der Szenarien, in welche die rechtlichen und technischen Kriterien als Analyseelemente eingegangen sind. In den folgenden Anforderungen und Gestaltungsvorschlägen wird auf die Analysefragen

Bezug genommen. Um die Anforderungen in ein schlüssiges Gesamtbild zusammenzufügen, werden sie am Beispiel des Hanival-Szenarios (Kapitel 4.2) erläutert, welches sich hierfür gut eignet, da es alle relevanten Problembereiche abdeckt.

Die dreiunddreißig Gestaltungsvorschläge zu Zusicherung und Unterrichtung (Abschnitt 5.2), sowie zu Protokollen und Auskunft (Abschnitt 5.3) bilden eine detailliertere Liste von Anforderungen und Gestaltungsvorschlägen, die sich in übergeordnete Aufgabenbereiche ordnen lassen. Diese fünf Aufgabenbereiche werden im Abschnitt 5.4 unten abschließend zusammengefasst.

5.2 Zusicherungen und Unterrichtung

1. **Zusicherungen und Präferenzen sollen in einer eindeutigen Formalisierung vorliegen, wobei der Inhalt der Zusicherungen und Präferenzen maschineninterpretierbar sein soll.**

(bezieht sich auf Analysefragen 7 und 13)

Da Zusicherungen und Präferenzen auch automatisch ausgewertet bzw. miteinander verglichen werden sollen, ist anzustreben, dass sie in maschineninterpretierbarer Form ausgedrückt werden. Um einerseits die Fehlinterpretation einer Zusicherung oder Präferenz auszuschließen und um andererseits möglichen Rechtsstreitigkeiten um unterschiedliche Auslegungen vorzubeugen, wird die Eindeutigkeit der Formalisierung gefordert. Eine Abweichung von diesen Forderungen, zum Beispiel in Fällen, in denen sich natürlichsprachliche Zusicherungen nicht maschineninterpretierbar abbilden lassen, sollte nur in begründeten Ausnahmen erfolgen.

Im Hanival-Szenario sind die Zusicherungen natürlichsprachlich formuliert und nur in soweit eindeutig, als dass sie als rechtliche Texte sorgsam formuliert wurden.

Lösungsansatz: Maschineninterpretierbarkeit wird durch Festlegung auf eine formale Sprache erreicht, Eindeutigkeit durch Einigung auf eine gemeinsame Ontologie.

2. **Es muss eindeutig erkennbar sein, auf welche Daten sich eine Zusicherung bezieht.**

(bezieht sich auf Analysefrage 2)

Dies ist wichtig, da verschiedene Dienste eines Anbieters unterschiedliche Zusicherungen geben können bzw. auch in einem Dienst durchaus

unterschiedliche Zusicherungen für verschiedene Teildaten eines Datensatzes gelten können.

Im Hanival-Szenario übergibt beispielsweise der Kunde der VO verschiedene Daten, die nachfolgend auch an verschiedene andere Akteure weitergereicht werden. Der Wiederverkäufer ist also dafür verantwortlich, dem Kunden für seine Kontaktdaten andere Zusicherungen zu machen als für seine Kontodaten.

Lösungsansatz: Zusicherungen werden in die Schnittstellenbeschreibung eines Dienstes integriert.

3. Es muss explizit erfasst sein, wer für die Zusicherung einsteht.

(bezieht sich auf Analysefrage 3)

Es muss möglich sein, zu jeder Zusicherung direkt zu erkennen, wer für ihre Einhaltung verantwortlich ist (siehe auch Analysefrage 3).

Da im Hanival-Szenario der Zusichernde auch immer der Verantwortliche ist, ist für den Kunden unmittelbar erkennbar, wer für die jeweiligen Zusicherungen einsteht.

Lösungsansatz: Der Verantwortliche wird im Zusicherungstext genannt.

4. Es muss erkennbar sein, wer die Zusicherung mitteilt.

(bezieht sich auf Analysefrage 5)

Im einfachsten Fall ist der Dienstanbieter, der für die Zusicherung einsteht, auch der, der sie dem Nutzer mitteilt. Findet diese Mitteilung jedoch nur mittelbar über einen weiteren Anbieter statt, so muss dieser Unterschied für den Nutzer erkennbar sein, und er muss (zusätzlich zu Anforderung 3) erkennen können, wer ihm die Zusicherung mitgeteilt hat.

Lösungsansatz: Jede Instanz, die die Zusicherung weiterleitet, wird im Zusicherungstext erkennbar gemacht.

5. Ein einfacher Zugang zu den Zusicherungen soll gewährt werden.

(bezieht sich auf Analysefragen 5 und 7)

Potentielle Nutzer eines Dienstes sollen problemlos vor der Nutzung die Zusicherungen des Anbieters einsehen können. Sinnvoll ist eine standardisierte Zugriffsmethode, die ein Minimum an Kommunikation voraussetzt (da so auch nur ein Minimum an Daten vor Bekanntgabe der Zusicherungen preisgegeben wird).

Der Wiederverkäufer ruft die Dienstleistungen von Hanival über einen Web Service ab; die dazugehörigen Zusicherungen kann der Wiederverkäufer nur über die Webseite von Hanival abrufen.

Lösungsansatz: Zusicherungen werden in die Schnittstellenbeschreibung eines Dienstes integriert. Der automatische Zugriff auf die Zusicherungen und deren Auswertung erfolgt mittels Anwendungssoftware.

6. Die Zusicherungen sollen nur vertragliche oder sonstige rechtlich relevante Aspekte der Datennutzung beschreiben.

(bezieht sich auf Analysefrage 6)

Wie bereits zu Analysefrage 6 erläutert, können Zusicherungen nahezu beliebig detailliert sein. Um sie nicht unnötig kompliziert zu machen, sollten sie jedoch nicht detaillierter sein als rechtlich bzw. vertraglich notwendig.

Im Hanival-Szenario wurden die Zusicherungen von Juristen unter Berücksichtigung der relevanten Aspekte formuliert.

Lösungsansatz: Zusicherungen können mit Hilfe eines Expertensystems erstellt werden, das über Mechanismen zur Generierung von gesetzeskonformen Formulierungen verfügt.

7. Die Zusicherungen sollen für den Nutzer verständlich dargestellt werden.

(bezieht sich auf Analysefrage 7)

Selbst Zusicherungen, die Anforderung 6 genügen, können sehr komplex werden. Diese kann ein Nutzer ohne umfangreiche rechtliche Vorkenntnisse nicht verstehen und beurteilen, daher ist eine allgemein verständliche Form der Darstellung von Zusicherungen nötig.

Die Zusicherungen des Wiederverkäufers im Hanival-Szenario liegen als natürlichsprachlicher, umfangreicher Text vor. Dies kann ihre Verständlichkeit für den Nutzer verringern oder ihn sogar abschrecken, sie überhaupt zu lesen.

Lösungsansatz: Die Zusicherungen werden in einem Formalismus ausgedrückt, der es ermöglicht, sie in verschiedenen Abstraktionsgraden darzustellen.

8. Eine mitgeteilte Zusicherung muss für den Urheber unabstreitbar sein.

(bezieht sich auf Analysefrage 8)

Wie bereits zu Analysefrage 8 erläutert, müssen Zusicherungen verbindlich sein, d.h. der Urheber darf nicht abstreiten können, sie in genau dieser Form gemacht zu haben. Mit der elektronischen Signatur existiert hier bereits ein Verfahren, durch das diese Anforderung erfüllt werden kann.

Der Wiederverkäufer teilt die Zusicherungen natürlichsprachlich auf seiner Webseite mit, die nicht elektronisch signiert ist. Da durch den Zugriff auf die Webseite der Urheber für den Kunden direkt ersichtlich ist, wird auf Signaturen verzichtet.

Lösungsansatz: Die Zusicherung wird vom Urheber auf Basis kryptographischer Methoden digital signiert.

9. **Es soll möglich sein, die virtuelle Organisation unter Beibehaltung der mitgeteilten Zusicherungen anzupassen.**

(bezieht sich auf Analysefrage 9)

In einer VO kann es vorkommen, dass ein Unternehmen ausscheidet und durch ein neu hinzugekommenes ersetzt wird. Diese dynamischen Änderungen sollen möglich sein, ohne dass die Zusicherungen, die dem Kunden gemacht wurden, neu ausgehandelt werden müssen oder das Unternehmen mit Kontakt zum Kunden gar vom Vertrag zurücktreten muss. Diese Anforderung gilt jedoch nicht nur für die VO: auch für die Formalisierung der Zusicherungen wird gefordert, dass sie z.B. den Austausch von Unternehmen und deren Diensten zur Laufzeit nicht unnötig einschränkt.

Falls der IZP im Hanival-Szenario nicht mehr verfügbar ist, sucht ein Mitarbeiter unter Berücksichtigung der bereits an den Wiederverkäufer gemachten Zusicherungen nach einem alternativen Serviceanbieter.

Lösungsansatz: Mit Hilfe semantischer Beschreibungen wird, soweit möglich, überprüft, ob geplante Änderungen an der VO unter Berücksichtigung der mitgeteilten Zusicherungen möglich sind. Zusicherungen, die mit dem in Anforderung 6 genannten Expertensystem erstellt wurden, erleichtern diese Änderungen der VO, da sie die Änderungsmöglichkeiten nicht unnötig einschränken.

10. **Es muss möglich sein, die mitgeteilten Zusicherungen an die virtuelle Organisation anzupassen.**

(bezieht sich auf Analysefrage 10)

Diese Anforderung ergänzt die vorangegangene: falls es nicht möglich ist, (möglicherweise unvermeidbare) Änderungen an der VO bei gleich

bleibenden Zusicherungen vorzunehmen, so muss ein Mechanismus existieren, um bereits mitgeteilte Zusicherungen in gegenseitigem Einverständnis an die neuen Gegebenheiten anzupassen. Alternativ muss der Kunde die Möglichkeit haben, vom Vertrag zurückzutreten.

Falls sich die VO im Hanival-Szenario so ändert, dass die Zusicherungen angepasst werden müssen, werden die neuen Zusicherungen dem Kunden durch den Wiederverkäufer mitgeteilt. Ist der Kunde mit diesen neuen Zusicherungen nicht einverstanden, so hat er die Möglichkeit, das Vertragsverhältnis zu beenden.

Lösungsansatz: Das Aushandeln neuer rechtskonformer Zusicherungen wird technisch „erzwingen“, bevor die Daten so verarbeitet werden, dass alte Zusicherungen verletzt würden. Die semantischen Beschreibungen von Zusicherungen ermöglichen hierbei, die notwendigen Änderungen zu identifizieren und bieten somit eine Grundlage zur Neuverhandlung.

11. Es muss möglich sein, anhand von Protokollen die Einhaltung der Zusicherungen im Nachhinein festzustellen.

(bezieht sich auf Analysefrage 11)

Durch Protokolle lässt sich die Verarbeitung der Daten durch den Service nachvollziehen. Somit können durch den Abgleich mit den Zusicherungen Vorgänge identifiziert werden, die nicht zusicherungskonform sind.

Im Hanival-Szenario werden die Protokolle nicht weitergegeben, daher ist eine Überprüfung der Einhaltung nur den Serviceanbietern möglich. Dies ist für sie allerdings mit hohem Aufwand verbunden, da der Abgleich nur manuell vorgenommen werden kann.

Lösungsansatz: Die Verwendung eines semantischen Formalismus als Grundlage für Beschreibung von Zusicherungen und zur Protokollierung ermöglicht die teilautomatisierte Überprüfung der Einhaltung.

12. Es soll möglich sein, die Einhaltung der mitgeteilten Zusicherung sicherzustellen.

(bezieht sich auf Analysefrage 12)

Hierfür ist ein Mechanismus nötig, der es dem Serviceanbieter technisch unmöglich macht, seine Zusicherungen zu verletzen – ein Teil der Infrastruktur des Anbieters muss seiner direkten Einflussnahme entzogen werden.

Da keiner der Akteure des Hanival-Szenarios auf diese Weise in seinen Handlungsmöglichkeiten eingeschränkt wird, kann die Einhaltung der Zusicherungen dort nicht technisch sichergestellt werden.

Lösungsansatz: Die Verwendung von DRM kann die Kontrolle der Datennutzung gewährleisten („DRM4privacy“).

13. **Es soll eine Möglichkeit existieren, Vertrauen zwischen Nutzer und Anbieter herzustellen.**

(bezieht sich auf Analysefragen 3, 8, 11 und 12)

Es wird eine Infrastruktur benötigt, die es einem Nutzer ermöglicht, begründetes Vertrauen in einen ihm bislang unbekanntem Serviceanbieter zu fassen. Durch Vertrauen kann der Teil der Zusicherung substituiert werden, der sich aus Gründen der Praktikabilität nicht ausdrücken lässt ((bewusste) Verletzung oder Fehlinterpretation der Zusicherung).

Im Hanival-Szenario kann der Wiederverkäufer durch eine unabhängige Zertifizierungsstelle seine Datenschutzpraxis prüfen lassen und, falls die Prüfung erfolgreich verläuft, dem Kunden gegenüber damit werben.

Lösungsansatz: Der Serviceanbieter unterzieht sich der Zertifizierung durch einen unabhängigen Dritten.

14. **Dem Nutzer soll die Möglichkeit gegeben werden, seine Präferenzen in einfacher Weise auszudrücken.**

(bezieht sich auf Analysefragen 13 und 14)

Da es sich bei den Nutzern oft um rechtliche und technische Laien handelt, sollen ihnen einfach zu bedienende Werkzeuge zur Verfügung gestellt werden, um Präferenzen in die in Anforderung 1 geforderte formale Form zu bringen. Diese Präferenzen können Grundlage einer teilautomatisierten Aushandlung neuer Zusicherungen sein.

Da die Nutzerpräferenzen und die Zusicherungen der Unternehmen im Hanival-Szenario nicht automatisiert ausgehandelt oder auch nur verglichen werden, besteht kein Grund für den Nutzer, seine Präferenzen explizit auszudrücken. Stattdessen gehen sie implizit in die von ihm zu treffende Entscheidung ein, ob er die mitgeteilten Zusicherungen akzeptiert.

Lösungsansatz: Die Bereitstellung einer wohldefinierten Ontologien, die sich auf die notwendigen Konzepte zur Beschreibung der Präferenzen des Nutzers beschränkt, dient als Basis eines Expertensystems, das den Nutzer bei der Erstellung seiner Präferenzen unterstützt.

15. **Ein im Workflow nachgelagerter Serviceanbieter muss die Zusicherungen der im Workflow vorgelagerten Serviceanbieter einhalten.**

(bezieht sich auf Analysefragen 1, 3 und 4)

Da der Serviceanbieter, der in direktem Kundenkontakt steht, verbindliche Zusicherungen für den gesamten Workflow macht, müssen nachgelagerte Anbieter sich an diese Zusicherungen halten.

Im Hanival-Szenario werden in den vertraglichen Vereinbarungen zwischen den verschiedenen Serviceanbietern die Zusicherungen geregelt, die der Wiederverkäufer dem Kunden geben kann.

Lösungsansatz: Damit die gemeinsamen Zusicherungen nicht im Vorhinein ausgehandelt werden müssen, wird ein Mechanismus eingesetzt, der aus Präferenzen und Zusicherungen neue Präferenzen generiert. So werden beim ersten Service eines Workflows Kundenpräferenzen und die Zusicherungen des Services abgeglichen, das Resultat geht wiederum als Menge von Präferenzen in den Abgleich mit den Zusicherungen des zweiten Service ein. Sind Präferenzen und Zusicherungen aufbauend auf demselben semantischen Formalismus spezifiziert, können die neuen Präferenzen mit Hilfe eines Reasoners teilautomatisiert abgeleitet werden.

16. **Kunde und Serviceanbieter müssen die Möglichkeit erhalten, einen Abgleich von Präferenzen und Zusicherungen durchzuführen.**

(bezieht sich auf Analysefragen 15 und 16)

Prinzipiell kann ein Abgleich zwischen sich nicht entsprechenden Präferenzen und Zusicherungen sowohl auf Seite des Anbieters als auch auf Kundenseite erfolgen. Um für verschiedene Marktsituationen beide Alternativen zuzulassen, muss sowohl Kunden als auch Anbietern die Möglichkeit des Abgleichs gegeben werden.

Wie bereits in Anforderung 14 erläutert, gibt es im Hanival-Szenario weder explizite Nutzerpräferenzen noch automatisierte Abgleichprozesse. Die Überprüfung der Zusicherungen des Anbieters findet stets auf Kundenseite statt.

Lösungsansatz: Anbietern und Kunden wird eine Software zur Durchführung des teilautomatisierten Abgleichs und zur Übermittlung des Ergebnisses zur Verfügung gestellt.

17. **Ein nachvollziehbarer Abgleich von Präferenzen und Zusicherungen muss möglich sein.**

(bezieht sich auf Analysefragen 15 und 16)

Der Abgleich muss so geschehen, dass er für den Servicenutzer und -anbieter nachvollziehbar und das Ergebnis korrekt von der abgleichenden Instanz begründbar ist. Im Fall, dass die Präferenzen nicht den vorgegebenen Zusicherungen entsprechen, sind Abgleichsstrategien anzuwenden, welche die Zusicherungen entsprechend den Präferenzen modifizieren, so dass die entstehende Zusicherung sowohl für den Servicenutzer als auch für den Serviceanbieter akzeptabel ist.

Wie in Anforderung 16 beschrieben, muss im Hanival-Szenario stets der Kunde überprüfen, ob er die Zusicherungen des Anbieters akzeptiert. Dadurch wird eine maximale Transparenz gewährleistet.

Lösungsansatz: Der Abgleichprozess wird für den Nutzer dadurch nachvollziehbar, dass ihm mitgeteilt wird, welche Zusicherungen und welche Präferenzen zum Ergebnis des Abgleichs geführt haben.

18. **Mehrstufige Abgleichungsprozesse in einer virtuellen Organisation müssen unterstützt werden.**

(bezieht sich auf Analysefragen 15 und 16)

Ein mehrstufiger Abgleichungsprozess entsteht immer dann zwangsläufig, wenn ein Service A, der vom Endkunden aufgerufen wird, einen Service B einer anderen Organisation aufruft. In diesem Fall muss der Service A die Zusicherungen aller nachgelagerten Services übernehmen. Falls ein Service in seiner Abarbeitung Verzweigungen besitzt, für die erst zur Laufzeit feststeht, welche nachgelagerten Services aufgerufen werden, so muss diese Tatsache ebenfalls in die mehrstufige Abgleichung eingehen. Im Ergebnis muss eine zusicherungskonforme Abarbeitung des Services möglich sein.

Da im Hanival-Szenario die Zusicherungen vertraglich ausgehandelt werden, treten keine mehrstufige Abgleichungsprozesse auf.

Lösungsansatz: Mit Hilfe formaler Methoden, wie sie in der Softwareverifikation verwendet werden, wird der Abgleich von Zusicherungen ermöglicht.

19. **Eine nachträgliche Unterrichtung (Benachrichtigung) muss durch geeignete Mechanismen ermöglicht werden.**

(bezieht sich auf Analysefragen 17 und 18)

Ändern sich (wie in Anforderung 10 beschrieben) die Zusicherungen, so ist eine Benachrichtigung des Kunden erforderlich. Hierfür werden Mechanismen benötigt, die Unterrichtung bzw. Benachrichtigung in mehrstufigen Serviceworkflows ermöglichen, in denen der Endkunde nicht allen nachfolgenden Serviceanbietern bekannt ist. Ebenso muss die Anerkennung der in der Benachrichtigung mitgeteilten Zusicherungen durch den Endkunden möglich sein.

Ändert Hanival einen seiner Vertragspartner bzw. ändert ein solcher seine Zusicherungen, so muss eine Benachrichtigung „manuell“ von Hanival an den Wiederverkäufer und von diesem an seine Kunden weitergegeben werden.

Lösungsansatz: Es werden standardisierte Kommunikationsschnittstellen bereitgestellt, die eine Weitergabe von Unterrichtungen bzw. Benachrichtigung entgegen der Workflowrichtung ermöglichen.

5.3 Protokolle und Auskunft

20. **Es muss eindeutig erkennbar sein, auf welche Daten sich ein Protokolleintrag bezieht.**

(bezieht sich auf Analysefragen 19, 20 und 22)

Die Protokolle dienen als Informationsquelle für das Erteilen der Auskunft. Hierfür enthalten die Protokolle Informationen über die Aktionen, die auf bestimmten Daten ausgeführt wurden. Da bei einem Dienstaufwurf unterschiedliche Daten, auf denen unterschiedliche Aktionen ausgeführt werden, übergeben werden können, muss klar erkenntlich sein, auf welche Daten sich ein Protokolleintrag bezieht.

Damit der Wiederverkäufer im Hanival-Szenario eindeutig erkennen kann, auf welche Daten sich ein Protokolleintrag bezieht, betreibt er umfangreiche Protokollierung aller Aktionen, die auf den Daten ausgeführt werden. Hierbei entsteht ein Datenvolumen, durch das die Protokollauswertung im Einzelfall sehr aufwendig wird.

Lösungsansatz: Das Protokoll wird als Metadatum an die Daten geheftet.

21. **Es muss erkennbar sein, dass protokolliert wurde.**

(bezieht sich auf Analysefrage 19)

Da beim Protokollieren von Aktionen auf personenbezogenen Daten diese Daten auch selber Teil des Protokolls werden können, muss im

Rahmen der Auskunftserteilung angegeben werden, dass Informationen zur Verarbeitung personenbezogener Daten protokolliert wurden.

Beim Wiederverkäufer im Hanival-Szenario fallen bei der Verarbeitung der Kundendaten verschiedene Protokolle, z.B. die eines Workflow-Management-Systems, an. Diese Tatsache muss er dem Kunden mitteilen, falls dieser Auskunft verlangt.

Lösungsansatz: Das Protokoll wird als Metadatum an die Daten geheftet.

22. Es muss eindeutig erkennbar sein, welcher Dienstanbieter der virtuellen Organisation einen Protokolleintrag erzeugt hat.

(bezieht sich auf Analysefrage 19 und 20)

Für die Verbindlichkeit eines Protokolls steht derjenige Dienstanbieter einer virtuellen Organisation ein, der das jeweilige Protokoll erzeugt hat. Wie bereits zu Analysefrage 19 erläutert, können jedoch mehrere Dienste im selben Protokoll protokollieren. Dies können auch Dienste unterschiedlicher Dienstanbieter sein. In einem solchen Fall muss erkenntlich sein, welcher Dienst und damit welcher Dienstanbieter welchen Protokolleintrag erzeugt hat.

Da im Hanival-Szenario keine gemeinsame Protokollierung erfolgt, ist das Protokoll stets bei dem Dienstanbieter gespeichert, der es auch erzeugt hat.

Lösungsansatz: Der für die Datennutzung Verantwortliche wird im jeweiligen Protokolleintrag benannt.

23. Protokolle sollen alle vertraglichen und sonstige rechtlich relevante Aspekte der Datennutzung beschreiben, darüber hinaus jedoch nur technische Aspekte, sofern sie zweckgebunden sind.

(bezieht sich auf Analysefragen 20 und 21)

Ein Dienst kann verschiedene Aktionen zu unterschiedlichen Zwecken auf den Daten ausführen. Dies kann und muss zum Teil in Protokollen erfasst werden. Hinzukommt, dass in den Protokollen die agierenden Dienste (siehe Anforderung 22) sowie die bearbeiteten Daten (siehe Anforderung 20) erfasst werden müssen. Protokolle können daher beliebig detailliert sein und somit ein immenses Datenaufkommen erzeugen. Allerdings haben nicht alle Aktionen eine ausreichende Relevanz, um deren Protokollierung zu rechtfertigen. Daher soll die Protokollierung

auf die vertraglichen und sonstige rechtlich relevante Aspekte sowie technisch notwendige Einträge reduziert werden.

Da der Wiederverkäufer im Hanival-Szenario durch umfangreiche Protokollierung zu vermeiden versucht, dass relevante Informationen verloren gehen, protokolliert er mehr als vertraglich bzw. rechtlich gefordert.

Lösungsansatz: Ein Filter für Protokolleinträge wird mit Hilfe eines Expertensystems oder durch Personen mit juristischem oder technischem Fachwissen erstellt.

24. **Protokolle müssen in einer eindeutigen Formalisierung vorliegen, wobei der Inhalt der Protokolle maschineninterpretierbar sein muss.**

(bezieht sich auf Analysefrage 21)

Erfolgt die Protokollierung in ein gemeinsam genutztes Protokoll, dann muss die virtuelle Organisation sich auf ein Protokollformat einigen. Aber auch in dem Falle, dass jeder Dienstanbieter der virtuellen Organisation seine eigenen Protokolle erstellt, ermöglicht die Verwendung eines standardisierten Formats die Teilautomatisierung der Auskunftserteilung. Um die Erzeugung der notwendigen Eindeutigkeit der Auskunft zu erleichtern, wie in Anforderung 26 gefordert, sollte auch die Formalisierung eindeutig sein.

Da der Wiederverkäufer im Hanival-Szenario sich auf einfache Protokollierungsmechanismen verlässt, liegen seine Protokolle nicht in der geforderten, maschineninterpretierbaren Formalisierung vor.

Lösungsansatz: Maschineninterpretierbarkeit wird durch Festlegung auf eine formale Sprache erreicht, Eindeutigkeit durch Einigung auf eine gemeinsame Ontologie.

25. **Ein Protokoll muss vom Urheber unabstreitbar sein.**

(bezieht sich auf Analysefrage 23)

Wie bereits in Anforderung 8 für Zusicherungen gefordert müssen auch Protokolle verbindlich sein. Der Urheber darf daher nicht abstreiten können, das Protokoll in der vorliegenden Form erstellt zu haben. Mit Hilfe der elektronischen Signatur kann diese Anforderung erfüllt werden.

Da die Protokolle im Hanival-Szenario nicht kommuniziert werden, wird ihre Urheberschaft nicht angezweifelt.

Lösungsansatz: Das Protokoll wird vom Urheber auf Basis kryptographischer Methoden digital signiert.

26. Die Auskunft soll eindeutig formalisiert mitgeteilt werden, wobei ihr Inhalt maschineninterpretierbar sein soll.

(bezieht sich auf Analysefrage 24)

Wenn die Auskunft vom Nutzer einer Dienstleistung auch teilautomatisiert ausgewertet werden können soll, ist eine maschineninterpretierbare Formalisierung unabdingbar. Um einerseits die Fehlinterpretation der Auskunft auszuschließen und um andererseits möglichen Rechtsstreitigkeiten um unterschiedlich ausgelegte Auskünfte vorzubeugen, wird die Eindeutigkeit der Formalisierung gefordert.

Im Hanival-Szenario wird die Auskunft des Wiederverkäufers über die personenbezogenen Daten des Kunden diesem in Briefform mitgeteilt.

Lösungsansatz: Die Auskunft wird auf Basis von Protokollen erstellt, die Anforderung 24 genügen.

27. Es soll erkennbar sein, wer Auskunft erteilt.

(bezieht sich auf Analysefrage 25)

Im einfachsten Fall ist der Dienstanbieter, der den Auftrag des Nutzers entgegennimmt, auch der, der dem Nutzer Auskunft erteilen muss. Findet die Auskunft jedoch nur mittelbar über weitere Dienstanbieter statt, so muss dieser Unterschied für den Nutzer erkennbar sein, und er muss zusätzlich erkennen können, wer für die Auskunft verantwortlich ist (siehe Anforderung 22).

Im Hanival-Szenario wird die Auskunft stets von dem Unternehmen erteilt, an das der Kunde seine Anfrage gestellt hat; eine besondere Kennzeichnung ist hierbei nicht nötig.

Lösungsansatz: Jede Instanz, die die Auskunft weiterleitet, wird im Auskunftstext erkennbar gemacht.

28. Eine einfache Methodik zum Ersuchen und zur Erteilung der Auskunft soll gewährt werden.

(bezieht sich auf Analysefragen 22, 24 und 25)

Nutzer eines Dienstes sollen problemlos später Auskunft vom Dienstanbieter ersuchen und auch erhalten können. Hierfür soll eine standardisierte Methodik genutzt werden, so dass der Aufwand in Verbindung mit einer standardisierten Formalisierung der Auskunft (siehe auch Anforderung 26) für den Nutzer gering gehalten und eine Teilautomatisierung des Vorgangs ermöglicht wird.

Im Hanival-Szenario ist es für den Kunden aufwändig, Auskunft vom Wiederverkäufer einzuholen, da er seine Anfrage schriftlich formulieren und an den Wiederverkäufer senden muss. Diesem entsteht ebenfalls ein gewisser Aufwand, da er die Anfrage des Kunden nicht automatisiert behandeln kann.

Lösungsansatz: Von jedem Dienstanbieter wird eine auf einem gemeinsamen Standard basierende Schnittstelle zum Ersuchen und zur Erteilung von Auskunft bereitgestellt. In der Dienstbeschreibung wird auf diese Schnittstelle verwiesen.

29. **Eine erteilte Auskunft muss von den Auskunftgebenden unabstreitbar sein.**

(bezieht sich auf Analysefrage 26)

Wie die Verbindlichkeit der Protokolle (siehe Anforderung 25) muss auch die Auskunft verbindlich sein. Es darf daher nicht vom Urheber der Auskunft abstreitbar sein, dass er die Auskunft in der vorliegenden Form erteilt hat. Auch hier stellt die elektronische Signatur eine Methode dar, mit deren Hilfe diese Anforderung erfüllt werden kann.

Die Auskunft, die die Unternehmen im Hanival-Szenario erteilen, kann nur dann als unabstreitbar angesehen werden, wenn sie dem Kunden in Briefform und unterschrieben mitgeteilt wird. Liegt die Auskunft hingegen in Form einer E-Mail vor, so könnte sie im Nachhinein vom Unternehmen abgestritten werden.

Lösungsansatz: Die Auskunft wird vom Verantwortlichen auf Basis kryptographischer Methoden digital signiert.

30. **Die zukünftige Auskunftsfähigkeit muss sichergestellt sein.**

(bezieht sich auf Analysefragen 22 und 27)

Wird die Auskunftsfähigkeit durch Protokolle hergestellt, so besteht je nachdem, wo protokolliert wird (siehe auch Analysefrage 19), die Möglichkeit, dass es beim Ausscheiden eines Teilnehmers aus der VO oder beim Auflösen der VO für den Kunden schwer wird, alle Unternehmen zu identifizieren, die an der Bearbeitung seines Auftrages beteiligt waren; dementsprechend kann er auch seinen Auskunftsanspruch nicht mehr vollständig geltend machen. Daher muss ein Mechanismus existieren, der ein Auskunftersuchen an die VO (als Abstraktion der einzelnen Auskunftersuchen) auch auf längere Dauer ermöglicht (mindestens so lange, wie es rechtlich notwendig ist).

Im Hanival-Szenario muss der Kunde seine Auskunftsbegehren direkt an die einzelnen Unternehmen richten, da jedes Unternehmen seine eigenen Protokolle führt; die Möglichkeit des Kunden, eine lückenlose Auskunft einzuholen, wird im Falle des Ausscheidens eines Unternehmens aus der VO noch zusätzlich dadurch erschwert, dass er dieses Unternehmen evtl. nicht mehr auffinden kann.

Lösungsansatz: Die Protokolleinträge, die die Weitergabe personenbezogener Daten behandeln, werden an die jeweils verarbeiteten Daten als Metadaten angeheftet; beim Ende der Serviceausführung gibt der Service diese Daten an die aufrufende Instanz zurück. Nach der Ausführung eines Workflows sammeln sich so alle Protokolleinträge bei der Instanz, die den Workflow angestoßen hat, oder beim Kunden selbst. Erlaubt der Kunde dieser Instanz die Speicherung des Protokolls, so kann er später per Auskunftersuchen dort anfragen, welche Unternehmen an der Verarbeitung seiner Daten beteiligt waren und an diese weitere Auskunftersuchen richten. Anderenfalls muss er das Protokoll selber speichern, um später die beteiligten Unternehmen rekonstruieren zu können.

31. **Berichtigung und Löschung von Nutzerdaten müssen möglich sein.**

(bezieht sich auf Analysefrage 28)

Die Datenschutzgesetze räumen jedem Betroffenen das Recht ein, die Berichtigung oder Löschung seiner Daten bei den Daten verarbeitenden Stellen zu verlangen. Damit der Dienstanbieter dieser Verpflichtung nachkommen kann, muss es ihm möglich sein, gezielt sowohl die Nutzdaten als auch Protokolleinträge und Backups über einzelne Personen zu manipulieren.

Den Unternehmen des Hanival-Szenarios ist die Berichtigung bzw. Löschung der Nutzdaten bedingt möglich. In Fällen, in denen der Aufwand zu groß wird (z.B. bei Backups auf CD-ROM), tritt an ihre Stelle die Sperrung.

Lösungsansatz: Nutzdaten und Protokolle werden in einer Datenbank oder einem Datenformat gespeichert, das feingranulare Manipulationen erlaubt.

32. **Die Sperrung von Nutzerdaten muss möglich sein.**

(bezieht sich auf Analysefrage 28)

Für Daten, die nicht gelöscht werden können oder dürfen muss ein Mechanismus existieren, der ihre weitere Nutzung bis auf das jeweils notwendige Minimum einschränkt. Wie schon in der vorigen Anforderung muss auch die partielle Sperrung von Teildaten eines größeren Datensatzes möglich sein.

Für die Unternehmen im Hanival-Szenario ist die Sperrung von Nutzerdaten zwar möglich, wird jedoch nur organisatorisch durchgesetzt, d.h. ihre Nutzung wird nicht technisch ausgeschlossen.

Lösungsansatz: Für die Umsetzung der Sperrung werden die Daten verschlüsselt und dort gespeichert, wo sie zuvor unverschlüsselt lagen. Der Schlüssel darf nachfolgend nur zum Durchsetzen rechtlicher Verpflichtungen wie Auskunft oder Audits eingesetzt werden.

33. Dem Servicenutzer sollen Berichtigung, Löschung und Sperrung seiner Daten leicht gemacht werden.

(bezieht sich auf Analysefrage 28)

Da Berichtigung, Löschung und Sperrung Vorgänge sind, die vom Nutzer selbst initiiert werden, reicht die technische Machbarkeit alleine als Anforderung nicht aus; es soll auch für den Nutzer problemlos möglich sein, sein Recht in Anspruch zu nehmen.

Die Unternehmen im Hanival-Szenario können ihre Kunden nur insoweit bei der Wahrnehmung ihrer Rechte unterstützen, als dass sie ihnen direkte Ansprechpartner (z.B. Datenschutzbeauftragte) und Kontaktmöglichkeiten nennen.

Lösungsansatz: Die im Lösungsansatz zu Anforderung 28 beschriebene Schnittstelle wird analog auch für Berichtigung, Löschung und Sperrung bereitgestellt.

5.4 Aufgabenbereiche

Die dreiunddreißig Gestaltungsvorschläge zu Zusicherung und Unterrichtung (Abschnitt 5.2 oben), sowie zu Protokollen und Auskunft (Abschnitt 5.3 oben) bilden eine detailliertere Liste von Anforderungen und Gestaltungsvorschlägen, die sich in übergeordnete Aufgabenbereiche ordnen lassen. Wir schlagen fünf solcher Aufgabenbereiche vor:

1. Eine *Verallgemeinerung von Zusicherungen* über den Datenschutz hinaus. Eine standardisierte Sprache für Zusicherungen kann etwa folgende Themenbereiche ansprechen:

- Datenschutzpolicys
 - Service-Level-Agreements
 - Quality-of-Service
 - Dienstleistungsverträge
2. *Protokolle* werden zur Zeit auf verschiedenen Ebenen geführt, zum Beispiel an Firewalls (IP-Pakete), an Web-Servern (HTTP-Requests und -Responses), an E-Mail-Servern (Annahme, Weiterleitung und Auslieferung von E-Mail). Dabei wird im Prinzip “alles“ in zeitlicher Abfolge protokolliert. Die Protokolldaten dienen teilweise zur Untersuchung von Fehlern oder Angriffen durch menschliche Experten, teilweise zum halbautomatisierten Data-Mining, um den unstrukturierten Datenmassen strukturierte inhaltliche Aspekte abzugewinnen. Tatsächlich haben Protokolldaten aber eine viel weitreichendere Bedeutung auch für
- A-posteriori Forensik für die IT-Revision
 - Erteilen von Auskunft über den Dienst an Kunden und Betroffene
 - Überprüfung von Zusicherungen für Kunden und Betroffene
 - Überprüfung von Zusicherungen und gesetzeskonformem Verhalten durch unabhängiges Audit
3. *Zusammensetzung von Zusicherungen*: Zusicherungen treten nicht isoliert auf. Zum Einen werden an derselben Stelle mehrere Zusicherungen zu verschiedenen Dienstaspekten zu verschiedenen Zeiten gegeben, zum Anderen werden besonders in einer SOA an verschiedenen Stellen verschiedene Zusicherungen gegeben, die sich dabei gleichwohl auf einen gemeinsamen übergeordneten Dienst beziehen. Daher sind einzelne Zusicherungen zu komplexen Zusicherungen zusammenzufassen. Dafür ist eine standardisierte Sprache erforderlich, die semantische Schlussfolgerungen zulässt. Dazu ist auch eine geeignete Authentifizierung zu liefern, die solche Zusicherungen rechtsverbindlich absichert.
4. *Zusicherung und Protokollierung*: Apriori-Zusicherungen, Protokollierung im laufenden Dienst, sowie die Auskunft und Überprüfung gehören in einen gemeinsamen Dienstkontext. Zur Zeit werden diese Aufgaben in ganz unterschiedlichen Formaten und Semantiken (d.h. informativ: in unterschiedlichen Sprachen) ausgeführt. Diese gehören zusammengeführt, damit Zusicherungen in semantisch klarer Weise festgehalten, zusammengesetzt, und später wiedergefunden und interpretiert werden können.

5. *Nutzungskompetenz*: Der Umgang mit Zusicherungen und Protokollen für die Unterrichtung, Auskunft und Überprüfung muss nicht nur technisch *möglich* sein, sondern die Anwender müssen zu ihrer Nutzung auch *fähig* sein. Über die standardisierte Sprache hinaus bedarf es Abstraktions- und Interpretationsverfahren, die aus der großen Datenmenge zur rechten Zeit die rechte Menge und Struktur an relevanten Aussagen zur Verfügung stellt. Das gilt sowohl auf der Ebene der Menschen, als auch auf der Ebene der automatisierten Prozesse. Diese beiden Aufgaben kann man mit den Stichworten

- Abstraktion
- und Schlussfolgerungen

zusammenfassen.

Kapitel 6

Innovation und Forschungsbedarf

6.1 Ergebnisse der Analyse

Die vorliegende Analyse hat ergeben, dass Chancen und Risiken der neuen Service-orientierten Architektur im Bereich der *Beherrschbarkeit* von SOA-Lösungen und des Nachvollzugs *verantwortlichen Handelns* mit SOA-Lösungen liegen. Zur Nutzung der Chancen wurden vier aussichtsreiche Faktoren zur Beherrschbarkeit und Verantwortlichkeit identifiziert:

1. Zusicherungen von Dienstqualität und Datenschutzkonformität,
2. Unterrichtung vor einem Dienst auf der Basis von Zusicherungen,
3. Protokollierung der Erbringung von Diensten und der Erhebung und Verarbeitung von Daten,
4. Auskunft zu jeder Zeit auf der Basis protokollierter Ereignisse.

Aufgrund rechtlicher und technischer Kriterien wurden fünf Anwendungsszenarien analysiert und in Bezug auf realistische Lösungsvorschläge für die Unterstützung der vier Beherrschbarkeitsfaktoren ausgewertet. Die rechtlichen Kriterien adressieren die informationelle Selbstbestimmung und andere Rechtsrahmen wie den Schutz von Betriebs- und Geschäftsgeheimnissen. Die technischen Kriterien beziehen sich auf die Kommunikationsbeziehungen und den Datenfluss zwischen den verteilten Komponenten. Dabei wurden diese Aspekte identifiziert: Personenbezug, Betroffene, die verantwortlichen Stellen, sowie der Zweck der Datenverwendung. Aufgrund der Datenflussanalyse wurden dann diese Rechtsgrundsätze untersucht: die Zulässigkeit der Datenverwendung, die Übermittlung an Drittstaaten, die Erforderlichkeit der

Datenverwendung, der Zweckbindungsgrundsatz, die Transparenz der Datenverwendung, die Qualität der Daten und allgemeine Anforderungen an die Datensicherheit.

Die fünf Szenarien wurden so ausgesucht, dass sie erstens eine gewisse Branchenbreite abdecken, und dass sie zweitens nicht nur den Datenschutz, sondern auch den Schutz von Geschäfts- und Betriebsgeheimnissen ansprechen. Der verteilte Musikdownload spielt in der Welt der virtuellen Güter und des Digitalen Rechtemanagements. Der Amazon Mechanical Turk behandelt Individuen sowohl als Auftraggeber, als auch als Auftragnehmer mit mehreren dazwischen geschalteten Web-Services über verschiedene Länder hinweg. Hanival repräsentiert die sich verändernde Welt von Diensteanbietern und Dienstebrokern im Internet-Service-Bereich. Die Produktionsstraßen im PSB-Modell schließlich gehören in die Welt der Produktpflege klassischer Flugzeugantriebe und adressiert vor allem den Schutz der Geschäfts- und Betriebsgeheimnisse im Firmenkundengeschäft (B2C).

Als Ergebnis der Szenarienanalyse wurden fünf Aufgabenbereiche beschrieben, die ihrerseits in weitere detailliertere Lösungsansätze aufgeschlüsselt wurden. Dieses sind die fünf Aufgabenbereiche zur Gestaltung einer beherrschbaren SOA für verantwortliches Handeln:

1. Eine *Verallgemeinerung von Zusicherungen* für Datenschutzpolicys, für Service-Level-Agreements, für den Quality-of-Service und für allgemeine Dienstleistungsverträge.
2. Einheitliche *Protokolle* für verschiedene Anwendungen wie für eine Forensik durch die IT-Revision, für das Erteilen von Auskunft, für die Überprüfung von Zusicherungen durch Kunden, Betroffene und durch ein unabhängiges Audit.
3. *Zusammensetzung von einfachen Zusicherungen* aus verteilten Diensten zu komplexen Zusicherungen.
4. Die *Verknüpfung von Zusicherung und Protokollierung* zu einem gemeinsamen Dienstkontext. Diese gehören zusammengeführt, damit Zusicherungen in semantisch klarer Weise festgehalten, zusammengesetzt, und später wiedergefunden und interpretiert werden können.
5. Die Stärkung der *Nutzungskompetenz*. Der Umgang mit Zusicherungen und Protokollen für die Unterrichtung, Auskunft und Überprüfung muss nicht nur technisch *möglich* sein, sondern die Anwender müssen zu ihrer Nutzung auch *fähig* sein. Dazu werden Abstraktions- und Interpretationsverfahren benötigt.

Wie eine Befragung führender SOA-Plattformanbieter ergeben hat, werden diese Aufgaben derzeit nur unzureichend unterstützt. Dies liegt zum einen am derzeitigen Reifegrad der untersuchten Technologien, z.B. wird der Standard WS-Security durchaus mehrdeutig interpretiert, zum anderen aber auch daran, dass grundlegender Forschungsbedarf besteht, um Aufgaben wie die einheitlichen Protokolle *erstmalig* abdecken zu können.

6.2 Handlungsempfehlungen und Forschungsbedarf

Die Ergebnisse dieser Analyse sind auf verschiedene Arten nutzbringend: Zunächst können Handlungsempfehlungen ausgesprochen werden, die auf Basis der organisatorischen Gegebenheiten und existierender Technologien bereits kurzfristig umgesetzt werden können. In einem weiteren Abschnitt wird darüber hinaus der Forschungsbedarf aufgezeigt, der sich aus der Analyse ergeben hat.

6.2.1 Handlungsempfehlungen

Die bisherigen technischen Lösungen¹ sind dafür geeignet, Teile der Anforderungen aus Abschnitt 5 umzusetzen oder zumindest einen ersten Beitrag zu ihrer vollständigen Umsetzung zu leisten.

Folgende Handlungsempfehlungen können gegeben werden:

- Unternehmen sollten ihre Dienste und Prozesse genau dokumentieren, so dass z.B. klar abgegrenzt werden kann, wo und wie personenbezogene Daten verarbeitet werden und welche Zusicherungen die Unternehmen zu machen in der Lage sind. Hierfür bieten sich die Dienste an, die einen großen Anteil an der Datenverarbeitung haben, sowie die Geschäftsprozesse, an denen der Kunde beteiligt ist.
- Unternehmen sollten sich selbst und ihre Geschäftspartner für die Prinzipien und Probleme des Datenschutzes sensibilisieren, sodass die Gefahr verringert wird, dass sich auf Grund von Unwissenheit datenschutzwidrige Geschäftspraktiken etablieren. Dies führt in weiterer Konsequenz dazu, dass juristische Verantwortlichkeiten innerhalb von Unternehmen wie auch zwischen Unternehmen klar erkannt und abgegrenzt werden müssen.

¹vgl. hierzu die Abschnitte 3.3.1 und 3.4.1

- Unternehmen sollten soweit wie möglich den allgemeinen Datenschutzprinzipien (wie beispielsweise dem Prinzip der Datensparsamkeit) folgen. Unter Umständen lässt sich dies bereits durch organisatorische Umstellungen (wie Verschlankung der Prozesse und Reorganisation der Zuständigkeiten) erreichen, sodass die Notwendigkeit technischer Lösungen reduziert wird.
- Unternehmen sollten sich mit existierenden Standards (wie z.B. EPAL) vertraut machen und sie nach Möglichkeit einsetzen, um praktische Erfahrungen mit aktuellen SOA- und Datenschutztechnologien zu sammeln. Dies unterstützt nicht nur die bereits genannte Sensibilisierung für den Datenschutz sondern kann auch unmittelbare Wettbewerbsvorteile (wie z.B. höhere Kundenzufriedenheit) bewirken.
- Zusicherungen in Form der Datenschutzunterrichtung können Unternehmen schon jetzt im P3P-Format anbieten. Auskunftsfunktionen, so wie sie üblicherweise etwa zur Korrektur von Name und Adressen durch die Kunden angeboten werden, können ohne Weiteres zu allgemeinen datenschutzrechtlichen Auskunftsfunktionen über alle personenbezogenen Daten erweitert werden. Es können ebenfalls schon heute technische und organisatorische Maßnahmen eingesetzt werden, um die Kompatibilität der Auskunftsdaten mit den Zusicherungen aus der Unterrichtung zu vergleichen. Hieraus ergeben sich in aller Regel Hinweise auf Potentiale zu mehr Datensparsamkeit.

Die oben aufgezeigten Handlungsempfehlungen lassen sich prinzipiell bereits heute realisieren. Dies ist jedoch mit hohem Aufwand verbunden, da für den Einsatz der bisherigen Technologien ein erheblicher Anteil manueller Tätigkeiten nötig ist. Für einen höheren Grad der Automatisierung, welcher langfristig für die Skalierbarkeit einer beherrschbaren Datenverarbeitung unabdingbar ist, sind die gegenwärtig bereits einsetzbaren Methoden und Technologien jedoch unzureichend.

6.2.2 Forschungsbedarf

Wie sich im Rahmen der Analyse gezeigt hat, werden viele der hier betrachteten Aufgaben weder von kommerziellen Plattformen gelöst, noch sind sie bisher überhaupt vollständig als Forschungsbedarf erkannt. So wird die Verteiltheit in Virtuellen Organisationen bei Themen wie den Policies bisher nur wenig diskutiert, die Protokollierung von Aktionen sogar fast gänzlich ignoriert und die integrierte Behandlung der identifizierten Aufgaben ist derzeit auf keiner uns bekannten Forschungsagenda zu finden.

Um die identifizierten Aufgaben zu lösen und Automatisierbarkeit zu erreichen, bedarf es unserer Analyse zufolge Anstrengungen in den folgenden vier Forschungsbereichen:

1. *Sprachdefinition*: Zu entwickeln ist eine formale Sprache zur integrierten Beschreibung von Daten, Restriktionen auf Daten, protokollierten Aktionen auf Daten und Zusicherungen der Dienste. Die Sprache muss maschinenlesbar, von Menschen verstehbar und normativ ausgerichtet sein, d.h. sie muss ausdrücken können, wer was gemacht hat (Audit) und wer zu was verpflichtet ist (Dienst- und Gesetzeserfüllung). Deontische Logiken für Verpflichtungen sind für verteilte Verpflichtungen, Verantwortlichkeiten und Restriktionen geeignet zu erweitern und in den SOA-Kontext von Webservices zu integrieren.
2. *Operationalisierung*: Die Sprache muss durch Werkzeuge operationalisiert werden, um aus verteilt vorliegenden Aussagen Schlussfolgerungen ableiten zu können. Hierbei muss es möglich sein, einzelne und zusammengesetzte Aussagen den Diensten und/oder Dienstleistern zuzurechnen.
3. *Rechtliche Relevanz*: Zur Anwendung in verschiedenen Szenarien, zum Beispiel im E-Commerce und E-Government werden konkrete Ontologien benötigt. Auf diese Weise wird die formale Sprache an den jeweiligen Nutzungskontext angepasst und somit mit der für den SOA-Kontext erforderlichen rechtlichen und inhaltlichen Relevanz versehen.
4. *Referenz-Architektur*: Zwecks realistischer Nutzung des hier vorgeschlagenen Ansatzes muss die vorgeschlagene Infrastruktur von Sprache, Sprachoperationalisierung und Ontologie in eine existierende Middleware integriert werden. Das Ziel sollte hier sein, eine Referenzarchitektur zu schaffen, die zu existierenden OpenSource- (z.B. J2EE/JBoss) oder kommerziellen Architekturen (z.B. Crossvision oder DotNet) kompatibel und integrierbar ist.

Eine Lösung, wie hier skizziert, würde die zuvor identifizierten Aufgaben lösen und dabei gleichzeitig Kernaufgaben der Beherrschbarkeit von Serviceorientierten Architekturen abdecken. Nur auf Basis dieser angestrebten Forschungsergebnisse kann das nachfolgend aufgezeigte Innovationspotenzial optimal ausgeschöpft werden.

6.3 Innovationspotenzial

Die vorgeschlagenen Forschungsaufgaben führen unmittelbar zu technischen Lösungen, die die rechtlichen Aspekte angemessen würdigen. Diese Lösungen führen zu technischen Innovationen (neuartige Software), zu ökonomischen Innovationen (Realisierung neuartiger Geschäftsmodelle), und zu Innovationen, die nicht das Recht ändern, aber aufgrund besserer Kompatibilität mit rechtlichen Vorgaben die Effizienz der Unternehmen erhöhen.

Technische Innovationen

Innovation 1: Die vorgeschlagenen semantischen Beschreibungen der Dienste erlauben ein wesentlich besseres Verständnis der internen und externen Prozesse aus einer technischen Sicht und damit eine bessere technische Nutzung der Middleware.

Innovation 2: Das Problem adäquater Service Governance, d.h. der Verwaltung von Diensten, ist ein gravierendes technisch-organisatorisches Problem, das durch die angestrebten Lösungen wesentlich erleichtert wird. Middleware, die Unterrichtung und Auskunft nativ unterstützt, wird aufgrund des technischen Vorsprungs einen Wettbewerbsvorteil erzielen können.

Innovationen 3 und 4: Der genannte Wettbewerbsvorteil entsteht vor allem auch dadurch, dass die Organisation, die diese verbesserte Middleware benutzt, sich flexibler mit anderen Organisationen vernetzen kann (3) und dabei ein kundenfreundlicheres System offerieren kann (4).

Ökonomische Innovationen

Innovation 5: Dieser eben erwähnte technische Fortschritt führt auch zu Innovationen auf der ökonomischen Ebene. Flexiblere und damit wirtschaftlichere Verkettungen von unternehmensübergreifenden Prozessen erlauben die Gründung neuer Unternehmen und Joint Ventures, die ohne eine solche Technologie nicht realisierbar gewesen wäre.

Innovation 6: Neuartige Geschäftsmodelle, die derzeit eher am Rande agieren, wie z.B. der Amazon Mechanical Turk oder die HumanGrid GmbH², werden leichter möglich durch Plattformen, die eine kontrollierte Weitergabe von Verantwortung ermöglichen.

²<http://www.humangrid.eu/>

Innovationen aufgrund verbesserter Kompatibilität mit rechtlichen Aspekten

Innovation 7: Compliance- und Auditing-Anforderungen erwachsen aus der Gesetzgebung, aus Bemühungen um Zertifizierungen und aus der Notwendigkeit, Nachweise über die eigenen Prozesse zu führen, um z.B. bessere Finanzierungsmöglichkeiten zu erhalten (z.B. wegen Basel-II). Eine wesentliche Innovation der hier vorgeschlagenen Forschungsaufgaben ergibt sich deswegen aus der deutlich erhöhten Konformität mit solchen gesetzlichen Anforderungen, Standardisierungsanforderungen oder vertragsrechtlichen Anforderungen.

Datenschutz-Innovationen

Innovation 8: Durch die Integration von Datenschutzmechanismen in SOA verbessert sich die Beherrschbarkeit ihrer Daten für Privatpersonen, was insbesondere für eine Durchdringung aller Lebensbereiche mit Informations- und Kommunikations-Technik (auch bspw. Electronic Government neben Electronic Commerce) erforderlich ist.

Wie oben gezeigt, entstehen vor allem Unternehmen, aber auch der Gesellschaft durch diese Innovationen erhebliche ökonomische Vorteile sowie der Vorteil einer verbesserten Konformität mit dem Datenschutzrecht. Diese Innovationen können jedoch nur aus erheblichen akademischen und industriellen Forschungsbemühungen hervorgehen – es besteht also die Notwendigkeit, Forschungsprojekte sowohl in der Wissenschaft als auch in der Industrie zu fördern.

Index

- Akzeptanz, 30
- Amazon Mechanical Turk, 84
- APPEL, 42
- Auskunft, 38, 51
- Beherrschbarkeit, 36
 - Faktoren, 37
 - subjektive, 40
- Betriebs- und Geschäftsgeheimnisse, 27
- Betroffener
 - Betroffenenrechte, 22
- Datenschutzrecht, 12
 - Grundprinzipien, 16
- Datensicherheit, 22
- Datensparsamkeit, 20
- Datenvermeidung, 20
- Drittstaaten, 19
- EPAL, 44
- Erforderlichkeit, 20
- Hanival, 69
- KAoS, 45
- Kosten, 29
- OWL, 45
- P3P, 42
- Personenbezug, 16
- PotatoSystem, 58
- Protokollierung, 39, 51
- PSB, 95, 102
- Rei, 45
- Service-Lebenszyklus, 35
- Service-orientierte Architektur, 6
- Sicherheit, 31
- SOA, *siehe* Service-orientierte Architektur
- Transparenz, 21
- TRIPS, 28
- Unterrichtung, 37, 41
- Verantwortlicher, 17
- Virtuelle Organisation, 5
- Web Service, 6
- WS-Policy, 44
- WSPL, 44
- XACML, 44
- Zulässigkeit, 18
- Zusicherung, 41
- Zusicherungen, 38
- Zweckbindung, 21

Literaturverzeichnis

- [4Fr06] 4FRIENDSONLY.COM INTERNET TECHNOLOGIES AG: *Technische Beschreibung des Micro-Payment-Systems Paybest*, 5 2006
- [AD05] ANDERSON, Anne H. ; DEVARAJ, Balasubramanian: XACML-Based Web Services Policy Constraint Language (WS-PolicyConstraints) / Sun Microsystems. 2005. – Working Draft. <http://research.sun.com/projects/xacml/ws-policy-constraints-current.pdf>
- [And06a] ANDERSON, Anne H.: A comparison of two privacy policy languages: EPAL and XACML. In: *SWS '06: Proceedings of the 3rd ACM workshop on Secure web services*. New York, NY, USA : ACM Press, 2006. – ISBN 1-59593-546-0, S. 53–60
- [And06b] ANDERSON, Anne H.: Domain-Independent, Composable Web Services Policy Assertions. In: *POLICY '06: Proceedings of the Seventh IEEE International Workshop on Policies for Distributed Systems and Networks (POLICY'06)*. Washington, DC, USA : IEEE Computer Society, 2006. – ISBN 0-7695-2598-9, S. 149–152
- [BB05] BAKER, M. A. ; BOAKES, R. J.: Semantic Logging Using the Resource Description Framework / Distributed Systems Group, University of Portsmouth. 2005. – Forschungsbericht
- [BGW05] BIZER, Johann ; GRIMM, Rüdiger ; WILL, Andreas: privacy4DRM. Datenschutzverträgliches und nutzungsfreundliches Digital Rights Management. / Bundesministeriums für Bildung und Forschung (BMBF). 2005. – Studie
- [Biz03] BIZER, Johann: Personenbezug bei Cookies. In: *Datenschutz und Datensicherheit (DuD)* 27 (2003), S. 644

- [Biz06] BIZER, Johann: Das Recht der Protokollierung. In: *Datenschutz und Datensicherheit (DuD)* 30 (2006), S. 270–273
- [Biz07] BIZER, Johann: Datenschutz durch Prozessmanagement. In: *Datenschutz und Datensicherheit (DuD)* 31 (2007), S. 289
- [Brü99] BRÜTSCH, David: *Virtuelle Unternehmen*. vdf Hochschulverlag an der ETH Zürich, 1999
- [CLM02] CRANOR, Lorrie ; LANGHEINRICH, Marc ; MARCHIORI, Massimo: A P3P Preference Exchange Language 1.0 (APPEL1.0) / W3C. 2002. – W3C Working Draft. <http://www.w3.org/TR/2002/WD-P3P-preferences-20020415/>
- [DDM04] DOMINGUE, J. ; DZBOR, M. ; MOTTA, E.: Magpie: Supporting Browsing and Navigation on the Semantic Web. In: NUNES, N. (Hrsg.) ; RICH, C. (Hrsg.): *Proceedings ACM Conference on Intelligent User Interfaces (IUI)*, 2004, S. 191–197
- [Dea04] DEAN, Mike (Hrsg.) ; SCHREIBER, Guus (Hrsg.): OWL Web Ontology Language Reference / W3C. 2004. – W3C Recommendation. <http://www.w3.org/TR/2004/REC-owl-ref-20040210/>
- [Die04] DIERSTEIN, Rüdiger: Sicherheit in der Informationstechnik - der Begriff IT-Sicherheit. In: *Informatik-Spektrum* 4 (2004), S. 343–353
- [DJMZ05] DOSTAL, Wolfgang ; JECKLE, Mario ; MELZER, Ingo ; ZIEGLER, Barbara: *Service-orientierte Architekturen mit Web-Services. Konzepte – Standards – Praxis*. Elsevier, Spektrum Akademischer Verlag, 2005
- [DKWW07] DÄUBLER, Wolfgang ; KLEBE, Thomas ; WEDDE, Peter ; WEICHERT, Thilo: *Bundesdatenschutzgesetz - Basiskommentar*. 2. Aufl. Frankfurt : Bund-Verlag, 2007
- [ECC06] EGELMAN, Serge ; CRANOR, Lorrie F. ; CHOWDHURY, Abdur: An analysis of P3P-enabled web sites among top-20 search results. In: *ICEC '06: Proceedings of the 8th international conference on Electronic commerce*. New York, NY, USA : ACM Press, 2006. – ISBN 1–59593–392–1, S. 197–207

- [GS05] GOLLA, Peter ; SCHOMERUS, Rudolf: *Bundesdatenschutzgesetz - Kommentar*. 8. Aufl. München : Verlag C. H. Beck, 2005
- [HBB96] HALLAM-BAKER, Phillip M. ; BEHLENDORF, Brian: Extended Log File Format / W3C. 1996. – Forschungsbericht. <http://www.w3.org/pub/WWW/TR/WD-logfile-960323.html>
- [JP04] JENSEN, Carlos ; POTTS, Colin: Privacy policies as decision-making tools: an evaluation of online privacy notices. In: *CHI '04: Proceedings of the SIGCHI conference on Human factors in computing systems*. New York, NY, USA : ACM Press, 2004. – ISBN 1-58113-702-8, S. 471-478
- [KE05] KEMPER, Alfons ; EICKLER, André: *Datenbanksysteme: Eine Einführung*. 5. Oldenbourg, 2005
- [KFJ03] KAGAL, Lalana ; FININ, Tim ; JOSHI, Anupam: A Policy Language for a Pervasive Computing Environment. In: *POLICY '03: Proceedings of the 4th IEEE International Workshop on Policies for Distributed Systems and Networks*. Washington, DC, USA : IEEE Computer Society, 2003. – ISBN 0-7695-1933-4, S. 63-74
- [KH06] KIETHE, Kurt ; HOHMANN, Olaf: Der strafrechtliche Schutz von Geschäfts- und Betriebsgeheimnissen. In: *Neue Zeitschrift für Strafrecht (NStZ)* (2006), S. 185-191
- [KK00] KÖHNTOPP, Marit ; KÖHNTOPP, Kristian: Datenspuren im Internet. In: *Computer und Recht (CR)* (2000), S. 248
- [Leo06] LEOPOLD, Nils: Protokollierung und Mitarbeiterdatenschutz. In: *Datenschutz und Datensicherheit (DuD)* 5 (2006), S. 274-276
- [MCG06] MILNE, George R. ; CULNAN, Mary J. ; GREENE, Henry: A Longitudinal Assessment of Online Privacy Notice Readability. In: *Journal of Public Policy and Marketing* 25 (2006), Nr. 2, S. 238-249
- [Mos03] MOSES, Tim (Hrsg.): XACML profile for Web Services, Working Draft 04 / OASIS. 2003. – Forschungsbericht. <http://www.oasis-open.org/committees/download.php/3661/draft-xacml-wspl-04.pdf>

- [Mos05] MOSES, Tim (Hrsg.): eXtensible Access Control Markup Language (XACML) Version 2.0 / OASIS. 2005. – OASIS Standard. http://docs.oasis-open.org/xacml/2.0/access_control-xacml-2.0-core-spec-os.pdf
- [Mös01] MÖSLEIN, Kathrin: Die virtuelle Organisation: Von der Idee zur Wettbewerbsstrategie. In: ROHDE, Markus (Hrsg.) ; RITTENBRUCH, Markus (Hrsg.) ; WULF, Volker (Hrsg.): *Auf dem Weg zur virtuellen Organisation*. Physica-Verlag Heidelberg, 2001, S. 13–31
- [Neu03] NEUMANN, Heike: Anonyme Zahlungssysteme - Bezahlen ohne seinen guten Namen. In: *Datenschutz und Datensicherheit (DuD)* 27 (2003), S. 270
- [NG05] NÜTZEL, J. ; GRIMM, R.: Musikvertrieb mit Potato Web Services. In: *Datenschutz und Datensicherheit (DuD)* 3 (2005), Nr. 2005, S. 125–129
- [Oes04] OESTEREICH, Bernd: *Objektorientierte Softwareentwicklung : Analyse und Design mit der UML 2.0*. Oldenburg Verlag München Berlin, 2004
- [PS03] POWERS, Calvin ; SCHUNTER, Matthias: Enterprise Privacy Authorization Language (EPAL 1.2) / W3C. 2003. – W3C Member Submission. <http://www.w3.org/Submission/2003/SUBM-EPAL-20031110/>
- [Sch03a] SCHAAR, Peter: Datenschutz bei Web-Services. In: *Recht der Datenverarbeitung (RDV)* (2003), S. 59–67
- [Sch03b] Kap. Datenschutzrecht In: SCHULTE, Martin (Hrsg.): *Handbuch des Technikrechts*. Berlin Heidelberg : Springer-Verlag, 2003, S. 582
- [Sch04] SCHLEIPFER, Stefan: Das 3-Schichten-Modell des Multimedia-datenschutzrechts. In: *Datenschutz und Datensicherheit (DuD)* 28 (2004), S. 727–733
- [Sim06] SIMITIS, Spiros (Hrsg.): *Bundesdatenschutzgesetz*. 6. Aufl. Baden-Baden : Nomos Verlagsgesellschaft, 2006
- [SMS+06] STEINERT, Bastian ; MÖLLER, Jan ; SOMMER, Philipp ; STEINHAUER, Sebastian ; HÜTTENRAUCH, Stefan ; QUECK, Tobias ;

- HAHMANN, Torsten: Dynamic Supply Chain Scenario for Internet Service Providers / EU Project Adaptive Services Grid. 2006. – Forschungsbericht
- [Spi05] SPINDLER, Gerald: Haftungs- und vertragsrechtliche Probleme von Web-Services. In: *Datenschutz und Datensicherheit (DuD)* (2005), S. 139–141
- [UBJ⁺03] USZOK, A. ; BRADSHAW, J. ; JEFFERS, R. ; SURI, N. ; HAYES, P. ; BREEDY, M. ; BUNCH, L. ; JOHNSON, M. ; KULKARNI, S. ; LOTT, J.: KAOs Policy and Domain Services: Toward a Description-Logic Approach to Policy Representation, Deconfliction, and Enforcement. In: *POLICY '03: Proceedings of the 4th IEEE International Workshop on Policies for Distributed Systems and Networks*. Washington, DC, USA : IEEE Computer Society, 2003. – ISBN 0-7695-1933-4, S. 93–96
- [UBJ⁺04] USZOK, Andrzej ; BRADSHAW, Jeffrey M. ; JEFFERS, Renia ; TATE, Austin ; DALTON, Jeff: Applying KAOs Services to Ensure Policy Compliance for Semantic Web Services Workflow Composition and Enactment. In: *International Semantic Web Conference, 2004*, S. 425–440
- [Ved07] VEDAMUTHU, Asir S. (Hrsg.) ; ORCHARD, David (Hrsg.) ; HIRSCH, Frederick (Hrsg.) ; HONDO, Maryann (Hrsg.) ; YENDLURI, Prasad (Hrsg.) ; BOUBEZ, Toufic (Hrsg.) ; ÜMIT YALÇINALP (Hrsg.): Web Services Policy 1.5 - Framework / W3C. 2007. – W3C Recommendation. <http://www.w3.org/TR/2007/REC-ws-policy-20070904>
- [Wei06] WEICHERT, Thilo: Auskunftsanspruch in verteilten Systemen. In: *Datenschutz und Datensicherheit (DuD)* 30 (2006), S. 694–699
- [Wol06] WOLTHUSEN, Stephen D.: Revisions sichere Protokollierung in Standardbetriebssystemen. In: *Datenschutz und Datensicherheit (DuD)* 30 (2006), S. 694–699
- [WS06] WENNING, Rigo ; SCHUNTER, Matthias: The Platform for Privacy Preferences 1.1 (P3P1.1) Specification / W3C. 2006. – W3C Working Group Note. <http://www.w3.org/TR/2006/NOTE-P3P11-20061113/>