

Service-orientierte Architekturen in virtuellen Organisationen

Chancen und Risiken für den Datenschutz

Daniel Pähler, Christoph Ringelstein, Felix Schwagereit

Das Paradigma der Service-orientierten Architekturen stellt neue Anforderungen an die Implementierung von Datenschutz zur Sicherstellung der Beherrschbarkeit dieser komplexen Systeme in virtuellen Organisationen.



Daniel Pähler

Wissenschaftlicher Mitarbeiter der Arbeitsgruppe „IT Risk Management“ der Universität Koblenz-Landau

E-Mail: tulkas@uni-koblenz.de



Christoph Ringelstein

Wissenschaftlicher Mitarbeiter der Arbeitsgruppe „Informationssysteme & Semantic Web“ der Universität Koblenz-Landau

E-Mail: cringel@uni-koblenz.de



Felix Schwagereit

Wissenschaftlicher Mitarbeiter der Arbeitsgruppe „Informationssysteme & Semantic Web“ der Universität Koblenz-Landau

E-Mail: schwagereit@uni-koblenz.de

Einleitung

Der Einsatz von Service-orientierten Architekturen (SOA) in Unternehmen ermöglicht die flexible Konfiguration von komplexen Arbeitsprozessen. Neben der Einbindung unternehmensinterner Dienste können auch Dienste externer Anbieter in den Arbeitsprozess integriert werden. Auf diese Weise entstehen virtuelle Organisationen (VO), die sich dynamisch an sich ändernde Anforderungen anpassen können. Mit der Komplexität der VO wachsen die Risiken für den Datenschutz. Auf der anderen Seite bietet jedoch gerade die höhere Flexibilität und Dynamik, die durch die Umsetzung der SOA gewonnen werden, die Chance und die Mittel, den Risiken entgegenzuwirken.

In diesem Artikel werden wesentliche Ergebnisse der Untersuchung „Technikanalyse und Risk Management für Service-orientierte Organisationen in Virtuellen Organisationen“ präsentiert¹.

Abschnitt 1 legt die Risiken dar, die für den Datenschutz in einer VO bestehen. Abschnitt 2 betrachtet, wie man die Datenverarbeitung beherrschen kann, um diese Risiken zu minimieren, worauf in Abschnitt 3 die heute existierenden Mittel daraufhin untersucht werden, inwieweit sie zur Beherrschbarkeit beitragen. Abschließend wird in Abschnitt 4 ein integrierter Lösungsansatz vorgestellt, der die Datenverarbeitung in einer VO beherrschbar macht.

1 Risiken

Datenschutz spielt nicht nur in einzelnen Unternehmen eine Rolle, sondern auch in

¹ Die Analyse wird vom BMBF finanziert und entsteht in Kooperation der Universität Koblenz mit dem ULD SH. Veröffentlichung 11/2007

einer VO. In dieser geben die höhere Komplexität und die neu auftretenden Problemstellungen, die sich aus der größeren Anzahl an beteiligten Parteien ergeben, dem Datenschutz eine neue Dimension. Einige herausragende Problemstellungen betrachten wir im Folgenden kurz.

1.1 Komplexität von Datenflüssen

Um die Datenschutzrichtlinien und die Datenschutzgesetze einzuhalten, benötigen Unternehmen eine Übersicht über ihre internen Datenflüsse. Allerdings fehlt diese häufig selbst kleineren Unternehmen. Eine Ursache hierfür ist die oft gewachsene Komplexität der Prozesse. In einer VO nimmt die Komplexität durch die Kombination der Arbeitsprozesse mehrerer Unternehmen zu großen integrierten Prozessen deutlich zu. Zusätzlich sind die Prozesse der VO weniger transparent, da die beteiligten Unternehmen sich nicht gegenseitig die Überwachung ihrer Datenflüsse gestatten.

1.2 Komplexität von Verantwortlichkeiten

Da eine VO aus vielen Einzelunternehmen besteht, muss klar erkennbar sein, welches Unternehmen für welche Aktionen, die während der Verarbeitung von personenbezogenen Daten ausgeführt wurden, verantwortlich ist [11]. Zusätzlich erlauben Flexibilität und Dynamik einer VO, den Arbeitsprozess zur Laufzeit anzupassen und beteiligte Unternehmen durch andere zu ersetzen. Diese Eigenschaft in Kombination mit der Tatsache, dass nur Unternehmen mit direktem Kundenkontakt ein Vertragsverhältnis mit dem Kunden haben, erschwert ihm die Identifikation der für die Verarbeitung

seiner Daten verantwortlichen Unternehmen. Daher sollte in den Verträgen bzw. den Zusicherungen zum Ausdruck kommen, dass gegebenenfalls eine Auftragsdatenverarbeitung oder Funktionsübertragung von Teilen der Dienstleistung stattfindet. In jedem Fall muss dies in der erteilten Auskunft erkennbar sein.

1.3 Internationale virtuelle Organisationen

Die Flexibilität, die durch die Umsetzung des Paradigmas der Service-Orientierung gewonnen wird, ermöglicht die ad-hoc Integration externer Dienste in Arbeitsprozesse. Diese Dienste können auch von Unternehmen angeboten werden, die im Ausland ansässig sind. Der Umstand, dass das Datenschutzrecht der EU-Länder die Übermittlung von Daten nur in Länder mit vergleichbaren Datenschutzstandards zulässt, begrenzt die Möglichkeiten, ad-hoc Kooperationen mit internationaler - nicht europäischer - Beteiligung einzugehen. Dieses Problem kann nicht technisch gelöst werden, sondern muss explizit vertraglich bzw. mit Hilfe von Handelsabkommen wie dem Safe Harbor Framework [10] geklärt werden.

1.4 Zusammenführung verteilter Datenbestände

Standardisierte Kommunikationsschnittstellen und Datenformate, wie sie grundlegend für SOA sind, erleichtern den Zugriff auf Daten, die verteilt bei verschiedenen Unternehmen vorliegen, sowie deren Auswertung erheblich. Dadurch kann es möglich sein, dass ansonsten separate Datenbestände kombiniert und neue Informationen von diesen abgeleitet werden können.

2 Beherrschbarkeit

Beherrschbarkeit der Datenverarbeitung ist ein Schlüsselkonzept für die Behandlung der sich in einer VO ergebenden Probleme. Sie 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“ [2]. Die Betroffenen² kön-

nen hierbei die Kunden der VO sein, deren personenbezogene Daten, und indirekt auch deren Datenschutzrechte in einem 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 betrachtet, wie die Beherrschung der Datenverarbeitung helfen kann, die aus dem Datenschutzrecht für die VO entstehenden Probleme zu lösen. Dem Kunden werden besonders durch sein Recht auf Auskunft sowie durch die Pflicht des Unternehmens zur Unterrichtung Mittel eingeräumt, um die Verarbeitung seiner Daten beherrschbar zu machen. Diese Rechte und Pflichten zwingen das Unternehmen, geeignete organisatorische und technische Maßnahmen umzusetzen, um in einer SOA Unterrichtung und Auskunft geben zu können. Hierfür ist erforderlich, dass ein Unternehmen seine eigene Datenverarbeitung beherrscht. Grundlegende Mechanismen, die zur Erfüllung dieses Erfordernisses beitragen, sind Zusicherungen und Protokollierung. In den folgenden Abschnitten werden die vier Beherrschbarkeitsfaktoren Unterrichtung, Auskunft, Zusicherungen und Protokollierung einzeln beleuchtet.

2.1 Unterrichtung

Um Betroffene 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 zwangsläufig entbunden werden.

Die Relevanz der Unterrichtung für die Beherrschbarkeit ergibt sich daraus, dass der Kunde nur auf Basis der Unterrichtung eine begründete Entscheidung treffen kann, ob er sein Recht auf informationelle Selbstbestimmung geschützt sieht und ob er dementsprechend seine Daten preisgibt.

2.2 Auskunft

Das gesetzlich vorgeschriebene Recht auf Auskunft erlaubt es Betroffenen, von datenverarbeitenden Stellen 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 dient⁴.

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 (der über ihn gespeicherten Daten) benötigt, um eine Beeinträchtigung dieser Belange vermeiden zu können (seine Daten berichtigen, löschen oder sperren zu lassen)⁵.

2.3 Zusicherungen

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

Aus technischer Sicht haben Zusicherungen starke Ähnlichkeit mit den so genannten Constraints (Randbedingungen), wie sie in der Softwaretechnik Anwendung finden. Hierin beschränken Constraints mögliche „Inhalte, Zustände oder die Semantik“ der Elemente [7]. 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 dadurch die Gesetzeskonformität der Prozesse des Unternehmens zu gewährleisten.

² Der „Betroffene“ ist in diesem Kontext nicht mit dem „Betroffenen“ im Sinne des BDSG zu verwechseln.

³ In Anlehnung an § 4 Abs. 3 BDSG.

⁴ In Anlehnung an § 34 Abs. 1 BDSG.

⁵ Vgl. [11].

2.4 Protokollierung

Die Aufgabe der Protokollierung in datenverarbeitenden Systemen ist die Ermöglichung der nachträglichen Rekonstruktion von Verhalten. Im Gegensatz zu Zusicherungen eignet sich Protokollierung nur a posteriori als Hilfsmittel zur Gewährung von Beherrschbarkeit. Um ihrer Aufgabe 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 kann ein Protokoll als objektive Aufzeichnung die nachträgliche Rekonstruktion von Datenflüssen auch aus unvorhergesehenen Perspektiven erlauben. Aus diesem Grund unterstützt Protokollierung die Auskunft wie auch das Auffinden von Verstößen gegen Datenschutzaufgaben oder Verträge. Deshalb sind Unternehmen zur Protokollierung der Zugriffe auf sensible personenbezogene Daten verpflichtet. Die Protokolle können allerdings auch selbst personenbezogene Daten enthalten und somit dem Datenschutzrecht unterliegen.

3 Situation heute

In der Praxis greift ein Nutzer auf eine im Web angebotene Dienstleistung überwiegend mit Hilfe eines Webbrowsers zu, dementsprechend werden auch Unterrichtung und Auskunft nicht über Web Services realisiert. Für Zusicherungen und Protokollierung hingegen existieren auch Web-Service-basierte Ansätze. Im Folgenden werden aktuelle Umsetzungen der Beherrschbarkeitsfaktoren aufgezeigt.

3.1 Unterrichtung

Unterrichtung wird von der Mehrzahl der Unternehmen als Text in einer Datenschutzerklärung bzw. Datenschutzrichtlinie gegeben. Der Inhalt der Datenschutzerklärung ist auf der Webseite publiziert und wird durch Verlinkung während der Beauftragung der Dienstleistung als Unterrichtung wirksam bzw. Vertragsbestandteil. Eine Datenschutzerklärung ist typischerweise umfangreich⁶ und für Personen ohne rechtliche Vorbildung schwer verständlich.

⁶ Im US-amerikanischen Raum beispielsweise umfasst sie durchschnittlich 2000 Wörter.

Der P3P-Standard (Platform for Privacy Preferences) [12] des World Wide Web Consortium (W3C) ist ein auf XML basierender Ansatz zum formalen Ausdruck von Datenschutzerklärungen eines Unternehmens gegenüber seinen Kunden.

Um eine P3P-Datenschutzerklärung zu verarbeiten, benötigt der Kunde ein Computerprogramm, das ihm die P3P-Aussagen verständlich darstellt und sie gegebenenfalls mit seinen Datenschutzpräferenzen abgleicht. Der Standard zum Formulieren von Datenschutzpräferenzen ist hierbei APPEL [1]. Obwohl die Verbreitung von P3P nach wie vor sehr eingeschränkt ist, bindet eine steigende Anzahl von Unternehmen P3P-konforme Datenschutzerklärungen in ihre Webseiten ein.

3.2 Auskunft

Die Einholung einer Auskunft bedarf der Initiative des Betroffenen; um den Antrag auf Auskunftserteilung zu stellen, muss dieser zunächst das verantwortliche Unternehmen identifizieren und es dann schriftlich kontaktieren; die Antwort erfolgt ebenfalls schriftlich. Dieser Vorgang 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 [11]. Außerdem kann der Betroffene seine Anfrage nicht automatisiert stellen, sondern muss sie ausformulieren. Bei internationalen Unternehmen kann dies nicht nur zu sprachlichen Problemen, sondern auch zu Rechtsunsicherheiten führen.

Schließlich werden Auskunftersuchen oft nicht oder nur unzureichend beantwortet, was auch daran liegt, dass viele Unternehmen organisatorisch und technisch nicht in der Lage sind, Auskunft zu erteilen [11].

3.3 Zusicherungen

In der Realität werden Zusicherungen zwischen Unternehmen entweder gar nicht oder manuell ausgehandelt und textuell als Bestandteil eines Vertrages eingebunden. Es existieren jedoch Standardisierungsbemühungen und Forschungsprojekte mit dem Ziel, Zusicherungen zu formalisieren und an die Ausführung von Webservices zu koppeln.

Bekannte Ansätze, die geeignet sind, in der SOA einer VO Anwendung zu finden, sind beispielsweise die Enterprise Privacy

Authorization Language (EPAL) [8] und die Web Services Policy Language (WSPL) [6].

3.4 Protokollierung

Die meisten Software-Systeme sind imstande, Protokolle über bestimmte Ereignisse zu führen. Der Detailgrad der Protokolleinträge reicht dabei von kurzen, auf den einzelnen Rechner bezogenen Meldungen über ausführliche, anwendungsspezifische Meldungen moderner Software-Systeme bis hin zu vollständigen Kommunikationsprotokollen, in denen alle ein- und ausgehenden Nachrichten eines Systems festgehalten werden.

Das automatisierte Verarbeiten von Protokollen ist dank standardisierter (wenngleich oft nicht weit verbreiteter) Dateiformate wie beispielsweise dem „Extended Log File Format“ des W3C [4] schon länger möglich; auch für eine zentrale Protokollierung in verteilten Systemen innerhalb von Unternehmen existieren bereits Lösungen (z.B. durch Software wie „syslog“). Dennoch sind einige Probleme betreffend die Protokollierung von datenschutzrelevanten Vorgängen in VO nach wie vor ungelöst. Zunächst protokolliert jedes Unternehmen nur seine eigenen Vorgänge. Dies macht es aus Kundensicht schwer, den Ablauf einer spezifischen Datenverarbeitung in einer VO zu rekonstruieren. Ein weiteres Problem ist die große Menge an potentiell relevanten Protokolleinträgen, die kaum manuell gesichtet werden kann. Für eine Protokollierung auf höherem Abstraktionsniveau, die eine Informationsselektion bzw. Informationsaggregation unterstützt, existieren jedoch bislang kaum Standards.

3.5 Zusammenfassung

Die in diesem Abschnitt benannten Standardisierungsansätze sind schon seit einigen Jahren in der Entwicklung. Jedoch besitzen sie weder die Reife noch die breite Akzeptanz, um Interoperabilität der Services innerhalb einer VO über die Grenzen der Lösung eines Anbieters hinaus zu gewährleisten.

4 Integrierter Lösungsansatz

Es stellt sich die Frage, in wie weit die aktuellen Technologien und Ansätze in der Lage sind, die noch offenen Probleme bei

der Implementierung von Datenschutz in SOA zu unterstützen.

Existierende Ansätze sind dafür geeignet, bestimmte Aspekte (wie Unterrichtung oder Protokollierung) zu unterstützen, jedoch deckt kein einzelner Ansatz alle Aspekte ab. Auf Grund der Abhängigkeiten zwischen Zusicherungen, Präferenzen und Unterrichtung, zwischen Unterrichtung und Auskunft sowie zwischen Auskunft und Protokollierung schlagen wir einen integrierten Ansatz für einen maschineninterpretierbaren Formalismus vor, der auf einer wohldefinierten Ontologie⁷ basiert. Die Verwendung eines maschineninterpretierbaren Formalismus ermöglicht es, viele Aufgaben teilautomatisiert durchzuführen, einfache Aufgaben sogar vollautomatisiert. Dies führt zu einer Verringerung der vom Anwender zu beherrschenden Komplexität. Eine Ontologie, sofern sie von allen Beteiligten genutzt wird, fördert ein gemeinsames Verständnis von Begriffen, und somit auch der Gegenstandsbereiche Datenschutz und Services. Dies führt unter anderem zu einer Verringerung des Aufwands für das Herstellen von Interoperabilität. Die folgenden Abschnitte geben einen kurzen Überblick darüber, welche Datenschutzaufgaben automatisiert oder zumindest teilautomatisiert werden können und wie existierende Technologien hierfür anwendbar sind.

4.1 Vergleich von Zusicherungen mit Präferenzen

Die Präferenzen des Kunden beschreiben, welche Verarbeitungsprozesse seiner personenbezogenen Daten der Kunde bereit ist zuzulassen. Werden die Zusicherungen und die Präferenzen nach dem o.g. maschineninterpretierbaren Formalismus spezifiziert, erlaubt dies den semiautomatisierten Vergleich. Somit ist im Falle der Nutzung einer Ontologie menschliches Eingreifen nur notwendig, wenn ein Konflikt auftritt, der nicht automatisch zu lösen ist.

Aktuelle auf semantischen Sprachen basierenden Ansätze zur Formalisierung von Zusicherungen wie z.B. Rei [5] erfüllen diese Anforderung bereits. Doch ist weder die Beschreibung von Web-Services mit diesen Ansätzen weit verbreitet, noch unterstützen sie Protokollierung oder Auskunft.

⁷ Nach Gruber ist eine Ontologie eine „explizite Spezifikation einer Begriffsbildung“ [3].

4.2 Kombinieren von Zusicherungen

Zusicherungen können verwendet werden, um den Kunden über die Nutzung seiner personenbezogenen Daten in der VO zu unterrichten. Um eine vollständige Unterrichtung für die VO durchzuführen, müssen alle Zusicherungen der beteiligten Unternehmen berücksichtigt und kombiniert werden. Eine Formalisierung auf Basis einer Ontologie unterstützt diese Kombination von Zusicherungen. Zusätzlich erlaubt eine hinreichende Formalisierung die teilautomatisierte Durchführung des Kombinationsprozesses.

Einige der vorgestellten Ansätze ermöglichen bereits das Kombinieren von Zusicherungen unterschiedlicher Parteien zu einer gemeinsamen Zusicherung. Werden diese Ansätze um Möglichkeiten zur Spezifizierung von Protokollen und Auskunft erweitert, genügen sie den hier vorgestellten Anforderungen.

4.3 Flexibler Standard für Protokollierung

Mit Techniken des Data Mining können Informationen über die Verarbeitung personenbezogener Daten aus Protokollen extrahiert werden. Die Automatisierung des Extraktionsprozesses und der Erteilung von Auskunft kann durch ein System unterstützt werden, das auf maschineninterpretierbaren Protokollen beruht, die insbesondere datenschutzrelevante Informationen explizit unterstützen.

Falls eine einzelne Applikation die Erzeugung ontologiebasierter Protokolle unterstützt, so sind diese Ontologien meist für den Anwendungsbereich der Applikation definiert und somit nicht applikationsübergreifend nutzbar. Darüber hinaus sind die vorhandenen Ansätze nicht geeignet, einen Abgleich der Protokolle mit den gemachten Zusicherungen durchzuführen. Aus diesen Gründen identifizieren wir die Entwicklung eines Standards, welcher eine applikation-sunabhängige Protokollierung auf Basis von kompatiblen Ontologien für einzelne Anwendungsfelder ermöglicht, als eine zukünftige Herausforderung. Darüber hinaus sollte dieser Standard mit dem für Zusicherungen verwendeten Formalismus kompatibel sein.

4.4 Zugriff auf Protokolle

Um die Extraktion der notwendigen Informationen aus den Protokollen zu ermöglichen, muss ein Zugang zu den einzelnen benötigten Protokollen bzw. Protokolleinträgen gegeben sein. Dies kann mit Methoden erreicht werden, die einen „single point of access“, d.h. eine einzelne für Aufbewahrung und Herausgabe der Protokolle verantwortliche Stelle, verwenden. Die zentrale Protokollierung ist eine solche Methode. Hierfür übermitteln alle Unternehmen der VO ihre Protokolle an einen Protokollierungsserver, über den sie später abrufbar sind. Obwohl für diese Methode bereits technische Lösungen existieren, sind diese nicht für die Anwendung in einer VO geeignet. Eine Ursache hierfür ist, dass sich eine VO spontan aus mehreren unabhängigen Unternehmen bilden und genauso schnell wieder auflösen kann. Deshalb ist es schwer, einen zentralen Protokollierungsserver zu etablieren, auf den sich die Unternehmen jedes Mal bei der Bildung einer neuen VO einigen müssen. Eine Alternative zu der zentralen Protokollierung ist die Verwendung von „Sticky Logs“ [9]. Dies sind Protokolle, welche direkt an das jeweilige Datum angehängt werden, und die die bisherige Verwendung bzw. Verarbeitung dieses Datums zum Inhalt haben. Wird das Datum weitergegeben, so muss auch das mit ihm assoziierte Sticky Log weitergegeben werden. Somit ist jede Information über die Verarbeitung dieses Datums innerhalb der VO als Metadatum mit dem Datum verknüpft und an einer Stelle verfügbar. Darüber hinaus besteht der Inhalt des Sticky Logs nur aus Protokollinformationen über das jeweilige Datum. Das Filtern von Protokollen nach speziellen Informationen, die ein konkretes Datum betreffen, ist somit überflüssig. Ein Nachteil dieses Ansatzes ist jedoch die Tatsache, dass das Sticky Log von jedem gelesen und manipuliert werden kann, der das Datum verarbeitet. Um dies zu vermeiden, ist der Einsatz von Sticky Logs nur in Verbindung mit Verschlüsselung und elektronischen Signaturen sinnvoll.

Aufgrund der Vorteile von Sticky Logs schlagen wir diese Technik als Lösung vor. Es existieren hierfür jedoch noch keine Implementierungen. Lediglich für Verschlüsselung und elektronische Signatur existieren bereits Standards.

4.5 Verfügbarkeit von Protokollen

Um die Erteilung von Auskunft durch die Rekonstruktion der Datenverarbeitung anhand der Protokolle zu ermöglichen, muss das Unternehmen diese Protokolle über einen bestimmten Zeitraum aufbewahren. Falls die Unternehmen einer VO ihre Protokolle selbst verwalten, kann es dazu kommen, dass nach dem Auflösen der VO die für eine Auskunftserteilung benötigten Informationen zum Zwecke der Auskunftserteilung nicht mehr verfügbar sind; die Rekonstruktion aller relevanten Datenverarbeitungsprozesse ist dann nicht mehr möglich.

Zur Lösung dieses Problems kann die Verwendung von Sticky Logs folgendermaßen beitragen: Da der Kunde die gewünschte Dienstleistung bei einem Unternehmen der VO beauftragt, so wird das Ergebnis der Dienstleistung dem Kunden auch von diesem Unternehmen mitgeteilt. Hierbei kann es die Protokolle in Form von Sticky Logs für die benötigte Zeitspanne vorhalten, um eine spätere umfassende Auskunftserteilung zu ermöglichen.

4.6 Standardisierte Auskunftserteilung

Die Auskunft, welche eine VO über die Verarbeitung und Existenz von personenbezogenen Daten erteilen muss, kann aus vielen Einzelinformationen der beteiligten Unternehmen bestehen. Um für den Kunden nachvollziehbar und verständlich zu sein, sollten die einzelnen Auskünfte zu einer Auskunft zusammengefasst werden. Dieses Zusammenfassen kann durch die Formalisierung und durch den Einsatz von Ontologien teilautomatisiert werden.

Diese hierfür notwendigen Formalismen zur Auskunftserteilung existieren zurzeit jedoch nicht und sind somit als Teil des integrierten Ansatzes zu entwickeln.

4.7 Auditfähigkeit

Für den Kunden ist es wünschenswert, die Einhaltung der Zusicherungen mit Hilfe der ihm auf Grund seines Auskunftersuchens mitgeteilten Informationen zu überprüfen. Wenn sowohl die Zusicherungen als auch die Auskunft auf Basis einer Ontologie formalisiert vorliegen, kann ein Abgleich auf Kundenseite zumindest teilautomatisiert vorgenommen werden.

Zur Umsetzung dieser Anforderungen existieren noch keine Ansätze. Insbesondere ist für einen Vergleich eine Formalisierung der erteilten Auskunft notwendig, welche ebenfalls noch nicht untersucht wurde. Daher beinhaltet der hier vorgeschlagene integrierte Ansatz eine Standardisierung für die Formalisierung der zu erteilenden Auskunft dergestalt, dass sie mit Zusicherungsformalismen kompatibel ist. So wird ein technisch unterstütztes Audit auf Basis eines Vergleichs von Zusicherungen mit erhaltener Auskunft ermöglicht.

Virtuelle Organisationen sind eine Form der Zusammenarbeit zwischen Unternehmen, deren Bedeutung und Einfluss in Zukunft noch wachsen werden. Als eine Bedingung für dieses Wachstum kann die Anwendung des Service-orientierten Architekturparadigmas auf Informationssysteme gesehen werden, welche zudem auf wohldefinierten Standards beruhen müssen, um die automatisierte Kommunikation zwischen den beteiligten Unternehmen zu erleichtern. Hierbei werden die Unternehmen jedoch mit Datenschutzproblemen konfrontiert, die durch den Einsatz einer SOA entstehen oder vergrößert werden.

In diesem Zusammenhang kommt der Beherrschbarkeit der Datenverarbeitung eine wichtige Bedeutung zu. Um den Begriff der Beherrschbarkeit zu operationalisieren, wurden die Mechanismen Unterrichtung, Auskunft, Zusicherungen und Protokollierung identifiziert. Bei der Untersuchung aktueller Umsetzungen dieser Mechanismen zeigten sich einige Schwächen in den existierenden Standards und ihrer Anwendung; das aus diesen Schwächen folgende Risiko einer rechtswidrigen Datenverarbeitung stellt einen Hemmschuh für den weiteren Nutzen von VO dar. Um diesem Problem zu begegnen, wurden mögliche Lösungsansätze vorgestellt.

Für die an VO beteiligten Unternehmen lohnt es sich, die im Zusammenhang mit dem Datenschutz aufgelisteten Probleme anzugehen und zu lösen: nicht nur wird ihnen die Gesetzeskonformität erleichtert, sondern es eröffnet ihnen die Möglichkeit, ihre Informationssysteme generell beherrschbarer zu machen. Schließlich können sie auch ihren Kunden mehr Kontrolle über ihre Daten zugestehen und sich somit einen Wettbewerbsvorteil verschaffen.

Danksagung

Wir danken Rüdiger Grimm und Steffen Staab von der Universität Koblenz sowie Sebastian Meissner, Martin Rost und Jan Schallaböck vom ULD für ihre Unterstützung und anregende Diskussionen. Dieser Artikel wurde im Rahmen der Untersuchung „Technikanalyse und Risk Management für Service-orientierte Organisationen in Virtuellen Organisationen“ vom BMBF gefördert.

Literatur

Fazit

- [1] Cranor, L., Langheinrich, M., Marchiori, M., A P3P Preference Exchange Language 1.0 (APPEL1.0), W3C, 2002.
- [2] Dierstein, R., Sicherheit in der Informationstechnik - der Begriff IT-Sicherheit, Informatik-Spektrum 4 2004, 343-353.
- [3] Gruber T. R.: A translation approach to portable ontologies. In: Knowledge Acquisition, Band 5, Nummer 2, 1993, 199-220.
- [4] Hallam-Baker, M., Behlendorf, B., Extended Log File Format, W3C, 1996.
- [5] Kagal, L., Finin, T., Joshi, A., 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', IEEE Computer Society, Washington, DC, USA, 2003, 63-74.
- [6] Moses, T (Hrsg.), XACML profile for Web Services, Working Draft 04, OASIS, 2003.
- [7] Oestereich, B., Objektorientierte Softwareentwicklung: Analyse und Design mit der UML 2.0, Oldenburg Verlag München Berlin, 2004.
- [8] Powers, C., Schunter, M., Enterprise Privacy Authorization Language (EPAL 1.2), W3C, 2003.
- [9] Ringelstein, C.; Schwagereit, F., Pähler, D., Opportunities and Risks for Privacy in Service-oriented Architectures, to appear at the 5th International Workshop for Technical, Economic and Legal Aspects of Business Models for Virtual Goods incorporating the 3rd International ODRL Workshop Oct 11 - 13 2007 in Koblenz, Germany.
- [10] Safe Harbor Privacy Principles, Issued by the U.S. Department of Commerce on July 21, 2000.
- [11] Weichert, T., Auskunftsanspruch in verteilten Systemen, DuD: Datenschutz und Datensicherheit 30 2006, 694-699.
- [12] Wenning, R., Schunter, M., The Platform for Privacy Preferences 1.1 (P3P1.1) Specification, W3C, 2006.