Datenschutz im Data Warehousing

Verfasser: Martin Hafner

Lehrstuhl: Prof. Dr. Robert Winter
Bericht Nr.: BE HSG/CC DW2/04
Datum: 2002-11-06

Universität St. Gallen –
Hochschule für Wirtschafts-, Rechts- und Sozialwissenschaften (HSG)

Institut für Wirtschaftsinformatik
Müller-Friedberg-Strasse 8
CH-9000 St. Gallen
Tel.: + 41 71 224-2420
Fax: + 41 71 224-2189

Prof. Dr. A. Back
Prof. Dr. W. Brenner
Prof. Dr. H. Österle
Prof. Dr. R. Winter

Inhaltsverzeichnis

Abbildungsverzeichnis

Tabellenverzeichnis

Abkürzungsverzeichnis

BDSG	Bundesdatenschutzgesetz
BSI	Bundesamt für Sicherheit in der Informationstechnik
CC DW2	Kompetenzzentrum Data Warehousing 2
CRM	Customer Relationship Management
DSG	Bundesgesetz über den Datenschutz
E-P3P	Enterprise Platform for Privacy Preferences
EPA	Enterprise Privacy Architecture
ERM	Employee Relationship Management
ETL	Extraction, Transformation, Load
EU-DSRL	Datenschutzrichtlinie der Europäischen Union
OLAP	Online Analytical Processing
P3P	Platform for Privacy Preferences
VDSG	Verordnung zum Bundesgesetz über den Datenschutz
W3C	World Wide Web Consortium
XML	Extended Markup Language

1 Einleitung

1.1 Motivation

Innerhalb eines sozialen Systems nimmt der Mensch verschiedene Rollen ein. Beispielsweise steht er als Bürger dem Staat, als Kunde Anbietern von Waren und Dienstleistungen, als Mitarbeiter seinem Arbeitgeber oder als Mitglied einer Organisation Menschen mit in Teilbereichen ähnlich gelagerten Lebensinteressen gegenüber. Alle diese Rollen im Zusammenleben von Menschen erfordern einen mehr oder weniger umfassenden Austausch von Wirtschaftsgütern.

Im heutigen Beziehungsgeflecht des Menschen gewinnt das immaterielle Wirtschaftsgut der Information zunehmend an Bedeutung. Zahlreiche Aktivitäten hinterlassen mehr oder weniger grosse Datenspuren, sei es bei der Benutzung von mautpflichtigen Strassen, deren Abrechnung elektronisch erfolgt, oder beim bargeldlosen Bezahlen, beim Telefonieren oder beim Wohnortwechsel, bei der Erfassung von Arbeitszeiten oder bei der Nutzung des Internets [Forum Recht Redaktion 2001].

Neben freiwillig oder zumindest potenziell bewusst hinterlassenen Datenspuren, die der Mensch für Interessierte zur Sammlung und Verwertung bereitstellt, werden Informationen von staatlichen und privaten Stellen auch aktiv gesammelt. Werkzeuge sind hier beispielsweise Kameraüberwachung und Internet-„Cookies“. Auch Mobiltelefone, die vielfach zu ständigen Begleitern des Menschen avanciert sind, haben für Daten sammelnde Stellen gegenüber konventionellen Telefonen den Vorteil, dass sie nicht nur das Abhören erlauben, sondern auch Informationen darüber liefern, wo sich der Benutzer aufhält [Forum Recht Redaktion 2001].

In der Tat ist das Potenzial von Überwachungsmechanismen nicht zu unterschätzen: „Als Horst Herold, Polizeipräsident von Nürnberg, 1967 die ersten Kameras der Bundesrepublik zur Überwachung öffentlicher Plätze installieren liess, waren die technischen Möglichkeiten noch unausgereift. Die Erhebung und Auswertung der Bilder war aufwendig und störungsanfällig. Trotzdem sank die Kriminalitätsrate in den folgenden zwei Jahren auf den Plätzen, die im Blickfeld des „Bildfunks“ lagen, um 26 Prozent. […] Schätzungen sprechen heute von 100.000 Kameras, die von privater, kommunaler oder polizeilicher Seite in Deutschland ihren Dienst tun. Die Kameras in Kaufhäusern, Banken, Bahnhöfen und zuweilen an Arbeitsplätzen ergeben ein für die Bürgerinnen und Bürger nicht durchschaubares engmaschiges Überwachungsnetz. In manchen städtischen Zentren kann man daher durchaus von einer flächendeckenden Überwachung sprechen.“ [Schiek 2001].

Der flächendeckende Einsatz beispielsweise von Überwachungskameras stellt für den Schutz der Privatsphäre des Einzelnen noch nicht die zentrale Bedrohung dar. Verfolgt man jedoch die Aussagen SCHIEKS weiter, so gelangt man zu der Erkenntnis, dass die Zusammenführung

von Daten beispielsweise aus dem Bereich der Überwachung einen wesentlichen kritischen Punkt hinsichtlich des Schutzes der Privatsphäre darstellt:

„Durch die Vielzahl unterschiedlicher – privater und öffentlicher – BetreiberInnen ist der Kameraeinsatz insgesamt nicht systematischer Natur, sondern verfolgt eher jeweils bestimmte strategische Ziele der BesitzerInnen. Diese Ziele haben entweder öffentlichen Charakter – z. B. die Beobachtung sogenannter Kriminalitätsschwerpunkte zur Gefahrenabwehr, oder privaten – z. B. den Schutz eines Gebäudes. Ein Austausch findet dabei nicht statt. Erst dort, wo private Sicherheitsunternehmen Videoüberwachung betreiben, kommt es zu einer Schnittstelle zwischen privater und öffentlicher Videoüberwachung, da diese Unternehmen ihr Material oft – und gerne – an Sicherheitsbehörden weiterreichen.“ [Schiek 2001].

Wie sich die Nutzung integrierter Daten darstellt, zeigt ein Beispiel der US-amerikanischen Polizei, die bei einem Football-Spiel in Tampa die Gesichter aller 75.000 Zuschauer, die sich im Stadion befanden, von 20 Kameras scannen liess. Die Bilder wurden von angeschlossenen Computern digitalisiert und mit einer Datenbank abgeglichen, in der mehrere Tausend digitale Fotos aus Polizei- und Gerichtsakten abgespeichert waren, angefangen von einfachen Delikten bis hin zu terroristischen Attentaten. Insgesamt wurde die Polizei durch die Massnahme auf 19 Personen aufmerksam, die per Haftbefehl gesucht waren. Zwar wurde in diesem Fall nur ein Abgleich zwischen Datenbanken mit straffällig gewordenen Menschen und den Besuchern des Footballspiels vorgenommen, jedoch wäre es problemlos möglich gewesen, die erhobenen Daten aller Besucher zu speichern, um sie bei anderen Gelegenheiten für weitere Abgleiche zu nutzen. Übertragen auf weitere Anwendungsfälle bedeutet dies, dass Autokennzeichen – wie im Londoner Bankenviertel bereits praktiziert – ebenfalls automatisiert erkannt werden können und auf diese Weise Bewegungsbilder einzelner Personen oder automatisch erstellte Verzeichnisse der Personen, die einen bestimmten Ort besucht haben, technisch problemlos realisierbar sind, wenn sie mit entsprechenden Daten abgeglichen werden können, notfalls mit der Personalausweisdatei [Schiek 2001].

Data Warehousing als Technologie zur Integration von Daten spielt im Kontext der genannten Szenarien eine besondere Rolle. Losgelöst von den einzelnen operativen Datenbeständen beispielsweise in einem Unternehmen werden Daten integriert und langfristig historisiert im Data Warehouse vorgehalten. Aus der Analyse dieser Daten können fundiert Massnahmen zur Steuerung eines Unternehmens oder seiner einzelnen Geschäftsbereiche abgeleitet werden [Jung/Winter 2000, S. 7]. Darüber hinaus können neue Geschäftsmodelle gestaltet werden [Jung/Winter 2000, S. 7], wozu insbesondere das Management von Kunden- und Mitarbeiterbeziehungen zu rechnen ist. Durch die detaillierte Kenntnis des Kunden bzw. Mitarbeiters können im Laufe der Zeit umfassende Persönlichkeitsprofile erzeugt werden, die für das Marketing, den Vertrieb und den Kundenservice bzw. die Planung und Steuerung des Produktionsfaktors „Arbeit“ von besonderem Interesse sind.

Die Folgen der Verarbeitung personenbezogener Daten unabhängig vom Integrationsgrad, mit dem Daten jedoch im Regelfall zunehmend sensibler werden, lassen sich wiederum anhand von Beispielen aus dem Bereich der Privatwirtschaft illustrieren:

Überwachungsdaten, die die Deutsche Bahn im Zuge der 24-Stunden-Überwachung auf ihren Bahnhöfen erhebt, stehen beispielsweise auch Sozialämtern und der Polizei zur Verfügung [Arbeitskreis gegen Überwachung 2002]. Die Folgen werden anhand des Beispiels deutlich, nach dem in Innenstädten die Überwachung des öffentlichen Raums alltäglich wird. „Unternehmer und Kaufleute „säubern" mit Hilfe der Polizei […] „ihre" City von Menschen, die wohl schädlich für den Konsumwillen der KundInnen sein könnten. […] Denn wer kann sich schon hemmungslos dem Konsum widmen, wenn vor dem Kaufhaus die Armut bettelt? Diese Leute werden dann einfach in Randbezirke verfrachtet. Doch dies führt zwangsläufig zur Ghettobildung. Leute, die […] nicht der Norm entsprechen, werden einfach abgeschoben. Doch mit solchen Massnahmen erreicht man keine soziale Ruhe, im Gegenteil: Unruhen verschärfen sich, die Kluft zwischen arm und reich wird immer grösser. Es entstehen privilegierte Menschen und solche die unerwünscht sind. Die Unerwünschten werden vertrieben." [Arbeitskreis gegen Überwachung 2002].

Diese und weitere wirtschaftliche und soziale Konsequenzen sind nur ein Teilbereich dessen, was aus leichtfertigem Umgang mit personenbezogenen Daten erwachsen kann. So zeigt ein Beitrag von HÖLLER [Höller 2002] aus dem Bereich der Mitarbeiterdatenverarbeitung, dass sich die Aufgabe der Privatsphäre am Arbeitsplatz durchaus nachteilig auf die Leistungsfähigkeit des Mitarbeiters auswirken kann. Eine Untersuchung der New Yorker Syracuse University an 130 Freiwilligen, deren Arbeit ständig kontrolliert wurde, ergab, dass je stärker die Überwachung des Mitarbeiters betrieben wird, desto weniger dieser von sich aus arbeitet. Er leistet bald nur noch „Dienst nach Vorschrift" und zeigt keinerlei Verantwortung für das Ergebnis seiner Arbeit.

Als Versuch der staatlichen Gegenlenkung zur uneingeschränkten Erhebung, Verarbeitung und Nutzung personenbezogener Daten durch öffentliche und private Datenverarbeiter existieren zahlreiche Gesetze und Richtlinien zum Datenschutz. Diese fokussieren in erster Linie den Schutz des Grundrechts des Einzelnen auf informationelle Selbstbestimmung, wie sie vom Bundesverfassungsgericht in der Bundesrepublik Deutschland 1983 identifiziert wurde [Bundesverfassungsgericht 1983]. Insbesondere besteht der Schutz dieses Grundrechts in einem hohen Mass an gesetzlichen Restriktionen wie der Zweckbindung und Einwilligung des Betroffenen bei der Verarbeitung personenbezogener Daten [BDSG 2002, §§ 3; 4a]. Damit in Verbindung steht, dass die personenbezogenen Daten auch nach der Bekanntgabe an eine Daten verarbeitende Stelle Eigentum des Betroffenen bleiben, so dass dessen Anspruch auf individuellen Schutz seiner Daten nicht unberechtigt ist.

1.2 Problemstellung und Zielsetzung

Im Fokus des vorliegenden Arbeitsberichts stehen Unternehmen, die über ein Data Warehouse verfügen und dieses bei der Verarbeitung personenbezogener Daten einsetzen.

Diese fallen nach QUADRI im Rahmen der vielfältigen Beziehungen eines Unternehmens v. a. im Zusammenhang mit Mitarbeitern und Geschäftspartnern an. Während es sich bei den Daten der Mitarbeiter hauptsächlich um Fähigkeiten und Erfahrungswerte handelt, die dem Unternehmen zur Verfügung stehen, muss im Bereich der Geschäftspartner eine weitere Trennung in Daten über Kunden und Zulieferer vorgenommen werden [Quadri 2001]. Da es sich bei Zulieferern in der Hauptsache nicht unmittelbar um natürliche Personen handelt, die der Datenschutz ausschliesslich fokussiert [BDSG 2001, §§ 1; 3], befasst sich der vorliegende Arbeitsbericht mit dem Umgang von Kunden- und Mitarbeiterdaten im Data Warehousing durch Unternehmen.

Bei der Integration von Kunden- bzw. Mitarbeiterdaten in einem Data Warehouse entstehen Persönlichkeitsprofile, die eine hohe Bandbreite an Merkmalen über den Betroffenen abbilden. Zum einen sind auf diese Weise im Hinblick auf Kundenprofile z. B. neue Geschäftsfelder für Unternehmen erschliessbar [Jung/Winter 2000, S. 7]. Hinsichtlich der Mitarbeiterprofile lassen sich z. B. umfassende Analysen zur Verbesserung der organisatorischen Gegebenheiten eines Unternehmens durchführen (siehe Abschnitt 2.2.2). Zum anderen profitieren sowohl Kunden als auch Mitarbeiter von der Vorhaltung von Persönlichkeitsprofilen, sei es z. B. im Fall von Kunden für deren individuelle Betreuung oder im Fall von Mitarbeitern für deren adäquate Beschäftigung und Entlohnung durch den Arbeitgeber (siehe Abschnitte 2.1.1 und 2.2.1).

Im Gegensatz hierzu sehen Richtlinien zum Datenschutz den uneingeschränkten Schutz personenbezogener Daten vor. Die Nachteile, die Kunden, Mitarbeitern, aber auch Unternehmen aus der Missachtung der Privatsphäre – u. a. auch im Zuge des Data Warehousings – erwachsen können, wurden in Abschnitt 1.1 skizziert und unterstreichen das berechtigte Anliegen des Datenschutzes unabhängig von seiner rechtlichen Verbindlichkeit .

Formaljuristisch betriebener Datenschutz und uneingeschränktes Data Warehousing mit personenbezogenen Daten stehen sich somit hinsichtlich ihrer Zielsetzungen offenkundig entgegen. Innerhalb dieses Spannungsfelds sind die persönlichen Interessen des einzelnen Kunden bzw. einzelnen Mitarbeiters insbesondere nach Schutz seiner Privatsphäre gelagert. Zudem sind auch Unternehmen sind daran interessiert, dass ihre Reputation nicht durch die Aufmerksamkeit der Öffentlichkeit im Zuge eines Datenschutzvorfalls beeinträchtigt wird (siehe Kapitel 2).

Zielsetzung des vorliegenden Arbeitsberichts soll es somit sein, Unternehmen mit einem Data Warehouse, in dem Kunden- bzw. Mitarbeiterdaten verarbeitet werden, Hinweise zu geben, wo ein Mittelweg zwischen uneingeschränktem Data Warehousing und formaljuristisch be-

triebenem Datenschutz verlaufen kann. Dieser soll mit Blick auf die Konstanten „Data Warehousing“ und „Datenschutz“ um Ausgleich zwischen den Interessen von Unternehmen und ihren Kunden bzw. Angestellten bemüht sein.

Die Informationen in diesem Arbeitsbericht geben einen Überblick über die Situation des Datenschutzes aus Sicht der Wirtschaftsinformatik. Der Arbeitsbericht erhebt keinen Anspruch auf Vollständigkeit hinsichtlich der Rechtslage und kann deshalb nicht als ein rechtlich verbindliches Dokument betrachtet werden. Die letztendliche Abklärung datenschutzrechtlicher Fragestellungen muss im Einzelfall durch Rechtsexperten erfolgen.

1.3 Aufbau der Arbeit

Zunächst werden die datenschutzrelevanten Interessen von Unternehmen sowie ihren Kunden und Arbeitnehmern analysiert und einander gegenüber gestellt (Kapitel 2). Im Anschluss daran werden in Kapitel 3 die Grundbegriffe bei der Verarbeitung personenbezogener Daten im Schweizerischen und deutschen Datenschutzgesetz (DSG und BDSG) dargestellt, wobei die Aussagen zur Rechtslage in der Bundesrepublik Deutschland in enger Beziehung zur Datenschutzrichtlinie der Europäischen Union (EU-DSRL) stehen. Das Kapitel schliesst mit der Beschreibung der Grundprinzipien des Datenschutzes.

Darauf aufbauend soll untersucht werden, an welchen Stellen des Data Warehousings konkret Gefährdungen für den Kunden- bzw. Mitarbeiterdatenschutz auftreten (Abschnitt 4.1). Anschliessend erfolgt eine Betrachtung, welche Massnahmen an den einzelnen Stellen wirksam sein können, um den Gefährdungen gezielt zu begegnen. Dabei werden zunächst die formaljuristischen Gegebenheiten (Abschnitt 4.2) des Kunden- und Mitarbeiterdatenschutzes, im zweiten Schritt aber auch das individuelle Kundenbedürfnis (Abschnitt 4.3) in den Mittelpunkt der Untersuchungen gestellt. Von einer Orientierung an Mitarbeiterbedürfnissen wird aufgrund der expliziten gesetzlichen Regelungen im Bereich des Mitarbeiterdatenschutzes abgesehen. Abschliessend wird eine Zusammenfassung mit Fazit und Ausblick gegeben (Kapitel 5).

2 Personenbezogene Daten im Unternehmen

2.1 Kunden und Unternehmen

Nach SCHMID, BACH und ÖSTERLE lassen sich im Kontakt zwischen Unternehmen und ihren Kunden drei Phasen identifizieren. Dabei handelt es sich um das Marketing, den Verkauf und den Kundenservice [Schmid/Bach/Österle 2000, S. 24-26].

In der Marketingphase verfolgt das Unternehmen das Ziel, potenzielle Kunden zu identifizieren und anzusprechen. Dies setzt voraus, dass sowohl auf bekannte Bedürfnisse des Kunden eingegangen wird als auch darüber hinausgehende Bedürfnisse geweckt werden. Zielsetzung der Marketingphase ist die Identifikation von Interessenten, die in der Verkaufsphase angesprochen werden. Gelingt es dem Unternehmen in der Verkaufsphase, von einem Interessenten einen Auftrag zu erhalten, kommt ein Vertrag zustande. Insbesondere im Rahmen dieses Vertragsverhältnisses, aber bereits auch in den vorgelagerten Phasen, werden zahlreiche Informationen zwischen den Geschäftspartnern ausgetauscht.

Für den Informationsfluss vom Kunden – als einer Privatperson – zum Unternehmen ist charakteristisch, dass es sich grösstenteils um personenbezogene Informationen handelt, d. h. Informationen, die einer natürlichen Person zugeordnet werden können. Die Gründe des Unternehmens für die Erhebung personenbezogener Daten können in zwei Kategorien unterteilt werden [Dittrich/Vavouras 2001, S. 116]:

Zum einen dient sie der Erfüllung vorvertraglicher und vertraglicher Leistungen. Zum anderen werden Daten erfasst, um dem Unternehmen für spätere Analysezwecke bzw. für gezielte Massnahmen der Marktbearbeitung und Kundenbetreuung zur Verfügung zu stehen. Beide Gründe für die Erhebung personenbezogener Daten durch Unternehmen legen nahe, dass dies sowohl im Interesse der Kunden als auch der Unternehmen geschieht.

Nationale und internationale Bestimmungen zum Datenschutz sehen indessen eine strikte Regulierung des Umgangs mit personenbezogenen und insbesondere sensiblen personenbezogenen Daten vor. Zwar sind sie als Mittel zu betrachten, das Interesse des Kunden am Schutz seiner Privatsphäre abzubilden, jedoch stehen sie nicht in uneingeschränktem Einklang mit den wirtschaftlichen Interessen von Kunden und Unternehmen [Rossnagel/Pfitzmann/Garstka 2001, S. 90 ff.].

Im weiteren Verlauf des Kapitels sollen zunächst die Interessen des Kunden und anschliessend die der Unternehmen skizziert werden. Dabei werden jeweils sowohl wirtschaftliche Interessen von Kunden und Unternehmen dargestellt, als auch das Interesse des Kunden am Schutz seiner Privatsphäre sowie das Interesse des Unternehmens an der Konformität mit der Datenschutzgesetzgebung und einer das Vertrauen des Kunden gewinnenden Aussenwirkung.

2.1.1 Interessen des Kunden

Wirtschaftliche Interessen

Im Zeitalter zunehmend transparenter und gesättigter Märkte richtet der Kunde sein Augenmerk insbesondere auf die individuelle Erfüllung seiner Bedürfnisse. Charakteristisch hierfür ist, dass der Anspruch des Kunden von einer gezielten und zugleich ganzheitlichen Kontaktsuche durch die Unternehmen ausgeht [Gentsch 2001, S. 80; Österle 2000, S. 26]. Im Rahmen von Mailingaktionen durch ein Unternehmen würde dies bedeuten, dass der Kunde ausschliesslich solche Mailings erhalten möchte, die für ihn relevant sind, zugleich aber alle seine Bedürfnisse abdecken.

Die ganzheitliche Abdeckung von Kundenbedürfnissen umfasst insbesondere die Bereitstellung sogenannter Value-added-Services, durch die dem Kunden im Rahmen der Wettbewerbsprofilierung des Unternehmens ausser dem Kernprodukt bzw. der Kerndienstleistung massgeschneiderte flankierende Dienstleistungen angeboten werden [Meffert/Bruhn 2000, S. 17]. Beispiele für erhöhten Servicegrad und persönliche Betreuung können Finanzierungsangebote im Zusammenhang mit dem Kauf eines Neuwagens oder eine um einen Skikurs angereicherte Hotelbuchung sein [Meffert/Bruhn 2000, S. 291].

Die Entwicklung in Richtung des Mobile Commerce weckt zudem den Anspruch des Kunden, immaterielle Leistungen nach Möglichkeit über die verschiedensten Kanäle unabhängig von Ort und Zeit, jedoch gemäss seinen Präferenzen zu erhalten. Als Beispiel hierfür können die von hoher Informationsintensität geprägten Dienstleistungen im Finanzdienstleistungssektor genannt werden [Winter 2002, S. 270].

Dem Interesse an einer kanalspezifischen, individuellen Ansprache kommen somit Geschäftsmodelle wie das des Online-Buchhändlers „Amazon“ [Amazon 2002] entgegen, wo mittels Analyse des Kundenverhaltens auf der Website und der Verwendung von Cookies das Angebot entsprechend den bisherigen Interessen des Besuchers aufbereitet wird.

Interesse am Schutz der Privatshäre

Neben ihren wirtschaftlichen Interessen haben viele Kunden auch das Bedürfnis nach dem Schutz ihrer Privatsphäre [Hoess/Kloss/Sweat 2001]. Nach Bekanntgabe personenbezogener Daten an öffentliche oder privatwirtschaftliche Stellen haben sie jedoch keinen unmittelbaren Einfluss mehr auf deren Verbleib und Verwendung. Das Recht auf informationelle Selbstbestimmung ist nach seiner Identifikation durch das Bundesverfassungsgericht der Bundesrepublik Deutschland 1983 [Bundesverfassungsgericht 1983] ins Bewusstsein gerückt und in vielen europäischen Staaten [Büllesbach 2002a] gesetzlich verankert worden.

Auch fehlerhafte Daten und Fehlinterpretationen bis hin zur missbräuchlichen Verwendung personenbezogener Daten haben immer wieder gravierende Folgen für den einzelnen. Die denkbaren Beispiele sind vielfältig und auf die Geschäftsbeziehungen zwischen Unternehmen

und ihren Kunden übertragbar: Mit Hilfe elektronischer Zahlungssysteme in Kantinen kann auf die Ernährungsgewohnheiten von Mitarbeitern geschlossen werden, was zu einem Kriterium für die weitere Beförderung werden kann. Ebenso rufen fehlerhafte Auskünfte von Kreditauskunfteien von Zeit zu Zeit Datenschutzskandale hervor [HSID 2000], in deren Folge selbst für mittelständische Unternehmen der Konkurs nicht ausgeschlossen werden kann.

Gegenüber einem grossen Unternehmen mit umfassenden organisatorischen Strukturen sowohl auf wirtschaftlichem als auch juristischem Sektor ist der gesetzliche Schutz des „schwächeren" Geschäftspartners durch Gesetze zum Schutz seiner informationellen Selbstbestimmung sinnvoll. V. a. besonders schützenswerte personenbezogene Informationen zu politischen, gewerkschaftlichen und religiösen Weltanschauungen oder über die wirtschaftlichen, ethnischen, strafrechtlichen, sozialen und gesundheitlichen Verhältnisse sowie die Intimsphäre [Schweizer 1999, S. 143 f.] können grosse Schäden für den Einzelnen hervorrufen, wenn mit ihnen unsachgemäss umgegangen wird [Botschaft DSG 1988].

Durch die Ansammlung und Integration von personenbezogenen Daten, die für sich genommen nicht sensibel sein müssen, entstehen vielfach hochsensible Persönlichkeitsprofile. So ist es möglich, dass Telekommunikationsanbieter mittels an sich wertneutraler Informationen wie der Information über Beginn, Ende und Dauer von Verbindungen, der Art der Verbindung (eingehender oder abgehender Anruf) und Kommunikation (Telefon, Fax etc.), Standort- und Interessensprofile erstellen können, die in den sensiblen Bereich personenbezogener Daten gehören [Schweizer 2001, S. 110].

2.1.2 Interessen des Unternehmens

Wirtschaftliche Interessen

Da Unternehmen zunehmend den Kundenprozess in den Mittelpunkt ihres Handelns stellen, decken sich ihre wirtschaftlichen Interessen vielfach mit denen der Kundschaft [Österle 2000, S. 28]. Die Unternehmen sehen sich einem zunehmenden Konkurrenzdruck sowie gut informierten Kunden gegenüber [Heinrich 2002, S. 50]. Der hohe Konkurrenzdruck ist auf eine gewisse Marktsättigung zurückzuführen, die dazu führt, dass der Kunde sich nach Angeboten umschaut, die seinen Bedürfnissen, insbesondere im Hinblick auf seine nachhaltige Betreuung und den Kundenservice, am ehesten entsprechen.

Die damit verbundene Abkehr von der Produktorientierung zur Kundenorientierung sowie die Erkenntnis, dass die Gewinnung neuer Kunden mit wesentlich höheren Kosten verbunden ist als die Sicherung des Fortbestands existierender Kundenbeziehungen (Langfristige Kundenbindung), legen nahe, dass Unternehmen auf umfassende Kundeninformationen (Kundenprofile) angewiesen sind, um ihr Leistungsangebot speziell an bestimmten Kundengruppen oder gar einzelnen Kunden zu orientieren [Österle 2000, S. 33] und somit den Kunden längerfristig zu binden. Dabei sind Kundeninformationen von umso höherem Wert für das Unternehmen,

je besser sie integriert sind und dementsprechend eine globalere Gesamtsicht auf den Kunden ermöglichen.

Dieses Vorgehen setzt beachtliche Potenziale im Hinblick auf Cross- und Upselling frei, d. h. bestehende Kunden können gezielt mit zusätzlichen und höherwertigen Produkten in Kontakt gebracht werden. Zudem lassen sich wenig profitable Kunden frühzeitig identifizieren, so dass ihre Profitabilität durch entsprechende Anreizsysteme bzw. Kundenbindungsprogramme verbessert werden kann [Winter 2002, S. 274 ff.]. Kundenbindungsprogramme wie das deutsche Payback-System oder die Schweizer Migros-Cumulus-Karte, mit deren Hilfe systematisch Einkaufsdaten von Kunden erfasst werden, haben z. B. mehrfachen Nutzen für die Unternehmen. Zum einen wird der Kunde an bestimmte Unternehmen gebunden, da er nur dort von Rabatten profitiert. Zum anderen liefern die Programme den Unternehmen weitere umfassende Kundenprofildaten, die beispielsweise für die Zuordnung von Kunden zu Kundensegmenten oder für Prognosen über künftiges Kaufverhalten genutzt werden können. Erfahrungen mit der Segmentierung von Kunden existieren bereits im Finanzdienstleistungssektor, wo auf diese Weise z. B. die künftige Rentabilität von Kunden optimiert werden kann [Bach/Gronover/Schmid 2000, S. 133].

Schliesslich liegt es im Interesse von Unternehmen, Kundendaten nach eigenem Ermessen sowohl mit Geschäftspartnern als auch innerhalb eines Konzerns zwischen rechtlich selbständigen Tochterunternehmen auszutauschen, was der Freisetzung von Cross- und Upselling-Potenzialen zusätzlich entgegenkommt.

Interesse an der Konformität mit der Datenschutzgesetzgebung und einer das Vertrauen des Kunden gewinnenden Aussenwirkung

Die fundierte Ermittlung der Rentabilität eines Kunden bzw. seiner Bedürfnisse ist nur aufgrund eines umfassenden Wissens über ihn möglich. Hinterlegt ist dieses Wissen in Form personenbezogener Daten, die im Zuge der Vertragsabwicklung oder von Marktforschungsaktivitäten erhoben werden.

An diesem Punkt stellt sich dem Unternehmen jedoch die Frage der datenschutzrechtlichen Zulässigkeit angesichts der Tatsache, dass die Verwendung personenbezogener Daten zu Auswertungszwecken über den eigentlichen Vertragszweck der Auftragserfüllung hinausgeht. Für Unternehmen ist es vorteilhaft, einmal erhobene personenbezogene Daten unbefristet für verschiedenste Zwecke einzusetzen, was vielfach jedoch den Interessen des Kunden entgegensteht, Misstrauen hervorruft und zu einem schlechten Erscheinungsbild des Unternehmens führen kann [Swift 2001, S. 227 f.].

Dem möchten Unternehmen entgegentreten, indem die datenschutzrechtlichen Bestimmungen gegenüber dem Kunden offenkundig praktiziert, Datenschutzbeauftragte bestellt und vereinzelt Massnahmen zur Verbesserung des Datenschutzniveaus im Unternehmen umgesetzt werden. Die zweite Zielsetzung, die solche Massnahmen neben dem Vertrauensgewinn gegen-

über dem Kunden haben, ist die notwendige Erfüllung datenschutzrechtlicher Bestimmungen, da sich offengelegte Verstösse durchweg nachteilig auf das Ansehen des Unternehmens auswirken und zudem mit – wenn auch geringen – Strafen belegt sind (siehe hierzu Abschnitt 3.5).

2.1.3 Gegenüberstellung der Interessen

Die Aussagen der Abschnitte 2.1.1 und 2.1.2 lassen sich zusammenfassend in einer Matrix der Chancen und Risken der umfassenden Verarbeitung von Kundendaten darstellen (Tab. 2-1).

	Chancen	**Risiken**
Unternehmen	• Erstellung von Kundenprofilen • Cross-/Up-Selling-Potenziale • Langfristige Kundenbindung • Kundensegmentierung • Prognosen	• Negatives Erscheinungsbild • Rechtsunsicherheit
Kunden	• Kanalspezifische, individuelle Ansprache • Spezielle Angebote • Erhöhter Servicegrad • Persönliche Betreuung	• Fehlerhafte Daten • Fehlinterpretation von Daten • Missbräuchliche Verwendung von Persönlichkeitsmustern • Eingriff in Privatsphäre • Missachtung d. informationellen Selbstbestimmung

Tab. 2-1: Chancen und Risiken der umfassenden Verarbeitung von Kundendaten durch Unternehmen

Die wirtschaftlichen Interessen von Kunden und Unternehmen verfolgen angesichts zunehmender Kundenorientierung sehr ähnliche Zielsetzungen. Anders verhält es sich bei den nicht wirtschaftlichen Interessen, d. h. dem Bedürfnis des Kunden nach informationeller Selbstbestimmung gegenüber der Bestrebung des Unternehmens, möglichst umfassend über personenbezogene Daten zu verfügen und diese zu nutzen, was dem Recht auf Privatsphäre entgegensteht.

Dieser Interessenkonflikt lässt sich kaum auflösen, indem Unternehmen strikt datenschutzrechtliche Bestimmungen umsetzen, da dies sowohl ihren wirtschaftlichen Interessen als auch

denen der Kunden entgegensteht. Vielmehr ist zu erwarten, dass der Kunde zumindest im Bereich des Online-Geschäfts zu Massnahmen des Selbstschutzes greift. Ein Indikator hierfür ist die Tatsache, dass 45% der Nutzer des World Wide Web in der Bundesrepublik Deutschland wegen datenschutzrechtlicher Bedenken auf den Kauf von Waren oder Dienstleistungen über dieses Medium verzichten [Hoess/Kloss/Sweat 2001]. Andere Formen des Selbstschutzes sind die Eingabe falscher Daten z. B. in Adressfeldern oder der Einsatz von Anonymisierungswerkzeugen, wie sie beispielsweise von der Firma Anonymizer [Anonymizer 2002] angeboten werden.

Die adäquate langfristige Reaktion von Unternehmen könnte darin bestehen, die Bedürfnisse ihrer Kunden im Hinblick auf deren Privatsphäre zu berücksichtigen sowie ihre Analyse- und Marketingaktivitäten entsprechend zu gestalten.

2.2 Unternehmen und ihre Mitarbeiter

Als einer der drei Produktionsfaktoren „Boden, Kapital und Arbeit“ nach Adam Smith steht der Mitarbeiter[1] im Vergleich zum Kunden in einem besonderen Verhältnis zum Unternehmen: Während der Mitarbeiter eine sogenannte Treueverpflichtung gegenüber dem Arbeitgeber eingeht [OR 2002, Art. 321a], besteht eine allgemeine Fürsorgepflicht des Arbeitgebers gegenüber dem Arbeitnehmer [OR 2002, Art. 328].

Neben den um Ausgleich zwischen Arbeitgeber und Arbeitnehmer bemühten gegenseitigen Pflichten stehen sich jedoch das auch im Arbeitsverhältnis zumindest mittelbar anzuwendende Grundrecht des Arbeitnehmers auf informationelle Selbstbestimmung [Bundesverfassungsgericht 1983] und andere vom BUNDESMINISTERIUM FÜR ARBEIT UND SOZIALORDNUNG nicht näher spezifizierte Grundrechte gegenüber [BMA 2000, S. 125].

Aus diesem Grund ist es notwendig, für die zahlreichen Persönlichkeitsprofile und sensiblen personenbezogenen Daten, wie sie in einem Unternehmen bedingt durch das oftmals langfristige Engagement von Mitarbeitern sowie gesetzliche Vorschriften anfallen, Regelungen zu implementieren, die einem Interessenausgleich förderlich sind. Zu beachten ist dabei, dass ähnlich wie bei der Beziehung zwischen Kunden und Unternehmen das Interesse der Arbeitsnehmer am Schutz ihrer personenbezogenen Daten keineswegs als homogen betrachtet werden kann, was in Abschnitt 2.2.1 näher ausgeführt wird. Hinzu kommt, dass der Vertragsgegenstand zwischen Arbeitgeber und Arbeitnehmer sehr vielfältig ist (Anforderungen an und Bezahlung von Hilfsarbeitern vs. Abteilungsleiter) und Leistungsbeurteilungen, d. h. der Grad der Vertragserfüllung, meist nur auf der Basis umfassender personenbezogener Merkmale zur Leistungserfassung durchgeführt werden können.

---

[1] Der Begriff Mitarbeiter bzw. Arbeitnehmer schliesst im Folgenden – wenn nicht ausdrücklich anders erwähnt – stets Bewerber eines Unternehmens, die sich in einem vorvertraglichen Status befinden, mit ein.

Im Folgenden werden die Interessen des Arbeitgebers und des Arbeitnehmers im Hinblick auf ihre wirtschaftlichen Ziele sowie ihr Interesse an einer Datenschutzkonformität geschildert und einander gegenübergestellt.

2.2.1 Interessen der Arbeitnehmer

Wirtschaftliche Interessen

Unter den wirtschaftlichen Interessen der Mitarbeiter werden im Folgenden jene ökonomischen Privatinteressen der Arbeitnehmer verstanden, die sowohl auf Angestellte anwendbar sind, deren Arbeitsalltag vornehmlich von klar strukturierten und standardisierten Tätigkeiten geprägt ist, als auch auf diejenigen, die in hohem Mass Verantwortung für die wirtschaftlichen Geschicke des Unternehmens tragen. Von Interessen, die über die gemeinsamen hinausgehen, soll im Folgenden abstrahiert werden (z. B. dominantes Interesse an der Einhaltung tariflicher Vereinbarungen auf Seiten von Arbeitern ohne ausgedehnte Sach- bzw. Personalverantwortung vs. Interesse an einer systematischen Karriereplanung für leitende Angestellte).

Somit soll insbesondere davon ausgegangen werden, dass der Arbeitnehmer seine Fähigkeiten dem Unternehmen zur Verfügung stellt, um auf diese Weise für seine persönliche finanzielle und soziale Sicherheit sowie gesellschaftliches Ansehen zu sorgen. Dies impliziert, dass der Mitarbeiter an der leistungsgerechten Bezahlung seiner Tätigkeit interessiert ist, wofür er in gewissem Masse auch zur Leistungserfassung und -beurteilung durch den Arbeitgeber bereit ist, die beispielsweise über die reine Zeiterfassung und entsprechende Lohnabrechnung hinausgeht. Nicht zuletzt könnte sich der Mitarbeiter davon die Anerkennung durch den Arbeitgeber in Form von finanziellen Anreizen und weitergehenden beruflichen Herausforderungen wie zunehmender Personal- oder Sachverantwortung versprechen.

Interesse am Schutz der Privatsphäre

Trotz seiner Neigung zur Kommunikation seiner Leistungen gegenüber dem Arbeitgeber ist der Mitarbeiter im Allgemeinen an der Privatsphäre am Arbeitsplatz, wie sie die Richtlinien der internationalen Arbeitsorganisation vorsehen [International Labour Office 1993, S. 75], interessiert.

Insbesondere spielt beim Interesse an der Privatsphäre am Arbeitsplatz die Zufriedenheit des Mitarbeiters eine grosse Rolle, die aus dem Gleichgewicht zu geraten droht, wenn das Grundrecht auf informationelle Selbstbestimmung missachtet wird. Insbesondere die unzulässige Erstellung und missbräuchliche Verwendung von Persönlichkeitsmustern über den Mitarbeiter sowie deren etwaige Fehlinterpretation oder Inkorrektheit beeinträchtigen das Verhältnis zwischen Arbeitgeber und Arbeitnehmer nachhaltig bzw. können gravierende Folgen für den Arbeitnehmer haben. Ein entsprechendes Beispiel, wie missbräuchlich Mitarbeiterdaten durch das Unternehmen erhoben und verwendet werden können, findet sich in Abschnitt 4.1.3.

2.2.2 Interessen des Arbeitgebers

Wirtschaftliche Interessen

Im Hinblick auf die personellen Ressourcen ist der Arbeitgeber angesichts seiner Wettbewerbsfähigkeit in erster Linie daran interessiert, Mitarbeiter sorgfältig aufgrund umfassender Merkmale auszuwählen und nach ihrer Einstellung im Rahmen der optimalen Wertschöpfung kontinuierlich einzuplanen. Insbesondere geschieht dies durch die Erhebung umfassender – mitunter auch sensibler – personenbezogener Daten (Einstellung) sowie deren langfristige Speicherung im Rahmen der rechtlichen Möglichkeiten.

Für die spätere optimale Einplanung des Mitarbeiters sind neben seinen Kompetenzen auch seine Leistungen massgeblich, die auf der Basis geeigneter Verfahren zur Leistungserfassung und -analyse objektiviert werden können. Dabei ist es für das Unternehmen naheliegend, Mitarbeiterdaten kontinuierlich zu erheben, zu speichern und auszuwerten, um auf diese Weise über ein vollständiges Leistungsprofil des Mitarbeiters zu verfügen. Dies wiederum kann es dem Unternehmen ermöglichen, kontinuierlich durch motivations- und fähigkeitsfördernde aber auch sanktionierende Massnahmen auf den Mitarbeiter einzuwirken.

Nicht zuletzt kann das Unternehmen durch umfassende Mitarbeiterinformationen etwaigen Schädigungen vorbeugen, die sich aus privatem Ressourcenverbrauch bis hin zu mangelnder Loyalität ergeben können.

Interesse an der Konformität mit der betrieblichen Datenschutzgesetzgebung und des Arbeitsfriedens

Sowohl in der Schweiz als auch in der Bundesrepublik Deutschland sehen sich Arbeitgeber Arbeitnehmervertretungen gegenüber mit gewichtigen Mitwirkungsrechten [MWG 2000, Art. 10; BetrVG 2001, § 87]. Insbesondere in der Bundesrepublik Deutschland obliegt dem Betriebsrat u. a. die Pflicht, darüber zu wachen, dass das Bundesdatenschutzgesetz (BDSG) im Unternehmen beachtet wird [BMA 2000, S. 428].

Da das Unternehmen im Allgemeinen bestrebt sein dürfte, seine Entscheidungen im Interesse geordneter Arbeitsabläufe mit dem Betriebsrat in Einklang zu bringen, sollte es die datenschutzrechtlichen Belange seiner Angestellten nicht ausser acht lassen. Neben dem Arbeitsfrieden ist das Unternehmen zudem an einem der Kundenbeziehung vergleichbaren Mass an Rechtssicherheit interessiert sowie eventuell an der Pflege der Aussenwirkung durch den Schutz der Privatsphäre des Mitarbeiters auch am Arbeitsplatz.

2.2.3 Gegenüberstellung der Interessen

Die Aussagen der Abschnitte 2.2.2 und 2.2.1 lassen sich zusammenfassend in einer Matrix der Chancen und Risken der Verarbeitung von Mitarbeiterdaten darstellen (Tab. 2-2).

Unternehmen	• Adäquater Einsatz • Mitarbeitermotivation • Leistungskontrolle • Fundierte Mitarbeiterbeurteilung	• Negatives Erscheinungsbild • Rechtsunsicherheit • Gefährdung des Arbeitsfriedens im Hinblick auf Betriebsrat
Arbeitnehmer	• Korrekte Mitarbeiterbeurteilung • Karriereentwicklung • Leistungsgerechte Bezahlung	• Fehlerhafte Daten • Fehlinterpretation von Daten • Missbräuchliche Verwendung von Persönlichkeitsmustern • Eingriff in Privatsphäre • Missachtung d. informationellen Selbstbestimmung
	Chancen	**Risiken**

Tab. 2-2: Chancen und Risiken der umfassenden Verarbeitung von Mitarbeiterdaten durch Arbeitgeber

Vergleichbar wie im Bereich des Verhältnisses zwischen Kunden und Unternehmen zeigt sich auch im Bereich des Mitarbeiterdatenschutzes eine weitgehende Übereinstimmung der wirtschaftlichen Ziele von Mitarbeitern und Unternehmen. Diese wird getragen von den hohen Synergieeffekten, die sich für die Unternehmen aus der Motivation ihrer Mitarbeiter und für die Mitarbeiter aus der leistungsgerechten und angemessenen Entlohnung ergeben.

Anders verhält es sich im Bereich der Interessen im Zusammenhang mit der Privatsphäre des Arbeitnehmers gegenüber dem Unternehmen. Während das Unternehmen in diesem Bereich zwar um Ausgleich bemüht ist, bestehen dennoch eindeutige Präferenzen in Richtung der umfassenden Integration von Mitarbeiterdaten, um den zentralen wirtschaftlichen Interessen der Mitarbeiterbeurteilung und -einplanung auf der Basis einer umfassenden Datengrundlage begegnen zu können.

Die Handlungsmöglichkeiten des Mitarbeiters sowohl in Richtung eines Mehr als auch eines Weniger an Persönlichkeitsschutz sind eher begrenzt, obschon Betriebsräte eingesetzt sind. Grund hierfür ist, dass die Datenschutzgesetzgebung mehr noch als im Bereich des Umgangs mit Kundendaten eindeutige Regelungen trifft, auf die in Abschnitt 4.1 im Rahmen der Darstellung möglicher Gefährdungen für den Datenschutz durch das Data Warehousing näher eingegangen wird.

Im Folgenden werden nun zunächst die datenschutzrechtlichen Bestimmungen, wie sie in der Schweiz und der Europäischen Union, dort insbesondere in der Bundesrepublik Deutschland, gelten, skizziert. Dabei wird davon ausgegangen, dass sie das Bedürfnis des Kunden bzw. des Mitarbeiters nach Schutz seiner Privatsphäre in maximaler Weise berücksichtigen, d. h. nicht unbedingt dem gewünschten Mass des Kunden bzw. Mitarbeiters entsprechen. Darauf aufbauend werden Konflikte zwischen den Grundprinzipien des Datenschutzes und dem Data Warehousing identifiziert, um abschliessend die Brauchbarkeit verschiedener datenschutzfreundlicher Ansätze zu bewerten.

3 Datenschutz in der Schweiz und der Europäischen Union

Angesichts der Fülle der datenschutzrechtlichen Begrifflichkeiten und Bestimmungen sollen im Folgenden nur die für die Untersuchung des Data Warehousings relevanten Aspekte betrachtet werden. Die Begriffsbestimmungen für das Schweizerische Datenschutzrecht orientieren sich an den Ausführungen von SCHWEIZER [Schweizer 1999, S. 125-145]. Für die vorliegenden Ausführungen zum Datenschutzrecht in der Europäischen Union (EU) und insbesondere der Bundesrepublik Deutschland bildet der Vortrag von SCHEJA [Scheja 2001] im Rahmen des 3. CC DW2-Workshops die Grundlage.

3.1 Gegenstand des Datenschutzes

In den ersten beiden Artikeln führt das Grundgesetz der Bundesrepublik Deutschland die freie Entfaltung der Persönlichkeit sowie die Unantastbarkeit der Menschenwürde an [Grundgesetz 1994, Art. 1-2]. Wert und Würde der menschlichen Person stehen im Mittelpunkt jeder rechtsstaatlichen Ordnung.

In dieser Werteordnung ist auch das Grundrecht auf informationelle Selbstbestimmung enthalten, d. h. die „Befugnis des Einzelnen, grundsätzlich selbst über die Preisgabe und Verwendung seiner persönlichen Daten zu bestimmen.“ [Bundesverfassungsgericht 1983, Abs. 1]. Dieses Grundrecht zu schützen ist Gegenstand des Datenschutzes.

3.2 Personendaten

Das rasche Wachstum der Datenbestände mit personenbezogenen Daten in öffentlichem und privatwirtschaftlichem Besitz sowie die ständig verbesserten Möglichkeiten zur Auswertung und Nutzung dieser Datenbestände stellen den Datenschutz vor umfangreiche Herausforderungen. Das Hauptaugenmerk liegt dabei auf der Verarbeitung besonders schützenswerter Personendaten. Hierzu gehören religiöse, weltanschauliche, politische und gewerkschaftliche Ansichten oder Tätigkeiten, der Gesundheitsstatus, die Intimsphäre, die Rassenzugehörigkeit, Massnahmen der sozialen Hilfe sowie administrative oder strafrechtliche Verfolgungen und Sanktionen [DSG 1992, Art. 3].

Einige dieser Daten, wie z. B. Massnahmen der sozialen Hilfe müssen an einzelnen Stellen, – – im Hinblick auf Mitarbeiterdaten u. a. auch in Unternehmen – gespeichert werden, obwohl ihre Bekanntgabe an unbefugte Personen grosse gesellschaftliche und wirtschaftliche Nachteile für die betroffene Person mit sich bringen kann. Eine weitaus grössere Gefahr für den Persönlichkeitsschutz des Betroffenen besteht jedoch darin, dass vereinzelt vorliegende Informationen über seine Person zusammengeführt und analysiert werden können. Einen Hinweis darauf, wie brisant die Bildung von sogenannten Persönlichkeitsprofilen ist, gibt das Beispiel aus den USA im Jahr 1966, als die Bevölkerung eine geplante „Super-Datenbehörde“ zu Fall brachte, die sämtliche verfügbare Daten aller Bürger zentral speichern sollte

[Oppliger 1997, S. 31]. Der Fall zeigt, dass durch die Zusammenführung von Daten in Persönlichkeitsprofilen hochgradig sensible Informationen entstehen können, worin der einzelne eine Gefährdung seines Bedürfnisses nach Privatsphäre sehen kann.

3.3 Begrifflichkeiten zur Beschreibung des Umgangs mit personenbezogenen Daten

Sämtliche Datenschutzgesetze und -richtlinien, angefangen beim Schweizerischen Bundesgesetz über den Datenschutz (DSG) vom 19. Juni 1992 [DSG 1992] über die EU-Richtlinie zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten und zum freien Datenverkehr (EU-Datenschutzrichtlinie (EU-DSRL)) vom 24. Oktober 1995 [EU-DSRL 1995] bis hin zum Bundesdatenschutzgesetz (BDSG) vom 23. Mai 2001 [BDSG 2001] – um nur einige Gesetze und Richtlinien zu nennen – beziehen sich auf den gesamten (Daten-)Bearbeitungs- (DSG) bzw. (Daten-)Verarbeitungsprozess (BDSG). Im Folgenden seien die Begrifflichkeiten des Schweizerischen DSG und des deutschen BDSG gegenübergestellt [DSG 1992, Art. 3; BDSG 2001, § 3, Abs. 4], die der Bearbeitungs- bzw. Verarbeitungsprozess umfasst:

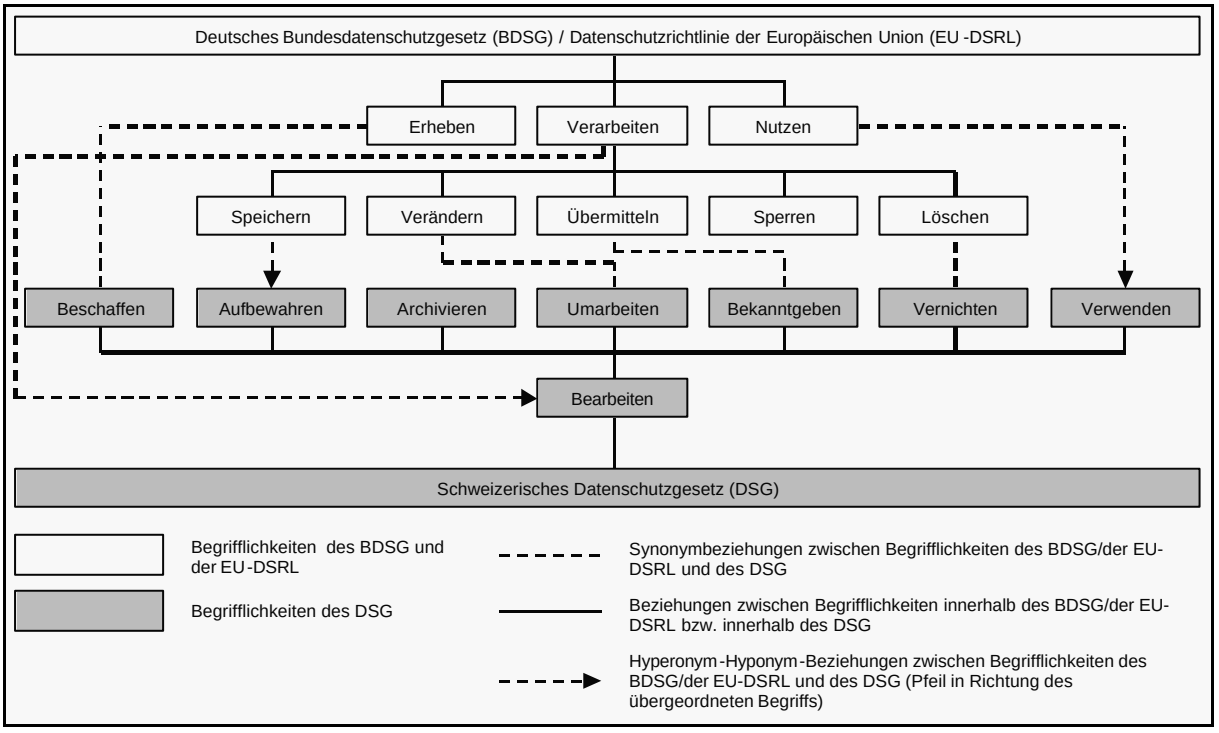

Abb. 3-1: Begrifflichkeiten des Schweizerischen DSG und des deutschen BDSG bzw. der EU-DSRL

Abb. 3-1 zeigt, dass die Begrifflichkeiten im Bezug auf den Umgang mit personenbezogenen Daten in der Schweiz und in Deutschland unterschiedlich sind. Während die Knoten die von SCHEJA [Scheja 2001] bzw. SCHWEIZER [Schweizer 1999, S. 133-145] verwendeten Begriffe

repräsentieren, stellen die Kanten die Beziehungen zwischen den Begriffen der Datenschutzbestimmungen dar. Die durchgezogenen Kanten repräsentieren dabei jeweils die begrifflichen Zusammenhänge innerhalb des BDSG und der EU-DSRL bzw. innerhalb des DSG. Die gestrichelten Kanten stehen für die semantischen Beziehungen zwischen den Begrifflichkeiten der Gesetzeswerke. Bei ungerichteten Kanten handelt es sich um Synonymbeziehungen, bei Hyperonym-Hyponym-Beziehungen weisen die Kanten vom untergeordneten zum übergeordneten Begriff.

Im Folgenden werden die Begrifflichkeiten des Schweizerischen und EU-Datenschutzrechts miteinander verglichen und ihre Bedeutung durch Beispiele illustriert.

Erheben/Beschaffen

Die Begriffe „Erheben“ und „Beschaffen“ können als Synonyme aufgefasst werden.

Unter Erheben wird nach der EU-DSRL das Beschaffen von Daten über den Betroffenen bei ihm selbst, bei Dritten oder aus sonstigen Quellen verstanden, während im DSG mit Beschaffen die direkte, indirekte oder durch technische Analysemittel durchgeführte Erhebung gemeint ist.

Die Erhebung bzw. Beschaffung personenbezogener Daten erfolgt in der Versicherungsbranche beispielsweise über die Kundenkontakte des Vertreters vor Ort, über Call Centers oder das Internet. Darüber hinaus kann sich ein Unternehmen Daten aus externen Datenquellen, so z. B. von Adresshändlern, beschaffen.

Im Bereich des Mitarbeiterdatenschutzes werden personenbezogene Daten zunächst im Rahmen des Bewerbungsverfahrens erhoben, was zum einen auf der Basis von (Online-)Bewerbungsunterlagen und persönlichen Gesprächen, zum anderen aber auch durch frühere Arbeitgeber (in der Schweiz nur mit Einwilligung des Betroffenen) geschieht [BMA 2000, S. 200; EDSB 1994, S. 9]. Im späteren Verlauf der Tätigkeit können Daten im Rahmen der Leistungserfassung automatisiert oder konventionell erhoben werden, um später zu einer Mitarbeiterbeurteilung herangezogen werden zu können. Zu beachten ist jedoch, dass diese Daten nicht die ausschliessliche Grundlage der Mitarbeiterbeurteilung bilden [International Labour Office 1993, S. 75].

Nutzen/Verwenden

Nutzen (EU-DSRL) und Verwenden (DSG) von Personendaten können nicht vollständig synonym verwendet werden. Während unter Nutzen jede sonstige Verwendung von Daten ausser der Verarbeitung verstanden wird, ist die Auffassung von Verwenden im Schweizerischen Datenschutzrecht globaler, da in diesem Fall nur ein Zweck, nicht aber die bereits erfolgte Aufbereitung von Daten vorausgesetzt wird.

Beispielhaft für das Nutzen personenbezogener Daten im Sinne der EU-DSRL kann der Gebrauch bereits gedruckter Adressaufkleber genannt werden, während Verwenden im Sinne

des DSG die Abfrage eines Adressbestands, den Druckvorgang sowie den letztendlichen Gebrauch der Adressaufkleber umfasst.

Verarbeiten/Bearbeiten

Verarbeiten (EU-DSRL) und Bearbeiten definieren sich durch ihre untergeordneten Begriffe, die in den folgenden Abschnitten „Speichern/Aufbewahren/Archivieren“, „Verändern/Umarbeiten“, „Übermitteln/Bekanntgeben/Sperren“ und „Löschen/Vernichten“ beschrieben werden. Da das Bearbeiten mehr umfasst als das Verarbeiten, ist das Bearbeiten übergeordnet.

Speichern/Aufbewahren/Archivieren

Mit Speichern (EU-DSRL) ist das Erfassen, Aufnehmen und Aufbewahren von Daten auf einem Datenträger zum Zwecke ihrer weiteren Verwendung oder Nutzung gemeint, während das Aufbewahren (DSG) die Festhaltung, Bereitstellung und Speicherung von Personendaten umfasst. Die beiden Begriffe beinhalten sich gegenseitig. Da der Begriff des Aufbewahrens durch die Bereitstellung von Daten weiter gefasst ist, kann dennoch von einer Hyperonym-Hyponym-Beziehung ausgegangen werden.

Das Archivieren ist im DSG der Aufbewahrung ausgegliedert. Im Bezug auf den Begriff „Speichern“ der EU-DSRL findet sich jedoch kein Anknüpfungspunkt, da das Speichern einen weiteren Verwendungs- oder Nutzungszweck verfolgt, während das Archivieren lediglich zu Sicherungs- und Dokumentationszwecken erfolgt.

Um das Beispiel der Versicherungsbranche weiter zu verfolgen, werden die erhobenen personenbezogenen Daten in den operativen Systemen des Unternehmens gespeichert. Dies kann ausschliesslich für die Abwicklung eines aktuellen Geschäftsvorfalls erfolgen, jedoch ist es gerade im Versicherungswesen notwendig, dass die Daten über längere Zeiträume archiviert werden, um eintretende Versicherungsfälle auf der Basis adäquat bereitgestellter Daten korrekt abwickeln zu können.

Im Bereich des Mitarbeiterdatenschutzes werden Mitarbeiterdaten spätestens zur Aufnahme der Beschäftigung in ein Personalinformationssystem eingepflegt, wobei beachtet werden sollte, dass nicht alle erhobenen Daten über den Bewerber relevant für die spätere Beschäftigung sind und dementsprechend nicht gespeichert werden sollten [BMA 2000, S. 128], um dem Grundsatz der Verhältnismässigkeit und Notwendigkeit genüge zu tun.

Verändern/Umarbeiten

Verändern (EU-DSRL) und Umarbeiten stellen Synonyme dar, da es sich in beiden Fällen um das inhaltliche Umgestalten von Daten handelt.

Personenbezogene Daten unterliegen beispielsweise durch familiäre Veränderungen laufenden Aktualisierungen, so dass sie inhaltlich verändert bzw. umgestaltet werden müssen.

Übermitteln/Bekanntgeben/Sperren

Unter dem Übermitteln (EU-DSRL) wird die Weitergabe von Daten an Dritte bzw. die Einsichtnahme oder der Abruf der Daten durch einen Dritten verstanden. Bekanntgeben (DSG) beinhaltet das Zugänglichmachen von Personendaten, wie das Einsichtgewähren, Weitergeben oder Veröffentlichen von Daten. Da beide Begriffe die gleichen Sachverhalte beschreiben, müssen sie als synonym betrachtet werden.

Unter Sperren versteht die EU-DSRL das Kennzeichnen von gespeicherten Daten, um ihre weitere Verarbeitung oder Nutzung einzuschränken. Im DSG ist dieser Aspekt als Limitierungsmassnahme der Bekanntgabe verknüpft, jedoch in der Systematik der Begrifflichkeiten nicht explizit angeführt.

Bei einem Versicherungswechsel kann es beispielsweise notwendig werden, dass die Versicherungsdaten von einem Versicherungsunternehmen an ein anderes übermittelt werden müssen. Für den Versicherten sieht die Datenschutzgesetzgebung vor, dass ihm seine persönlichen Daten jederzeit und in der Regel ohne Kostenaufwand zugänglich gemacht werden. Werden personenbezogene Daten vom Versicherten als fehlerhaft angemahnt, so sieht der Datenschutz die Sperrung der Daten vor.

Ein Beispiel für die Bekanntgabe im Bereich von Arbeitnehmerdaten ist die Tatsache, dass diese innerhalb von Unternehmen den zuständigen Sachbearbeitern zugänglich gemacht werden, wobei jedoch bei der Bekanntgabe von besonders schützenswerte personenbezogene Daten erhöhte Rücksicht auf die Belange des Mitarbeiters geboten sein sollte [BMA 2000, S. 128].

Löschen/Vernichten

Schliesslich müssen auch das Löschen (EU-DSRL) und Vernichten (DSG) als synonym interpretiert werden, da beide das unwiederbringliche Unkenntlichmachen gespeicherter Daten meinen.

So erlegt der Datenschutz z. B. Versicherungsunternehmen eine bestimmte Zeit nach Beendigung des Versicherungsverhältnisses auf, sämtliche personenbezogenen Daten des ehemaligen Versicherungsnehmers zu löschen.

Ebenso sieht das Schweizerische Datenschutzrecht die Löschung von Daten abgelehnter Bewerber nach Abschluss des Anstellungsverfahrens bzw. von Mitarbeiterdaten nach einer angemessenen Aufbewahrungsfrist nach Beendigung des Beschäftigungsverhältnisses vor [EDSB 1994, S. 12; 16].

3.4 Grundprinzipien des Datenschutzes

Massstäbe für die formaljuristische Zulässigkeit und den Umfang des Umgangs mit personenbezogenen Daten sind folgende Grundprinzipien [Baeriswyl 2001]:

- Die *Rechtsgrundlage*, aufgrund derer die Bearbeitung personenbezogener Daten notwendig oder zulässig ist. Nach SCHEJA [Scheja 2001] ist die Verarbeitung personenbezogener Daten grundsätzlich verboten. Sie ist nur zulässig, wenn eine Rechtsvorschrift dies erlaubt oder der Betroffene eingewilligt hat [EU-DSRL 1995, Art. 7].
  Z. B. sollte somit vor der Verarbeitung jeglicher personenbezogener Daten geprüft werden, ob die Verarbeitung gesetzlich vorgeschrieben bzw. zulässig ist oder ob die Einwilligung des Kunden eingeholt werden muss bzw. die Interessen beispielsweise des Arbeitgebers im Rahmen eines Einstellungsverfahrens im Vergleich mit dem Grundrecht auf informationelle Selbstbestimmung seitens des Arbeitnehmers überwiegen [BMA 2000, S. 128].
- Die *Zweckgebundenheit*, deren Forderung darin besteht, dass sich der Verarbeitungs- oder Bekanntgabezweck nicht vom Erhebungszweck unterscheiden darf.
  Vom grundsätzlichen Einverständnis eines Versicherungsnehmers zur Verarbeitung seiner personenbezogenen Daten kann beispielsweise nur ausgegangen werden, wenn die Verarbeitung ausschliesslich der Vertragserfüllung dient und nur unerlässliche Daten verarbeitet werden. Für jede darüber hinausgehende Zielsetzung wie z. B. Marketing- oder Analysezwecke sollte das Einverständnis des Versicherungsnehmers explizit eingeholt werden, was selbstverständlich mit nicht unerheblichen Aufwand verbunden ist. Im Bereich des Mitarbeiterdatenschutzes bildet der Arbeitsvertrag den zentralen Zweck zur Verarbeitung von Mitarbeiterdaten durch den Arbeitgeber [EDSB 1994, S. 6].
- Die *Verhältnismässigkeit*, die lediglich die Erhebung und Bearbeitung eines Minimums an personenbezogenen Daten zulässt, was im Allgemeinen auch mit den Begriffen der Datensparsamkeit und Datenvermeidung umschrieben wird. Zudem ist soweit möglich von Anonymisierung und Pseudonymisierung[2] Gebrauch zu machen [EU-DSRL 1995, Art. 6].
  Der Grundsatz der Verhältnismässigkeit fordert von einem Versicherungsunternehmen, dass beispielsweise nur die für die korrekte Kalkulation der Versicherungsprämie und Abwicklung unerlässlichen personenbezogenen Daten erhoben werden. Eine Vorratshaltung an Daten ist dem Datenschutz zufolge nicht zulässig. Gleiches gilt entsprechend für den Arbeitnehmerdatenschutz [OR 2002, § 328b].
- Die *Integrität*, die die durchgängige Richtigkeit der Daten und ihrer Interpretation verlangt.

---

[2] „Anonymisierung ist eine Veränderung personenbezogener Daten derart, dass die Einzelangaben über persönliche und sachliche Verhältnisse nicht mehr einer bestimmten oder bestimmbaren natürlichen Person zugeordnet werden können. […] Pseudonymisierung ist das Verändern personenbezogener Daten durch eine Zuordnungsvorschrift derart, dass die Einzelangaben über persönliche oder sachliche Verhältnisse ohne Kenntnis oder Nutzung der Zuordnungsvorschrift nicht mehr einer natürlichen Person zugeordnet werden können.“ [LDA Brandenburg 2000, S. 184 f.] In Anlehnung an KÖHNTROPP eignet sich die Anonymisierung nicht, wenn mehrere personenbezogene Informationen verkettet oder in Beziehung gesetzt werden sollen [Köhntropp 2000, S. 47].

Grosse wirtschaftliche und soziale Nachteile kann ein Kunde erleiden, wenn beispielsweise seine Versicherung unrichtige Daten über ihn vorhält, die zu einer Falschbeurteilung seines Versicherungsfalls führen können. Insbesondere sollte auch bedacht werden, dass die Zusammenführung personenbezogener Daten aus verschiedenen Quellen zu Fehlinterpretationen führen kann. Ein Halter mehrerer Fahrzeuge, der des öfteren seine Kraftfahrzeugversicherung in Anspruch nehmen muss, darf aufgrund allein dieser Tatsache beispielsweise nicht in eine höhere Risikogruppe des Lebensversicherungsgeschäfts eingestuft werden, da die Schäden an den Fahrzeugen womöglich durch die Angestellten seines Unternehmens verursacht wurden.
Im Bereich des Mitarbeiterdatenschutzes hat der Arbeitgeber nach dem DSG [DSG 1992, Art. 5] beispielsweise die Pflicht, sich regelmässig der Korrektheit der bearbeiteten Mitarbeiterdaten zu vergewissern.

- Die *Sicherheit*, d. h. technische und organisatorische Massnahmen.
  Ein Versicherungsunternehmen verfügt beispielsweise über hochsensible wirtschaftliche und soziale Daten seiner Versicherten. Aus diesem Grund sollten die Zugriffe auf diese Daten beschränkt sein und sensible Daten nur verschlüsselt gespeichert und übertragen werden. Die oben erwähnte Tatsache, dass besonders schützenswerte personenbezogene Daten nur bestimmten Sachbearbeitern zugänglich gemacht werden sollten, verdeutlicht auch in diesem Bereich die Relevanz des Grundsatzes der Sicherheit durch technische und organisatorische Massnahmen.
- Die *Transparenz*, die es dem Betroffenen ermöglicht, sich jederzeit Klarheit darüber zu verschaffen, wo, welche Daten durch wen bearbeitet werden, so dass er auch jederzeit von seinem Auskunftsrecht Gebrauch machen kann.
  Beispielsweise dürfen im Schweizerischen Datenschutzrecht keine Mitarbeiterdaten ohne vorherige Information der Mitarbeiter mit Hilfe von Überwachungs- oder Kontrollsystemen erhoben werden [EDSB 1994, S. 18].
- Die *Verantwortung*, d. h. dass der Betroffene auf den Rechtsgrundsatz von Treu und Glauben vertrauen kann, wonach er davon ausgehen kann, dass seine Daten ausschliesslich zu dem von ihm angenommenen Zweck bearbeitet werden.

3.5 Folgen von Verstössen gegen datenschutzrechtliche Bestimmungen

Datenschutzverstösse werden von Gesetzeswegen in der Regel mit Geldbussen geahndet, die gegenüber den Potenzialen, die durch die systematische Analyse und Nutzung personenbezogener Daten gewonnen werden, gering erscheinen.

In der Bundesrepublik Deutschland werden vorsätzliche oder fahrlässige Ordnungswidrigkeiten in leichten Fällen mit Geldbussen bis € 25.000 bzw. in schwereren Fällen bis € 250.000 geahndet [BDSG 2001, § 43]. Bei vorsätzlicher Handlung gegen Entgelt oder in der Absicht, sich oder einen anderen zu bereichern oder einen anderen zu schädigen, sieht das

BDSG eine Freiheitsstrafe von bis zu zwei Jahren vor [BDSG 2001, § 44]. Im Schweizer Recht geht das Strafgesetzbuch (StGB) auf die Folgen von Verstössen gegen den Datenschutz ein. Es sieht ohne Nennung des Strafmasses Geldbussen oder Freiheitsstrafen vor, wenn besonders schützenswerte personenbezogene Daten oder Persönlichkeitsprofile, die nicht frei zugänglich sind, aus Datensammlungen beschafft werden [StGB 2002, Art. 179^{novies}].

Die vorgesehenen Sanktionen stellen jedoch kaum ein geeignetes Mittel dar, um das Bedürfnis der Bürgerinnen und Bürger nach Privatheit wirksam durchzusetzen. Gründe hierfür sind die unzureichende personelle Ausstattung von Datenschutzbehörden, aber auch die ständig zunehmende Komplexität in den Datenbeständen von Unternehmen und öffentlichen Stellen, die eine systematische Kontrolle wesentlich erschwert.

4 Datenschutz und Data Warehousing

Die gemeinsame Betrachtung der Aussagen von Kapitel 2 und 3 führt zu der Erkenntnis, dass die formaljuristischen Forderungen des Datenschutzes einerseits das Bedürfnis des Kunden nach Schutz seiner Privatsphäre ungeachtet von Unternehmensinteressen abbilden, andererseits jedoch das Interesse des Kunden an personalisierten Dienstleistungen durch Unternehmen weitgehend ausser Acht lassen. Im Hinblick auf das Verhältnis zwischen Unternehmen und ihren Angestellten sehen die gesetzlichen Regelungen verstärkt einen Interessenausgleich vor, da hier zentrale Grundrechte einander gegenüberstehen (vgl. Abschnitt 2.2).

Im Folgenden soll somit für das Verhältnis zwischen Kunden und Unternehmen mit „Datenschutz“ weniger Persönlichkeitsschutz im formaljuristischen Sinn als vielmehr das Bedürfnis des Kunden nach Schutz seiner Privatsphäre unter Berücksichtigung seines Interesses am Zusatznutzen [Österle/Winter 2000, S. 28] durch das Wissen des Unternehmens über die Bedürfnisse seiner Kunden [Österle/Winter 2000, S. 33] assoziiert werden. Insofern Mitarbeiter ebenfalls ein zweigeteiltes Interesse hinsichtlich der Verarbeitung ihrer personenbezogenen Daten im Data Warehousing haben (Zusatznutzen, z. B. in Form leistungsgerechter Bezahlung, vs. Privatsphäre am Arbeitsplatz), wird diese Assoziation auch für diesen Bereich verfolgt.

4.1 Mögliche Konflikte zwischen dem Data Warehousing und dem Bedürfnis des Kunden bzw. Mitarbeiters nach Schutz seiner Privatsphäre

Im Folgenden wird entlang der Referenzarchitektur für das Data Warehousing, wie sie im CC DW2 verwendet wird [Auth/von Maur/Helfert 2002, S. 39], konkret aufgezeigt, an welchen Stellen des Data Warehousings möglicherweise das Bedürfnis des Kunden bzw. Mitarbeiters nach informationeller Selbstbestimmung übergangen wird. Zielsetzung ist dabei weder der formaljuristische Abgleich zwischen den Methoden des Data Warehousings und der Datenschutzgesetzgebung noch die Infragestellung der Data-Warehouse-Architektur. Es sollen vielmehr die – hinsichtlich der Bedürfnisse von Kunden bzw. Mitarbeitern nach Schutz ihrer Privatsphäre – kritischen Phasen des Data Warehousings identifiziert werden und auf ihre Datenschutzkonformität hin untersucht werden. Datenschutzkonformität wird in Übereinstimmung mit der Definition zu Beginn von Kapitel 4 als maximale Ausprägung des Kunden- bzw. Mitarbeiterbedürfnisses nach Privatsphäre verstanden.

Im Rahmen des 3. CC DW2-Workshops wurden solche kritischen Phasen identifiziert. Abb. 4-1 gibt einen konsolidierten Überblick über die erarbeiten kritischen Stellen. In den einzelnen Abschnitten dieses Unterkapitels soll entlang der in Abb. 4-1 markierten Stellen bzw. Phasen untersucht werden, welche Vorgänge dort stattfinden und eventuell den Bedürfnissen des Kunden bzw. Mitarbeiters entgegenstehen. Die letzte Ziffer des jeweiligen Unterabschnitts bezeichnet jeweils die Nummer der kritischen Stelle in Abb. 4-1.

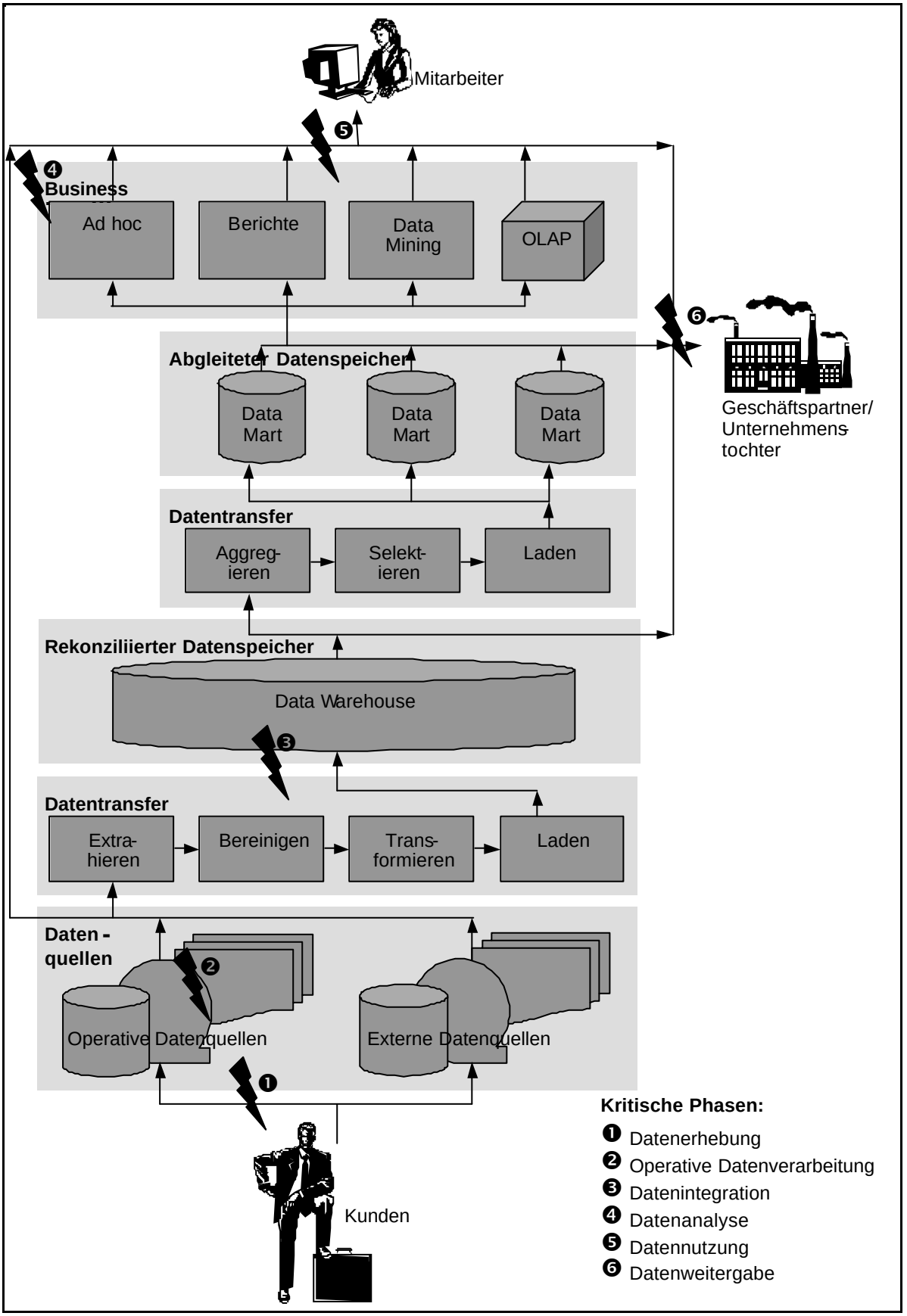

Abb. 4-1: Kritische Phasen für den Datenschutz im Data Warehousing

4.1.1 Datenerhebung

Erhebungskanäle

Der Kontakt zwischen Kunden und Unternehmen erfolgt angesichts der technischen Möglichkeiten zunehmend über die verschiedensten Kanäle, angefangen beim persönlichen Kundenkontakt über Call Centers und E-Commerce bis hin zum Mobile Computing. Alle diese Kanäle sollten im Auge behalten werden, wenn man von der Erhebung personenbezogener Daten direkt beim Kunden spricht.

Mitarbeiterdaten werden ebenfalls über vielfältige Kanäle erhoben. Dabei lässt sich ebenfalls eine Einteilung in konventionelle Kanäle (z. B. Bewerbungsgespräch, Bewerbungsunterlagen) und elektronische Kanäle (z. B. elektronische Bewerbung, Rechnernutzung, Zeiterfassung, Zugangskontrolle etc.) vornehmen.

Bei der Wahl des Kanals zur „Übertragung“ personenbezogener Daten sollte in besonderer Weise auf Vertraulichkeit und Integrität geachtet werden. Insofern die Datenerhebung durch Mitarbeiter bzw. (zukünftige) Kollegen geschieht, sollte sich das Unternehmen ihrer Zuverlässigkeit und Verschwiegenheit vergewissern. Bei elektronischen Kanälen ist in erster Linie die Übertragungssicherheit kritisch, was z. B. mittels digitaler Signaturen und sonstiger kryptographischer Verfahren behoben werden kann, jedoch nicht im Fokus dieser Arbeit liegt.

Direkte Datenerhebung beim Kunden bzw. Mitarbeiter

Als problematisch für den Datenschutz kann sich an dieser Stelle die unzureichende Aufklärung des Kunden bzw. Mitarbeiters über den Verwendungszweck seiner personenbezogenen Daten erweisen. Dies ist insbesondere dann der Fall, wenn die Daten für Analysezwecke verwendet werden sollen, von denen in der Regel zum Zeitpunkt der Erhebung die Zielsetzung noch nicht feststeht bzw. auch zum Zeitpunkt der Analyse keine konkrete Hypothese formuliert wird. Dies ist beispielsweise der Fall, wenn bei der Anwendung algorithmisch aufwändiger Analyseverfahren (z. B. Data Mining) Verhaltensmuster identifiziert werden sollen. Somit kann vom Kunden bzw. Mitarbeiter in der Regel nur sehr eingeschränkt eine Einwilligung eingeholt bzw. vorausgesetzt werden, die zudem die Mächtigkeit und Detailfragen der Datenanalyse kaum vollständig abdecken kann.

Im Hinblick auf spätere Auswertungen besteht prinzipiell die Tendenz zur Erhebung von Kunden- bzw. Mitarbeiterdaten, die für die Vertragsgestaltung irrelevant sind, jedoch v. a. in ihrer Gesamtheit äusserst sensibel sein können. So ist es beispielsweise für den Kunden vom Standpunkt des eigentlichen Vertragszwecks kaum einsichtig, warum er vor der Nutzung eines kostenlosen E-Mail-Accounts vollständige Angaben über Familienstand, Personen im Haushalt, beruflichen Status, PC- und Internet-Nutzung oder gar über seinen schulischen und beruflichen Werdegang machen soll.

Speziell für die Erhebung von Mitarbeiterdaten lässt sich eine Einteilung in vorvertragliche und vertragliche Datenerhebungen vornehmen. Die vorvertragliche Datenerhebung dient in erster Linie zur Abklärung der Eignung des Bewerbers. Datenquellen sind hierbei z. B. konventionelle oder elektronische Bewerbungsunterlagen und der Direktkontakt im Rahmen des Bewerbungsgesprächs.

Die Erhebung personenbezogener Daten während des Beschäftigungsverhältnisses erfolgt z. B. im Rahmen von Mitarbeiterbeurteilungen oder aus Sicherheitsgründen. Möglichkeiten sind dabei das direkte Gespräch, aber auch akustische, optische oder elektronische Kontrolleinrichtungen[3]. Beispiele hierfür sind der Mitschnitt von Telefonaten mit Kunden, was z. B. im Call Center praktiziert wird, die Produktionsüberwachung mit Hilfe von Kameras oder die Messung der Häufigkeit, Art und Weise der Rechnernutzung bis hin zur Erfassung der Tastenanschläge [EDSB 1994, S. 17-21]. Gut illustriert dies das folgende Beispiel:

Mit speziellen Computerprogrammen können Vorgesetzte „jeden Tastenanschlag und jede Anwendung auf dem PC der Angestellten nachvollziehen. Jede besuchte Website wird angezeigt und jede E-Mail wird mitgelesen. […] Bei der Eingabe bestimmter Schlüsselwörter ist sogar eine Fotografie des fraglichen Bildschirmes möglich." Auf diese Weise sind Analysen denkbar, warum manche Mitarbeiter „nur einen Leistungsoutput von 20% erbringen, andere aber 80%" [TDG-Germany 2002].

Als konfliktär kann sich die Erhebung von Mitarbeiterdaten herausstellen, wenn Daten ohne die Zustimmung des (künftigen) Mitarbeiters oder in einem Umfang erhoben werden, der sich nicht mit dem Vertragszweck bzw. mit dem Zweck der Eignungsfeststellung eines Bewerbers deckt [EDSB 1994, S. 6]. Darüber hinaus sehen die Datenschutzgrundsätze zum Umgang mit Mitarbeiterdaten vor, dass nur Daten, die „mit dem Arbeitsplatz oder der zu leistenden Arbeit in Zusammenhang stehen", erhoben werden dürfen [EDSB 1994, S. 9]. In diesem Zusammenhang wird der Bewerber bzw. Mitarbeiter nicht belangt, wenn er eine unzulässige Frage des (künftigen) Arbeitgebers nicht wahrheitsgemäss beantwortet [EDSB 1994, S. 9; BMA 2000, S. 31].

Externe Datenquellen

Externe Datenquellen lassen sich differenzieren in öffentlich zugängliche Datensammlungen, die personenbezogene Daten listenmässig im Rahmen sogenannter „Hardfacts" beinhalten (z. B. Telefonbuch), und Datensammlungen, die weitergehende Informationen enthalten, so z. B. Daten von Adresshändlern. Während erstere aufgrund ihrer Öffentlichkeit als daten-

[3] Der spezielle Bereich von „Überwachungs- und Kontrollsystemen am Arbeitsplatz" [EDSB 1994, S. 17] ist in der Bundesrepublik Deutschland und der Schweiz unterschiedlich geregelt. Während in der Bundesrepublik die Überwachung zu Zwecken der Sicherheit, der Leistungs- und der Verhaltenskontrolle mit Zustimmung des Betriebsrats zulässig ist [BMA 2000, S. 127], ist die Verwendung solcher Systeme durch den Arbeitgeber in der Schweiz „schon aus Gründen des Gesundheitsschutzes" nicht zulässig, „wenn sie der Überwachung des Verhaltens" von Mitarbeitern am Arbeitsplatz dient [ArGV3, Art. 26].

schutzrechtlich eher unproblematisch anzusehen sind [BDSG 2001, § 28], kann die Rechtslage bei nicht öffentlich zugänglichen Sammlungen personenbezogener Daten problematischer sein, da das Unternehmen, das die Daten übernehmen möchte, nicht ohne weiteres von der ursprünglichen Einwilligung des Betroffenen zur Datenbekanntgabe ausgehen kann, weil die Übernahme eine Änderung des Bearbeitungszwecks beinhalten kann.

Insbesondere im Verhältnis zwischen Unternehmen und ihren Bewerbern stammen zahlreiche Daten aus externen Quellen. Im Rahmen des Bewerbungsverfahrens werden z. B. Gesundheitsdaten im Rahmen ärztlicher Eignungsgutachten erhoben und Aussagen über die gesundheitliche Eignung des Bewerbers an das Unternehmen weitergeleitet. Weitere personenbezogene Daten werden in sogenannten Assessment Centers erhoben oder stammen aus graphologischen Gutachten, psychologischen Leistungs- oder allgemeinen Persönlichkeitstests [EDSB 1994, S. 10 f.]. Darüber hinaus kann der künftige Arbeitgeber personenbezogene Daten von früheren Arbeitnehmern beziehen [EDSB 1994, S. 9; BMA 2000, S. 200]. Umfang und Zweck derartiger Datenerhebungen sind jedoch durch die einschlägigen Gesetzgebungen stark dahingehend reglementiert, dass von einem umfassenden Interesse des Bewerbers am Schutz seiner Privatsphäre ausgegangen wird [BMA 2000, S. 125].

4.1.2 Operative Datenverarbeitung

Da die operativen Systeme in der Regel Daten zur Abwicklung von Verträgen verarbeiten, kann im Allgemeinen von einer hochgradigen Datenschutzkonformität ausgegangen werden, sofern keine personenbezogenen Daten involviert sind, die nicht unmittelbar einem Vertragszweck dienen.

Als Teil der operativen Systemlandschaft kann bei der Datenarchivierung von einer längerfristigen zweckgebundenen Speicherung ausgegangen werden. Der Zweck der Datenaufbewahrung im Rahmen einer Kundenbeziehung besteht in erster Linie in der Absicherung des Unternehmens im Hinblick auf Gewährleistungsfälle, was datenschutzrechtlich unproblematisch ist. Eine darüber hinausgehende Speicherung zu Archivzwecken, die nicht mehr der Vertragserfüllung dient, muss dahingegen nicht generell im Interesse des Kunden liegen.

Die rein operative Verarbeitung von Mitarbeiterdaten erstreckt sich beispielsweise auf die Bereiche der Personaldatenverwaltung, der Personalabrechnung mit all ihren Unterfunktionen, angefangen von der Zeitermittlung, über Lohnberechnungen bis hin zu Reisekosten, sowie der Terminüberwachung [Scheer 1998, S. 486 f.]. Diese Aufgaben finden hauptsächlich im Rahmen des Vertragszwecks statt, so dass sie sich als datenschutzrechtlich unproblematisch herausstellen. Wie im Bereich der Kundendatenverarbeitung stellt sich auch hier die Datenarchivierung als kritisch heraus, wenn Mitarbeiterdaten über eine Aufbewahrungsfrist von fünf, in Einzelfällen zehn, Jahren nach Ausscheiden des Mitarbeiters aus dem Unternehmen aufbewahrt werden. Dabei sollte von Seiten des Datenschutzes her beachtet werden, dass

nur diejenigen Daten beibehalten werden sollten, deren Aufbewahrung für den ehemaligen Mitarbeiter von ausdrücklichem Interesse ist (z. B. Arbeitszeugnisse) [EDSB 1994, S. 16].

4.1.3 Datenintegration

ETL-Phase

Wie bereits mehrfach festgestellt wurde, sieht der Datenschutz keine Möglichkeit zur Zweckänderung im Laufe der Verarbeitung personenbezogener Daten durch das Unternehmen vor. Bei der Übernahme personenbezogener Daten aus operativen Systemen in ein Data Warehouse findet jedoch eine solche Veränderung statt. Es sind in dieser Phase des Data Warehousings weniger die Verfahren des ETL-Prozesses, die aus Sicht des Kunden bzw. Mitarbeiters bedenklich sein können, als vielmehr die Änderung des Bearbeitungszwecks.

Im Bereich des Mitarbeiterdatenschutzes rücken in diesem Zusammenhang die dispositiven Aufgaben [Scheer 1998, S. 486] des Arbeitgebers in den Mittelpunkt der Betrachtung. Insbesondere der Bereich der Personalplanung basiert u. a. auf den Kompetenzmerkmalen und Leistungsdaten der Mitarbeiter. Während diese Daten für sich genommen in engem Zusammenhang mit dem Arbeitsplatz bzw. der durch den Mitarbeiter zu leistenden Arbeit stehen [EDSB 1994, S. 9], stösst ihre Nutzung zu Zwecken, die über die rein operative, der Vertragserfüllung dienenden Verarbeitung hinausgehen, auf die gespaltene Interessenlage des Mitarbeiters. Einerseits ist er an korrekter und begründeter Leistungsbeurteilung, adäquatem Einsatz im Unternehmen bei angemessener Entlohnung sowie der Weiterentwicklung des Unternehmens u. a. zur Sicherung seines Arbeitsplatzes interessiert. Andererseits sind die schutzwürdigen Interessen des Arbeitnehmers hinsichtlich seiner Privatsphäre in höherem Masse als beim Kunden betroffen, da das Beschäftigungsverhältnis im Gegensatz zur Kundenbeziehung schon von Gesetzeswegen die Speicherung besonders schützenswerter personenbezogener Daten vorsieht, so z. B. Versicherungsdaten [EDSB 1994, S. 13].

Data Warehouse

Mit dem Data Warehouse ist die Integration von Daten und somit die Erstellung von Persönlichkeitsprofilen eng verbunden. Da die Zusammenschau personenbezogener Merkmale in den Bereich sensibler Informationen zu rechnen ist, ergibt sich an dieser Stelle ein potenzieller Konflikt mit den Interessen des Kunden. Ein Beispiel aus dem Bereich des Mitarbeiterdatenschutzes verdeutlicht dies. In dem Lehrfilm „Wer ist Albert Schneider?“ werden die sinkenden Leistungsdaten des wenige Jahre vor dem Ruhestand befindlichen Albert Schneider elektronisch erfasst. Wegen einer kurzfristigen Erkältung wird Albert Schneider krankgeschrieben, was ebenfalls elektronisch festgehalten wird. Schliesslich verfügt der Arbeitgeber von Albert Schneider über eine betriebseigene Tankstelle, wo Mitarbeiter ihre Privatfahrzeuge verbilligt betanken können und der fällige Betrag zudem erst am Monatsende direkt vom Gehalt abgebucht wird. Kurz vor seiner Krankmeldung tankt Albert Schneider sein

Fahrzeug, die Füllmenge und der Rechnungsbetrag werden gespeichert. Gleich am ersten Tag nach Ende des Krankenstandes, tankt Albert Schneider erneut, da seine erwachsene Tochter während der Krankmeldung das väterliche Fahrzeug ausgiebig nutzte. Diese Randinformation ist neben sinkender Arbeitsleistung, Krankmeldung und Benzinrechnungen jedoch nicht elektronisch erfasst, so dass Albert Schneider in der Gefahr steht, dass das Unternehmen durch Analyse seines Persönlichkeitsprofils zu dem unrichtigen Schluss kommt, er würde krankfeiern.

Gemäss der Definition von Inmon [Inmon 1996, S. 35] werden Daten im Data Warehouse über lange Zeiträume gespeichert, um die historische Entwicklung von Daten nachvollziehen zu können. Die Problematik, die sich daraus ergibt, wurde bereits im Zusammenhang mit der Datenarchivierung diskutiert. Im Bezug auf das Kern-Data-Warehouse stellt sich auf Seiten des Datenschutzes auch die Frage der Verhältnismässigkeit, d. h. es muss davon ausgegangen werden, dass zahlreiche personenbezogene Daten „auf Vorrat“ unabhängig von einem bestimmten Verarbeitungs- bzw. bestimmbaren Analysezweck im Data Warehouse vorgehalten werden.

Schliesslich fordern die Datenschutzbestimmungen die Richtigkeit und Integrität von personenbezogenen Daten. Probleme, eine ausreichende Datenqualität im Rahmen des Data Warehousings zu gewährleisten und zu quantifizieren [Helfert/Herrmann/Strauch 2001, S. 1] unterstreichen die Fragwürdigkeit der Datenschutzkonformität an dieser Stelle. Die Integration verschiedener personenbezogener Merkmale kann zuweilen ein verzerrtes Persönlichkeitsbild liefern, da beispielsweise nicht zuletzt durch die Datenüberführung von einem Datenmodell in ein anderes in der Regel ein gewisses Mass an Semantik eingebüsst wird. Weitaus zentraler als das Datenqualitätsproblem ist jedoch die Qualität der Interpretation von Persönlichkeitsprofilen.

SCHEJA formulierte auf dem 3. CC DW2-Workshop in diesem Zusammenhang das Beispiel einer Call-Center-Applikation, die den Anrufer aufgrund seiner Zugehörigkeit zur Berufsgruppe „Lehrer“ grundsätzlich automatisch ans Ende der Warteschleife setzt, da dieser Berufsstand im Beziehungsmanagement des Unternehmens als überdurchschnittlich schwierig gilt.

Für den Mitarbeiterdatenschutz sei abschliessend darauf hingewiesen, dass die Zusammenführung von Mitarbeiterdaten im Data Warehouse zu noch umfassenderen Persönlichkeitsprofilen und einer Akkumulierung besonders schützenswerter personenbezogener Daten führt als dies ohnehin schon in der Personalakte der Fall ist, wo bereits aufgrund gesetzlicher Bestimmungen umfangreiche sensible Daten vorgehalten werden [EDSB 1994, S. 9].

4.1.4 Datenanalyse

Da Analysewerkzeuge für OLAP oder Data Mining neben dem Direktzugriff (Ad-hoc-Access) auf den Gesamtdatenbestand des Data Warehouse die zentralen Zugriffsmöglichkeiten

auf das Data Warehouse darstellen [Jung/Winter 2000, S. 11], sollten sie durch entsprechende Autorisierungskonzepte gesichert werden, um dem Anspruch des Kunden und Mitarbeiters nach vertraulicher und integrer Verarbeitung seiner jeweiligen personenbezogenen Daten nachzukommen. Dabei handelt es sich jedoch um Fragestellungen konkreter technischer und organisatorischer Massnahmen zum Datenschutz, die in dieser Arbeit nicht weiter verfolgt werden sollen, jedoch beispielsweise im IT-Grundschutzhandbuch des deutschen Bundesamtes für Sicherheit in der Informationsverarbeitung (BSI) ausgeführt sind [BSI 2002].

Insbesondere bei weltweit tätigen Unternehmen ist für jedes Analysewerkzeug eine gesonderte Untersuchung notwendig, ob alle Funktionalitäten den jeweiligen nationalen Datenschutzbestimmungen entsprechen. Auf diese Weise sollten differenzierte Massnahmen zur Rechtevergabe erarbeitet werden.

Vielfach wohnen jedoch den Analyseverfahren selbst bereits datenschutzrechtliche Probleme inne. OLAP- und Data-Mining-Werkzeuge bieten beispielsweise die Möglichkeit, Kundeneinschätzungen und -segmentierungen weitgehend automatisiert durchzuführen. Werden die Ergebnisse anschliessend auf der gleichen Datengrundlage von einem Mitarbeiter überprüft, so ist das Vorgehen nach geltender Rechtslage zulässig (streng genommen, sofern der Analysezweck definiert und die Einwilligung des Betroffenen vorliegt), wohingegen dem Trend beispielsweise zu vollautomatisierter Kundensegmentierung auf Seiten des Datenschutzes mit grosser Skepsis begegnet wird. Da die o. g. Analyseverfahren prinzipiell auch zur Beurteilung von Mitarbeitern in Frage kommen, sei darauf hingewiesen, dass Mitarbeiterbeurteilungen nicht ausschliesslich auf Basis von technischen Überwachungs- und Kontrolleinrichtungen durchgeführt werden dürfen, woraus sich ableiten lässt, dass vollautomatisierte Mitarbeiterbeurteilungen nicht durchgeführt werden sollten [International Labour Office 1993, S. 75].

Da durch Verfahren zur Datenanalyse aus einer Reihe von explizit vorliegenden Persönlichkeitsmerkmalen weitere implizite, d. h. bis dahin unbekannte oder zumindest nirgends verzeichnete Persönlichkeitsmerkmale generiert werden können, sollte der Funktionsumfang von Analysetools einer Überprüfung auf Konformität mit den Bedürfnissen des Kunden bzw. des Mitarbeiters hinsichtlich des Schutzes seiner Privatsphäre unterzogen werden.

Ihren eigentlichen Wert erhalten die Ergebnisse aus einschlägigen Analyseverfahren in der Regel durch die Zusammenführung mit den zugrundeliegenden Persönlichkeitsprofilen. Für diesen weiteren Ausbau von Persönlichkeitsprofilen sollten die Aussagen zum datenschutzrechtlichen Umgang mit der Integration personenbezogener Daten in Abschnitt 4.1.3. beachtet werden.

4.1.5 Datennutzung

Im folgenden wird v. a. die datenschutzrelevante Rolle des Mitarbeiters im Unternehmen diskutiert, insofern er Kunden- oder Mitarbeiterdaten verarbeitet.

Mitarbeitern eines Unternehmens sollten nur diejenigen personenbezogenen Daten zugänglich sein, die für die Erfüllung ihrer Aufgaben benötigt werden. Andernfalls wäre von formaljuristischer Seite her eine unverhältnismässige Bekanntgabe personenbezogener Daten feststellbar, was insbesondere im Bereich besonders schützenswerter Mitarbeiterdaten vermieden werden sollte [BMA 2000, S. 128; EDSB 1994, S. 8]. Im Gegensatz zum Austausch personenbezogener Daten zwischen Unternehmen bleibt in diesem Fall zwar der Inhaber der Datensammlung, d. h. der Unternehmer, identisch, jedoch würden personenbezogene Daten ggf. unnötiger Weise zugänglich gemacht werden.

Handelt es sich bei den Mitarbeitern zudem um Analysten, so geht mit der Bekanntgabe zumeist eine Änderung des ursprünglichen Bearbeitungszwecks einher, zumal auch unabhängig vom Data-Warehouse-Einsatz direkt aus den operativen Systemen Persönlichkeitsprofile erzeugt werden können.

Ähnlich verhält es sich mit der Bekanntgabe von Ergebnissen aus Analyseverfahren an Mitarbeiter. Auch hierbei kann es sich um personenbezogene Daten handeln, die dem Mitarbeiter gemäss den Forderungen des Datenschutzes nicht vorbehaltlos bekannt gegeben werden sollten.

Sämtliche Mitarbeiter im Unternehmen, die mit natürlichen Personen bzw. deren Daten in Kontakt kommen, sollten sich der jeweiligen datenschutzrechtlichen Bestimmungen bewusst sein. Fehlende Schulung und Kompetenz sowohl im Bereich des direkten Kundenkontakts als auch im Umgang mit Kunden- und Mitarbeiterdaten innerhalb des Unternehmens kann dazu führen, dass Kunden misstrauisch bzw. die Interessenvertretungen der Arbeitnehmer auf den Plan gerufen werden. Dies kann insbesondere dann der Fall sein, wenn der Eindruck entsteht, dass mit personenbezogenen Daten nicht nachvollziehbar umgegangen wird.

4.1.6 Datenweitergabe

Eine für den Datenschutz besonders relevante Stelle ist der dem Data Warehousing nachgelagerte Bereich der Datenweitergabe, d. h. der Austausch personenbezogener Daten zwischen Unternehmen. In diesem Zusammenhang sind die unterschiedlichsten Konstellationen vorstellbar:

- Sender und Empfänger sind rechtlich nicht selbständige Teile eines Unternehmens.
- Sender und Empfänger sind rechtlich unabhängige Unternehmen bzw. Unternehmensteile.
- Sender und Empfänger tauschen Daten im Rahmen eines fusionsbedingten Mergers aus.
- Personenbezogene Daten werden im internationalen Raum weitergegeben.
- Sender und Empfänger handeln mit personenbezogenen Daten (Data Trading).
- Der Empfänger verarbeitet die Daten im Auftrag des Senders.

- Beim Empfänger handelt es sich um staatliche Stellen, die z. B. Sozialversicherungsdaten erhalten, deren Erhebung gesetzlich vorgeschrieben ist [EDSB 1994, S. 15].
- Sender und Empfänger sind der frühere und zukünftige Arbeitgeber eines Stellensuchenden [BMA 2000, S. 200; EDSB 1994, S. 9].

Bei allen Formen der Datenbekanntgabe bzw. -weitergabe sehen die Datenschutzbestimmungen enge Grenzen vor. Während der Datenaustausch innerhalb eines Unternehmens im Grossen und Ganzen abgesehen von Mitarbeiterdaten (vgl. Abschnitt 4.1.5) unproblematisch ist, jedoch nach Auffassung des Datenschutzes dem Grundsatz der Verhältnismässigkeit genügen muss, gestaltet sich der Austausch von Daten zwischen rechtlich selbständigen Unternehmen bzw. Unternehmenseinheiten wesentlich problematischer, da dies nicht ohne weiteres in den Allgemeinen Geschäftsbedingungen des Unternehmens festgeschrieben werden kann, sondern vielmehr die neuerliche Einwilligung des Kunden notwendig wäre. Auch der Arbeitnehmer kann sein Recht auf Privatsphäre nicht uneingeschränkt abtreten [OR 2002, Art. 328b].

Insbesondere die Bekanntgabe personenbezogener Informationen ins Ausland ist laut Datenschutzgesetzgebung nur zulässig, wenn im Empfängerland eine gleichwertige Qualität des Datenschutzes, insbesondere hinsichtlich seiner rechtlichen Regelungen gegeben ist. Beispielsweise kann selbst ausschliesslich innerhalb eines weltweit tätigen Unternehmens die Weitergabe sensibler Informationen wie der Religionszugehörigkeit problematisch sein, da sich hieraus persönliche Nachteile für den Betroffenen ergeben können, wenn im Empfängerland z. B. keine Religionsfreiheit besteht. Aus diesem Grund ist die Zulässigkeit der Datenübermittlung mit den zuständigen staatlichen Stellen abzuklären.

Schliesslich kann der Austausch personenbezogener Daten zwischen Unternehmen auf der Basis von Verkauf, Austausch, Leasing, Vermietung oder Schenkung [Schweizer 1999, S. 292] stattfinden. Selbstverständlich existieren auch in diesem Zusammenhang vielfältige datenschutzrechtliche Bestimmungen.

Im Fall der Auftragsdatenverarbeitung besteht die Möglichkeit, dass die Weisungsgebundenheit des Auftragnehmers durch diesen unterlaufen wird, wenn personenbezogene Daten nicht im Sinne des Auftraggebers verarbeitet werden. Grundsätzlich ist die weisungsgebundene Auftragsdatenverarbeitung zulässig. Ohne die Weisungsgebundenheit liegt jedoch eine unzulässige Datenbekanntgabe vor. Insbesondere sieht der Datenschutz länderspezifische Regelungen zur Auftragsdatenverarbeitung auch innerhalb von Konzerngesellschaften vor [Scheja 2001].

4.1.7 Zusammenfassung

Die obigen Ausführungen haben gezeigt, dass im Data Warehousing mehrere kritische Phasen identifiziert werden können, an denen das Interesse des Kunden bzw. Mitarbeiters am Schutz seiner Privatsphäre nicht ohne weiteres berücksichtigt wird.

Bereits die Erhebung personenbezogener Daten erfolgt nicht unbedingt zweckorientiert. Insbesondere die Änderung des ursprünglichen Verarbeitungszwecks würde die neuerliche Einwilligung des Kunden bzw. des Mitarbeiters[4] erfordern, was jedoch mit erheblichem Aufwand für das Unternehmen verbunden sein kann.

Darüber hinaus stellen sich die umfassenden Möglichkeiten zur Bildung von Persönlichkeitsprofilen, die langfristige Speicherung von Daten im Data Warehouse, ihr grosser Umfang und schliesslich die vielfältigen Verfahren der Datenanalyse als wenig konform mit dem Interesse des Kunden bzw. Mitarbeiters am Schutz seiner personenbezogenen Daten dar.

Weniger augenscheinlich, aber nicht weniger von Bedeutung ist in diesem Zusammenhang die kaum umfassend realisierbare Aufklärung des Kunden bzw. Mitarbeiters über die Verwendung seiner Daten, insbesondere im Hinblick auf die komplexen Analysemöglichkeiten.

Abschliessend stellt sich insbesondere für ein weltweit tätiges Unternehmen die grundsätzliche Frage, nach welchen Datenschutzbestimmungen zu verfahren ist. Während beispielsweise in den USA grösstenteils von einer Selbstregulierung der Privatwirtschaft im Hinblick auf datenschutzrechtliche Interessen ausgegangen wird, existieren in Europa weitgehend strikte nationale und internationale Bestimmungen und Richtlinien, die bei Unterschreitung eines bestimmten Datenschutzniveaus sanktionierende Massnahmen folgen lassen können [Swift 2001, S. 231; S. 235 ff.]. Nach Aussagen von BÜLLESBACH folgt die DaimlerChrysler AG zumindest im Bereich von Kundendaten im Fall ungleicher nationaler Datenschutzbestimmungen den jeweils restriktiveren Bestimmungen. Da es sich um ein global tätiges Unternehmen handelt, liegt es im Bestreben des Chief Privacy Officers, die weltweit strengsten Datenschutzbestimmungen in Form sogenannter Codes of Conduct zu realisieren [Büllesbach 2001, S. 4].

4.2 Gesetzesorientierte Massnahmen zur Verbesserung des Datenschutzes im Data Warehousing

Nach der ausführlichen Beschreibung der kritischen Faktoren bezüglich der Berücksichtigung der Datenschutzbedürfnisse von Kunden im Rahmen des Data Warehousings werden im Folgenden zentrale beim 3. CC DW2-Workshop identifizierte Massnahmen dargestellt, die vor-

[4] Da das Vertragsverhältnis zwischen Mitarbeiter und Unternehmen wesentlich umfassender ist als das zwischen Kunde und Unternehmen, ist der Fall der Zweckänderung in der Verarbeitung von Mitarbeiterdaten schwerer feststellbar als in der Kundenbeziehung. Darauf deutet auch die Tatsache hin,

nehmlich eine Annäherung des Data Warehousings an ein hohes Mass an Datenschutzkonformität fokussieren.

Im Grossen und Ganzen handelt es sich dabei um gesetzlich vorgesehene Massnahmen, die dazu führen, dass Unternehmen bei ihrer Einhaltung formaljuristisch korrekt handeln. Selbstverständlich müssen die folgenden Massnahmen vielfach jedoch auch vor dem Hintergrund gesehen werden, dass sie die Handlungsfreiheit von Unternehmen bei der Verarbeitung personenbezogener Daten einschränken.

Die folgenden Unterabschnitte beziehen sich auf die einzelnen kritischen Phasen aus Abb. 4-1. Die Unterabschnitte folgen mit ihrer letzten Ziffer der Nummerierung der kritischen Phasen.

4.2.1 Datenerhebung

Direkte Datenerhebung beim Kunden bzw. Mitarbeiter

Um den Kontakt zwischen Kunden und Unternehmen datenschutzkonform zu gestalten, kann die Erhebung personenbezogener Daten auf ein Mass beschränkt werden, das den Wunsch des Kunden nach massgeschneiderten Dienstleistungen durch das Unternehmen ausreichend abbildet, jedoch nicht darüber hinausgeht. Im Hinblick auf die Erhebung von Mitarbeiterdaten sollten die entsprechenden datenschutzrechtlichen Regelungen Anwendung finden, die geprägt sind von der Orientierung am Vertragszweck und einem Interessenausgleich zwischen Mitarbeiter und Unternehmen.

Die eng damit verbundene Strategie der Datensparsamkeit und Datenvermeidung unterstützt ebenfalls die Konformität mit den einschlägigen Datenschutzgesetzen [BDSG 2001, § 3a]. Es sollte also das Bestreben des Unternehmens sein, ausschliesslich die personenbezogenen Daten zu erheben und zu speichern, die es für die Gestaltung eines Vertragsverhältnisses benötigt. Darüber hinaus sollte auf die Bedürfnisse des Kunden bzw. Mitarbeiters im Hinblick auf den Schutz seiner Privatsphäre eingegangen werden.

Hinsichtlich der Erhebung personenbezogener Daten zu Auswertungs- als auch ausschliesslich operativen Zwecken, sollte eine umfassende Aufklärung des Kunden bzw. des Mitarbeiters stattfinden [BDSG 2001, §§ 4a; 28; 33], an deren Ende sie ihre explizite Zustimmung zur Verarbeitung bestimmter personenbezogener Daten geben können. Idealerweise geht das Unternehmen bei der Erhebung von Kundendaten nach einer sogenannten „Opt-in"-Strategie vor, die es dem Kunden in jedem Einzelfall ermöglicht, der Verarbeitung seiner Daten zuzustimmen. Für die Erhebung von Mitarbeiterdaten werden zumindest in Deutschland meist

dass das Grundrecht der „informationellen Selbstbestimmung" nicht unmittelbar für das Verhältnis zwischen Arbeitgeber und Arbeitnehmer anwendbar ist [BMA 2000, S. 125].

betriebsweite Vereinbarungen zwischen dem Arbeitgeber und dem Betriebsrat getroffen [BMA 2000, S. 127].

Einen weiteren Ansatz zur Bewerkstelligung des Kundenbedürfnisses nach Schutz der Privatsphäre stellt die Implementierung von Verfahren dar, die es dem Kunden unbürokratisch ermöglichen, fehlerhafte Daten zu korrigieren [BDSG 2001, §§ 3 34; 35; DSG 1992, Art. 5; 8]. Da auch der Arbeitgeber gesetzlich verpflichtet ist, sich der Korrektheit der Daten über den Arbeitnehmer regelmässig zu vergewissern [EDSB 1994, S. 14], sind ähnliche Verfahren auch für die Einsichtnahme und Qualitätssicherung von Personalakten denkbar.

Grundlegend für die Realisierung von datenschutzfreundlichen Massnahmen ist die umfassende Sensibilisierung von Mitarbeitern, insbesondere da sie in der Phase der Datenerhebung im direkten Kontakt mit dem Kunden bzw. dem (künftigen) Mitarbeiter stehen und so das Unternehmen samt seiner Aufgeschlossenheit gegenüber dem Datenschutz repräsentieren.

Externe Datenquellen

Neben der direkten Datenerfassung beim Kunden oder Mitarbeiter selbst bezieht das Unternehmen personenbezogene Daten auch aus externen Datenquellen wie beispielsweise Adressverzeichnissen oder früheren Arbeitgebern.

In diesem Fall sollten organisatorische Regelungen gefunden werden, die den Kunden bzw. Mitarbeiterwunsch nach vertraulichem Umgang mit Daten aus externen Datenquellen sicherstellen. Gehen deren Datenfelder über einen rein listenmässigen, allgemein zugänglichen Informationsgehalt hinaus, sollten die gleichen Datenschutzgrundsätze beachtet werden wie bei der direkten Erhebung personenbezogener Daten beim Kunden. Insbesondere sollten beispielsweise die im Rahmen einer „Opt-in"-Strategie ggf. erfasssten Kundenwünsche zum Umgang mit personenbezogenen Daten, aber auch Kennzeichnungen besonders schützenswerter personenbezogener Daten von Kunden und Mitarbeitern übernommen werden.

Dienen die Daten aus externen Datenquellen nicht zur Ergänzung von Persönlichkeitsprofilen, sondern lediglich zu nicht personalisierten Analysezwecken, eignen sich an dieser Stelle eventuell Anonymisierungs- und Pseudonymisierungsverfahren [BDSG 2001, § 3]. Darüber hinaus sind neben der sparsamen Verwendung von Daten auch Massnahmen der Datenorganisation wie z. B. die Prüfung und Erfassung der Datenherkunft oder eine feldbezogene Klassifikation der Schutzbedürftigkeit denkbar.

4.2.2 Operative Datenverarbeitung

Wie in Abschnitt 4.1.2 festgestellt wurde, ist die Datenarchivierung diejenige Komponente der operativen Datenverarbeitung, der in erhöhtem Mass Beachtung im Hinblick auf die datenschutzrelevanten Kunden- und Mitarbeiterinteressen zugemessen werden sollte. Im Gegensatz zum Data Warehouse dient das Archiv lediglich der längerfristigen Aufbewahrung von u. a. personenbezogenen Daten, um beispielsweise Gewährleistungsfällen nachkommen

zu können oder Mitarbeiterzeugnisse längerfristig verfügbar zu haben. Zur Sicherstellung des elektronischen Archivs sollte neben einer fristgerechten Löschung [BDSG 2001, § 35] personenbezogener Daten dem Betroffenen auch die Möglichkeit gegeben werden, seine Daten einzusehen und sie nötigenfalls zu korrigieren [BDSG 2001, §§ 3; 34; 35; DSG 1992, Art. 5; 8]. Im Hinblick auf die Zugriffsmöglichkeiten von Mitarbeitern sollte auch für archivierte Daten ein umfassendes Autorisierungskonzept existieren, das mit dem der übrigen operativen Systeme konform ist [BDSG 2001, § 9; DSG 1992, Art. 7; VDSG 1993, Art. 9; 10].

4.2.3 Datenintegration

ETL-Phase

In der ETL-Phase des Data Warehousings findet in der Mehrheit der Fälle eine Änderung des Erhebungszwecks statt, da die Daten nicht mehr ausschliesslich zur Vertragsgestaltung, sondern integriert und beispielsweise auch zu Analyse- und insbesondere im Bereich von Kundendaten zu Marketingzwecken genutzt werden können. Um diesen Übergang gemäss den Datenschutzbedürfnissen des Kunden bzw. des Mitarbeiters zu gestalten, können operative Daten auf ihre tatsächliche Notwendigkeit [BDSG 2001, § 3a] in der Analyse- und Nutzungsphase hin überprüft sowie diesbezüglich der Wille des Kunden bzw. die Bereitschaft des Mitarbeiters oder seiner Interessenvertretung beispielsweise zur Verwendung automatisch erfasster Leistungsdaten explizit aufgegriffen werden. Zudem sollten etwaige Datenkennzeichnungen, die deren Schutzwürdigkeit abbilden, übernommen werden. Die Forderung der Datenschutzgesetze nach Korrektheit der Daten [DSG 1992, Art. 5; BDSG 2001, § 35] kann in der ETL-Phase verhältnismässig einfach realisiert werden, da dort ohnehin Datenbereinigungen und -berichtigungen durchgeführt werden [Hinrichs 2001, S. 50].

Zusätzlich kann auch an dieser Stelle über Verfahren der Anonymisierung und Pseudonymisierung nachgedacht werden, da hierdurch personenbezogene Daten soweit vom Kunden bzw. Mitarbeiter entkoppelt werden können, dass deren Bedürfnis nach Schutz der Privatsphäre genüge getan werden kann. In diesem Fall erübrigt sich die Einwilligung des Betroffenen zur analytischen Verarbeitung der personenbezogenen Daten.

Organisatorische und technische Massnahmen [BDSG 2001, § 9; DSG 1992, Art. 7; VDSG 1993, Art. 9; 10] wie Autorisierungskonzepte für die ETL-Phase oder die physische Trennung von Datenbeständen nach identifizierenden und nicht-identifizierenden personenbezogenen Daten können die Bemühungen um kunden- und mitarbeiterbedürfnisgerechten Datenschutz an dieser Stelle des Data Warehousings zudem abrunden.

Data Warehouse

Damit das Kern-Data-Warehouse, das personenbezogene Daten in integrierter Form enthalten kann, dem Interesse des Kunden bzw. den auch bei weitgehender Liberalität unaufgebbaren Rechten des Mitarbeiters an seiner Privatheit standhält, bieten sich eventuell die Anonymisie-

rung, der Einsatz umfassender Autorisierungskonzepte sowie die Möglichkeit für den Kunden bzw. Mitarbeiter zur Einsichtnahme in ihre Daten an [BDSG 2001, §§ 3; 9; 34; 35; DSG 1992, Art. 5; 7; 8; VDSG 1993, Art. 9; 10].

4.2.4 Datenanalyse

Beim Übergang der Daten vom Data Warehouse in die Data Marts stehen erneut Autorisierungskonzepte im Mittelpunkt, da sich durch die Integration und Aggregation von Daten kaum mehr Aussagen über die ursprünglichen Zugriffsberechtigungen, wie sie bei der zugrundeliegenden operativen Datenverarbeitung gelten, treffen lassen, so dass die Vertraulichkeit und Integrität von Kunden- und Mitarbeiterdaten in Frage gestellt ist.

Im Umgang mit Auswertungstechnologien sollten die Mitarbeiter besonders geschult werden, da die Auswertung von Daten normalerweise nicht Bestandteil eines allgemeinen Vertragsverhältnisses zwischen dem Unternehmen und seinen Kunden bzw. Mitarbeitern ist. Der Direktzugriff auf die Datenbestände des Data Warehouse sollte ebenso wie die Verwendung vordefinierter Reports aber auch frei formulierbarer Analysen durch exakte Autorisierungskonzepte geregelt werden, um den Persönlichkeitsschutz des einzelnen nicht ausser acht zu lassen.

Gleiches sollte für die Verarbeitung personenbezogener Daten mittels ausgereifter Analysewerkzeuge wie OLAP- oder Data Mining Tools gelten. Beispielsweise können mittels Verfahren künstlicher Intelligenz beim Einsatz von Data Mining Muster identifiziert werden, die bis zu diesem Zeitpunkt nur implizit existierende Persönlichkeitsmerkmale explizit darstellen. Aus diesem Grund sollte im Vorfeld der Anwendung von Data-Mining-Verfahren bereits die Anonymisierung personenbezogener Daten in Erwägung gezogen werden, ebenso wie ein umfassendes Autorisierungskonzept, das es Mitarbeitern gezielt ermöglicht, auf die neu generierten personenbezogenen Daten zuzugreifen.

Möglicherweise nicht im Interesse des Kunden oder Mitarbeiters ist die Rückführung von personenbezogenen Analyseergebnissen ins Data Warehouse, wo die Ergebnisse mit den zugrundeliegenden personenbezogenen Daten integriert werden, so dass zunehmend detaillierte Persönlichkeitsprofile entstehen, deren Sensibilität die bisherige Sensibilität übersteigen kann.

Aus diesem Grund sollten auch in diesem Zusammenhang organisatorische Regelungen [BDSG 2001, § 9; DSG 1992, Art. 7; VDSG 1993, Art. 9; 10] in Form von Vorschriften, Reviews und der Festlegung von Verantwortlichkeiten definiert werden, sofern der Betroffene bzw. bei Mitarbeitern oftmals die Interessenvertretung die Zustimmung zur Verwendung der personenbezogenen Daten gegeben hat.

Wie in mehreren Phasen des Data Warehousings können auch hier Anonymisierungs- und Pseudonymisierungsverfahren zweckdienlich sein, allerdings sollte auch der sparsame Um-

gang mit Daten angedacht werden. Schliesslich kann auch ein möglicher Funktionalitätsverzicht von Analysewerkzeugen in Erwägung gezogen werden, um die Bedürfnisse des einzelnen nach Schutz seiner Privatsphäre nicht ausser Acht zu lassen.

4.2.5 Datennutzung

Da der Zugriff eines Mitarbeiters auf personenbezogene Daten grundsätzlich den juristischen Sachverhalt einer Bekanntgabe darstellt, sollte sein Zugriff auf sämtliche Systeme, in denen personenbezogene Daten verarbeitet werden, durch Autorisierungskonzepte [BDSG 2001, § 9; DSG 1992, Art. 7; VDSG 1993, Art. 9; 10] reglementiert werden.

Da dem Mitarbeiter beim Umgang mit personenbezogenen Daten insgesamt eine Schlüsselrolle zukommt, sollten umfassende organisatorische Massnahmen getroffen werden, die seine Kompetenzen umfassend regeln. Insbesondere der Zugriff auf besonders schützenswerte personenbezogene Daten oder Persönlichkeitsprofile sollte nur Mitarbeitern gestattet werden, deren Aufgabenspektrum dies erfordert. Andernfalls empfiehlt es sich, die Daten zu anonymisieren bzw. zu pseudonymisieren.

In jedem Fall empfiehlt sich jedoch die regelmässige Schulung von Mitarbeitern, die mit der Verarbeitung personenbezogener Daten betraut sind, sowie deren schriftliche Verpflichtung auf den Datenschutz, wie es beispielsweise bei der Deutschen Telekom praktiziert wird [Königshofen 2002, S. 66 f.].

4.2.6 Datenweitergabe

Der Austausch von Daten mit anderen Unternehmen oder rechtlich unabhängigen Unternehmensteilen eines Konzerns sollte ebenfalls durch Organisationsvorschriften datenschutzrechtlich abgesichert werden [BDSG 2001, § 9; DSG 1992, Art. 7; VDSG 1993, Art. 9; 10]. Dies bedeutet, dass jedem Mitarbeiter sein Handlungsrahmen transparent darlegt wird, nachdem durch Schulungen eine angemessene Aufklärung stattgefunden hat.

Eine Möglichkeit zu grösserer Sorgfalt im Hinblick auf das Datenschutzbedürfnis des Kunden bzw. betroffenen Mitarbeiters stellen bei der Weitergabe personenbezogener Daten zwischen Unternehmen wiederum Verfahren der Pseudonymisierung ggf. auch der Anonymisierung [BDSG 2001, § 3] dar. Der Pseudonymisierung kann jedoch der Vorzug gegeben werden, da beispielsweise rückübermittelte Daten wieder „entschlüsselt“ werden müssen, um sie im Rahmen der Vertragserfüllung weiterzubearbeiten. Mitarbeiterdaten sollten aufgrund der besonderen Schutzpflichten des Unternehmens gegenüber dem Arbeitnehmer [BMA 2000, S. 125] nur sehr eingeschränkt weitergegeben werden.

4.2.7 Zusammenfassung

In den vorhergehenden Abschnitten wurde versucht, Massnahmen zu finden, die den Interessen des Kunden bzw. Mitarbeiters am Schutz seiner Privatsphäre an verschiedenen Stellen des Data Warehousings entgegenkommen. Da die Gefährdungen für den Datenschutz jedoch nicht isoliert betrachtet werden können und zahlreiche Massnahmen ohnehin übergreifend sind, sollten verschiedene unternehmensweite oder zumindest Business-Unit-weite Massnahmen getroffen werden, um dem Interesse des Kunden bzw. Mitarbeiters am Schutz seiner Daten in einem für das Unternehmen nützlichen Mass entgegenzukommen. Insbesondere ist an dieser Stelle ein umfassender Verfahrenskatalog zu nennen, der die tatsächliche und angestrebte Gestaltung von Vorgängen im Umgang mit personenbezogenen Daten detailliert beschreibt. Nicht zuletzt sollte ein Datenschutzbeauftragter bestellt werden, der sowohl die Interessen des Kunden bzw. der Mitarbeiter als auch die des Unternehmens ausgewogen im Auge behält.

Die in Abschnitt 4.2 beschriebenen und in Tab. 4-1 nochmals übersichtsartig aufgeführten gesetzesorientierten Massnahmen kommen vornehmlich dem in den Abschnitten 2.1.2 und 2.2.2 beschriebenen Interesse des Unternehmens an der Konformität mit der Datenschutzgesetzgebung entgegen.

Angesichts ihrer sehr eingeschränkten Durchsetzungsmöglichkeiten stellt die Datenschutzkonformität v. a. im Bereich von Kundendaten jedoch keinen besonderen wirtschaftlichen Anreiz für ein Unternehmen dar. Vielmehr ist eine dauerhafte und profitable Kundenbeziehung von wirtschaftlicher Relevanz. Diese ist jedoch von dem Interesse des Unternehmens an maximalem Wissen über den einzelnen Kunden und dessen in sich gegensätzlichem Interesse an individueller Betreuung bei gleichzeitiger Wahrung seiner Privatsphäre geprägt. Schliesslich muss davon ausgegangen werden, dass jeder Kunde frei darüber verfügen möchte, wem er welche Daten zu welchen Zwecken und für welche Dauer überlässt. Zudem ist zu erwarten, dass der Kunde den Unternehmen gegenüber aufgeschlossen und auskunftsfreudig ist, die seine persönlichen Interessen auch im Hinblick auf Wahrung seiner Privatsphäre respektieren [Swift 2001, S. 239].

Im Hinblick auf Mitarbeiterdaten ist es für das Unternehmen aufgrund der Existenz nicht gering zu schätzender arbeitnehmerseitiger Mitwirkungsrechte (vgl. Tab. 4-1) sinnvoll, im Interesse des Arbeitsfriedens auf die Datenschutzbedürfnisse der Mitarbeiter ebenfalls umfassend einzugehen. Als Verhandlungsargument des Unternehmens gegenüber dem Betriebsrat eignet sich jedoch eventuell die Notwendigkeit der Personalplanung zur nachhaltigen Sicherung des wirtschaftlichen Überlebens. Die Qualität und Fundiertheit der Personalplanung ihrerseits lässt sich durch integrierte Datensichten sowie aufwändige Analyseverfahren weiter verbessern, was durchaus im Interesse der Arbeitnehmer liegen kann, so dass diese zu einem umfassenderen Verzicht auf ihre Privatsphäre bereit sein könnten, sofern sehr exakt gefasste Rahmenbedingungen formuliert werden, die die Möglichkeiten des Arbeitgebers definieren. Ob

diese jedoch tatsächlich weiterführend sein können als die dargestellten derzeitigen Regelungen, bleibt in der Praxis zu überprüfen.

Mit vornehmlich die gesetzlichen Vorgaben fokussierenden Massnahmen wird die Zielsetzung eines echten Interessenausgleichs zwischen Unternehmen und ihren Kunden bzw. Mitarbeitern nur unvollständig erreicht. Pauschale Massnahmen wie beispielsweise die Anonymisierung vor der Ausführung von Data-Mining-Verfahren hindern das Unternehmen an seinem wirtschaftlichen Interesse der Erstellung und Ergänzung von Persönlichkeitsprofilen zum Nutzen des Kunden bzw. Mitarbeiters und des Unternehmens. Zum anderen wird der Wille all jener Kunden übergangen, die ihre personenbezogenen Daten zur Verwendung in weitgehend automatisierten Analyseverfahren zur Verfügung stellen, um durch das Unternehmen noch besser betreut zu werden. Entsprechendes gilt für diejenigen Mitarbeiter, die an einer umfassenderen Messung ihrer Arbeitsergebnisse interessiert sind, um auf diese Weise für sich und das Unternehmen wirtschaftliche Vorteile zu erlangen.

Phase	Daten-erhebung		Operative Datenverarbeitung	Daten-integration		Datenanalyse	Datennutzung	Datenweitergabe
Massnahme	Direkte Datenerhebung	Externe Datenquellen		ETL-Phase	Data Warehouse			
Datenvermeidung & Datensparsamkeit	K/M	K/M		K/M				
Zweckdefinition & -bindung	K/M	K/M						
Aufklärung & Zustimmung d. Betroff.	K/M	K/M		K/M				
Fehlerkorrektur	K/M	K/M	K/M	K/M				
Mitarbeiterschulung	K/M	K/M				K/M	K/M	K/M
Techn. & org. Massnahmen	K/M	K/M	K/M	K/M	K/M	K/M	K/M	K/M
Anonymisierung/ Pseudonymisierung		K/M		K/M	K/M	K/M	K/M	K/M
Fristgerechte Löschung			K/M					
Einsichtnahme d. Betroffenen				K/M	K/M			
Funktionalitätsverzicht						K/M		
Schriftl. Datenschutzverpflicht. d. Mitarb.							K/M	
Betriebsvereinbarung	M	M		M		M		

K: Anwendung der Massnahme im Kundendatenschutz
M: Anwendung der Massnahme im Mitarbeiterdatenschutz

Tab. 4-1: Übersicht über gesetzesorientierte Massnahmen zum Datenschutz mit Zuordnung zu den datenschutzrelevanten Phasen des Data Warehousings

4.3 Kundenbeziehungsorientierte Massnahmen zur Verbesserung des Datenschutzes im Data Warehousing

Der Persönlichkeitsschutz von Angestellten in einem Unternehmen ist rechtlich wesentlich detaillierter reglementiert ist als im Bereich des Kundendatenschutzes. Zudem haben die Arbeitnehmer im Vergleich zum Kunden relativ starke Interessenvertretungen sowohl innerhalb von Unternehmen als auch unternehmensübergreifend. Diese beiden Aspekte schränken die Gestaltungsspielräume des Arbeitgebers bei der individuellen Verarbeitung von Mitarbeiterdaten stark ein, so dass sie in diesem Abschnitt, der sich mit Konzepten beschäftigt, die in den

Mittelpunkt ihrer Datenschutzbestrebungen den Willen des Betroffenen stellen, nicht weiter verfolgt werden. Aus diesem Grund werden im Folgenden ausschliesslich Kundendaten fokussiert.

Zunächst werden die „IBM Enterprise Privacy Architecture (EPA)“ sowie deren Verfeinerung, die „Enterprise Platform for Privacy Preferences (E-P3P)“, in ihren für den Datenschutz relevanten Zügen vorgestellt [Karjoth/Schunter/Waidner 2002]. Aus Sicht eines US-amerikanischen Autors wird als zweiter Ansatz das Datenschutzmanagement im Data Warehousing nach SWIFT skizziert [Swift 2001, S. 225-293].

4.3.1 IBM Enterprise Privacy Architecture

Die IBM Privacy Architecture setzt sich zum Ziel, maximalen Nutzen aus personenbezogenen Daten für das Unternehmen zu ziehen. Zugleich soll jedoch den Forderungen der einschlägigen Datenschutzrichtlinien Rechnung getragen werden, weshalb dem Kunden weitreichende Einflussmöglichkeiten auf die Verwendung und den Umfang seiner personenbezogenen Daten gewährt werden.

Im einzelnen verfolgt die IBM Privacy Architecture folgende Zielsetzungen:

- Die gesammelten personenbezogenen Daten stellen einen erheblichen Wert für das Unternehmen dar, wie z. B. der gemeinhin übliche Adresshandel zeigt. Unternehmen sind somit an der ständigen Erhaltung und dem Ausbau dieses Werts interessiert, was durch die IBM Enterprise Privacy Architecture erreicht werden soll.
- Vor allem innerhalb weltweit tätiger Unternehmen müssen verschiedenste Datenschutzbestimmungen beachtet werden, was nach Meinung von Experten (z. B. [Büllesbach 2001]) durch internationale Datenschutzstandards realisiert werden muss. Im Zuge des weltweiten elektronischen Handels spielen angemessene elektronische Datenschutzstandards ein besondere Rolle. Aus diesem Grund soll mit Hilfe der IBM Enterprise Privacy Architecture die Verwaltung von Datenschutzregeln möglich sein.
- Durch die transparente Implementierung und Nutzung der IBM Privacy Architecture gelingt es Unternehmen, das Vertrauen des Kunden weiter für sich zu gewinnen. Jedoch sollte die Zielsetzung eines Netzwerks von Vertrauenswürdigkeit und Verlässlichkeit [Weichert 2002, S. 27] am Markt über technische Massnahmen hinaus durch die aktive Mitarbeit von Unternehmen in nationalen und internationalen Gremien [Büllesbach 2002b, S. 54] abgerundet werden.

Die IBM Privacy Architecture bietet eine unternehmensweite integrierte Plattform für das Datenschutzmanagement. Die im Folgenden beschriebene Enterprise-Privacy-Architecture-Pyramide (EPA-Pyramide) stellt die verschiedenen Ebenen des Datenschutzmanagements dar.

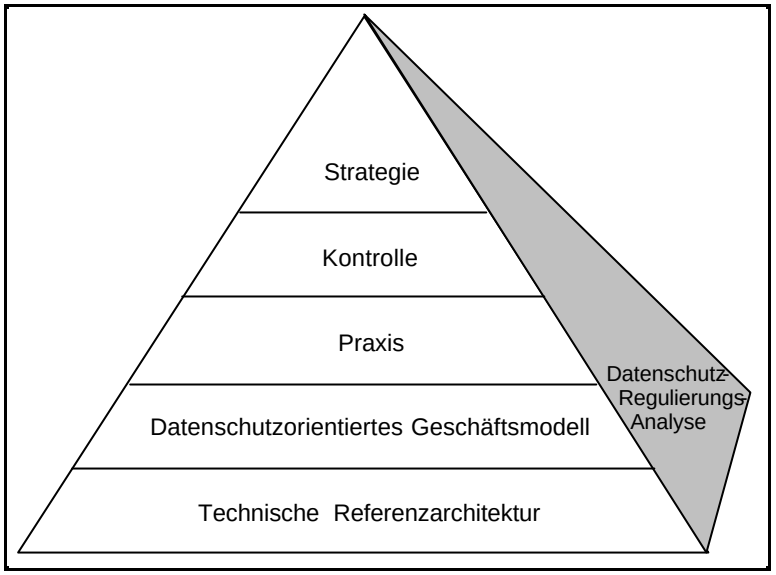

Abb. 4-2: IBM Enterprise Privacy Architecture Pyramid [Karjoth/Schunter/Waidner 2002, S. 69]

Strategie

Auf der Strategieebene werden die Philosophie, die Grundsätze sowie die anzuwendenden Bestimmungen im Hinblick auf die Datenschutz- und Sicherheitsstrategie des Unternehmens definiert.

Kontrolle

Die Kontrollebene sieht allgemeine Kontrollen zur Durchsetzung der auf der Strategieebene definierten Grundsätze vor. Ihr zentrales Element ist ein Inventar an Datenschutzanforderungen, die den gesetzlichen Bestimmungen als auch den darüber hinausgehenden Ansprüchen des Unternehmens genüge tun. Mit Hilfe von Routinen zur Kontrolle der Regelungen wird die Umsetzung der Datenschutzanforderungen forciert. Zudem können auf der Kontrollebene die berücksichtigten Datenquellen nach ihrer Sensibilität klassifiziert werden. Weitere Definitionen, die getroffen werden, sind organisatorische Rollen im Hinblick auf den Datenschutz, Verantwortungsbereiche sowie Mitarbeiterschulungsprogramme.

Praxis

Auf der Praxis-Ebene werden die definierten Datenschutzgrundsätze für die Unternehmensabläufe umgesetzt, d. h. für Verfahren, Programme und Aktivitäten. Die Gesamtheit aller Datenschutzvorgaben der einzelnen Bereiche bildet die Datenschutzdeklaration des Unternehmens gegenüber dem Kunden, für den die Praxis-Ebene schliesslich vorsieht, seine persönlichen Datenschutzpräferenzen zu bestimmen, seine Daten einzusehen und Vorgehensweisen zu definieren, die der Schlichtung von Interessenkonflikten dienen.

Datenschutzorientiertes Geschäftsmodell

Auf der Ebene des datenschutzorientierten Geschäftsmodells fokussiert das Datenschutzmanagement einzelne Geschäftsvorgänge unter Berücksichtigung der unternehmensweit deklarierten Datenschutzgrundsätze. Die berücksichtigten Geschäftsvorgänge spielen sich zwischen dem Unternehmen und seinen Kunden, seinen Mitarbeitern sowie seinen Schwesterunternehmen ab. Das datenschutzorientierte Geschäftsmodell besteht aus drei Submodellen, dem Parteien-, dem Daten- und dem Regelmodell.

Das Parteienmodell identifiziert grob den Kunden als Datensubjekt (Data Subject) sowie den Nutzer (Data User). Die Parteienmodellierung erfolgt aufgrund ihrer Komplexität objektorientiert mit Hilfe von Klassen- und Kollaborationsdiagrammen. Das Datenmodell kommt den Datenschutzanforderungen entgegen, indem personenbezogene, pseudonymisierte und anonymisierte Daten unterschieden werden. Das Regelmodell bildet schliesslich sämtliche Datenschutzgrundsätze in Regeln ab, so dass für alle Daten hinterlegt wird, welche Parteien, welche Handlungen zu welchem Zweck unter welchen Vorbedingungen und Verpflichtungen durchführen dürfen.

Technische Referenzarchitektur

Die technische Referenzarchitektur implementiert die Enterprise-Privacy-Architecture-Pyramide modellhaft (Abb. 4-3). Sie sieht hierfür drei Hauptkomponenten vor, das Policy Management System, das Privacy Enforcement System und die Audit Console. Mit Hilfe des Policy Management Systems wird die Datenschutzpolitik des Unternehmens definiert und an den Authorization Director des Privacy Enforcement Systems weitergeleitet. Das Privacy Enforcement System stellt das Kontrollsystem dar, das den Schutz der sensiblen Daten durchsetzt. Dazu überwacht es die betreffenden personenbezogene Daten verarbeitenden Applikationen mit Hilfe eines Resource Monitors, der je Transaktion den Authorization Director im Hinblick auf die Zulässigkeit der Operation konsultiert. Nur bei Zulässigkeit der Operation wird die Transaktion ausgeführt. Neben seiner Echtzeitüberwachugsfunktion speist der Resource Monitor die Audit Console mit Logfiles über die durchgeführten Transaktionen, die idealer Weise weitgehend automatisch ausgewertet werden, um Datenschutzverstösse im Nachhinein ermitteln zu können.

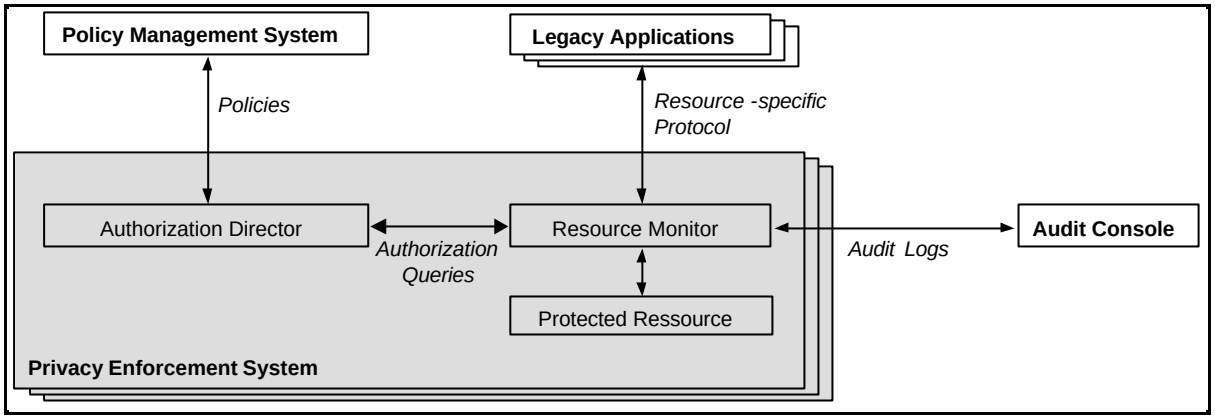

Abb. 4-3: Die Komponenten des Datenschutzsystems eines Unternehmens [Karjoth/Schunter/Waidner 2002, S. 73]

4.3.2 IBM Enterprise Platform for Privacy Preferences (E-P3P)

Die Enterprise Platform for Privacy Preferences (E-P3P) stellt eine Verfeinerung der Enterprise Privacy Architecture (siehe Abschnitt 4.3.1) dar, die in diesem Zusammenhang als Referenzarchitektur betrachtet werden kann.

Das Vorgehen von E-P3P ist zunächst die Identifikation personenbezogener Daten in den verschiedenen Systemen. Die Gesamtheit der Systeme, die personenbezogene Daten verarbeiten, stellt den Anwendungsbereich von E-P3P dar.

Anschliessend werden die durch die Datenschutzpolitik des Unternehmens gegebenen Datenschutzrichtlinien formalisiert, indem die natürlichsprachliche Beschreibung der Datenschutzpolitik neben den Bestimmungen zur Berücksichtigung von Kunden- und Unternehmensinteressen in eine maschinenlesbare Form überführt werden[5]. Schliesslich werden die Optionen zur Berücksichtigung der Kundenwünsche hinsichtlich des Persönlichkeitsschutzes formalisiert und dem Kunden zur Verfügung gestellt. Für den Datenschutzbeauftragten, aber auch den Kunden selbst, besteht darüber hinaus die Möglichkeit, die über den Kunden gespeicherten Daten sowie deren Verwendung in Form von Protokollen einzusehen.

[5] Die Datenschutzpolitik des Unternehmens lässt sich formalisiert mit der Platform for Privacy Preferences (P3P) darstellen. P3P ist der Vorschlag eines Datenschutzstandards für das World Wide Web durch das World Wide Web Consortium (W3C), bei dem die Datenschutzpolitik eines Unternehmens in XML formuliert und auf der Website publiziert werden kann. Komponenten von P3P sind ein Schema personenbezogener Daten, ein Vokabular zur Beschreibung von Datenschutzpraktiken, ein Protokoll zur Verknüpfung der XML-Syntax mit Webinhalten und schliesslich eine Präferenzsprache für die Benutzer von Webinhalten, mit deren Hilfe sie ihre persönlichen Datenschutzbedürfnisse automatisiert mit der Datenschutzpolitik des Unternehmens abgleichen können. Weitere Details zum Datenschutzstandard P3P finden sich in [Cranor et al. 2002]. Mit Hilfe von E-P3P können im Gegensatz zu P3P spezifische Datenflüsse im Unternehmen mit Blick auf den Datenschutz definiert werden [Karjoth/Schunter/Waidner 2002, S. 68].

Im Hinblick auf den Datenschutz werden drei relevante Parteien unterschieden, der Kunde, der Benutzer sowie der Datenschutzbeauftragte (Privacy Officer). Abb. 4-4 fokussiert darüber hinaus auch den Sicherheitsbeauftragten (Security Officer), dessen Verantwortung jedoch hauptsächlich im Bereich der Datensicherheit angesiedelt ist, welche nicht Gegenstand dieser Arbeit ist.

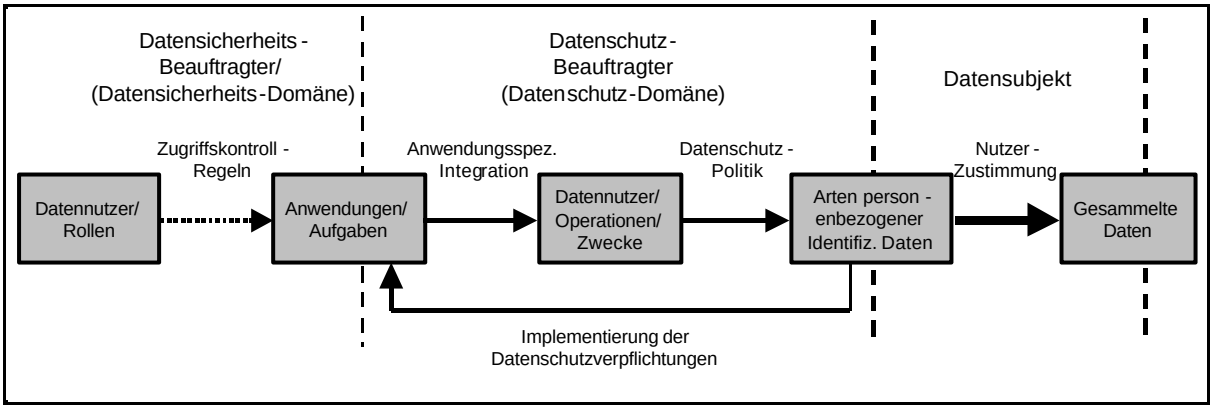

Abb. 4-4: Gewaltentrennung zwischen Sicherheits-, Datenschutzbeauftragter und Kunde [Karjoth/Schunter/Waidner 2002, S. 76]

Der Security Officer definiert für die verschiedenen Anwendungen und Aufgaben im Unternehmen gemäss der Benutzerzugriffspolitik das Autorisierungskonzept. Auf diese Weise wird exakt festgelegt, welche Mitarbeiter auf welche Daten zugreifen können. Im Bereich des Datenschutzes (Privacy Domain) definiert der Datenschutzbeauftragte die Datenschutzpolitik sowie deren anwendungsspezifische Integration (Deployment Policy). Dies bedeutet, dass das Autorisierungskonzept für die einzelnen Applikationen und Aufgaben mit der Datenschutzpolitik unter Berücksichtigung Personen identifizierender Datenfelder, in Einklang gebracht wird. D. h., dass nur diejenigen Mitarbeiter auf personenbezogene Daten zugreifen, deren Rolle vom Standpunkt der Vertraulichkeit dies vorsieht und die zudem gemäss Datenschutzpolitik dazu berechtigt sind.

Werden nun personenbezogene Daten gesammelt, so werden sie bei der Verarbeitung mittels der Applikationen und Aufgaben des Unternehmens gemäss den integrierten Datenschutzgrundsätzen sowie den individuellen Kundenwünschen behandelt.

Die Datenschutzkontrolle erfolgt durch eine Anfrage der Applikation an das Datenschutzsystem unter Angabe der beabsichtigten Operation sowie der involvierten personenbezogenen Daten. Die beabsichtigte Operation wird in der Menge der datenschutzrelevanten Operationen und Zwecke eingeordnet und schliesslich auf ihre Zulässigkeit hin geprüft.

Die Berücksichtigung der Kundenwünsche wird durch die Verwaltung der Einverständniserklärungen realisiert. Dabei wird die Zustimmung des Kunden zum Umfang der über ihn gesammelten Daten sowie zur Datenschutzpolitik im Allgemeinen verwaltet. Zudem werden seine konkreten Datenschutzbedürfnisse in Form der von ihm gewählten Optionen verwaltet.

Beispiele für derartige Optionen können das Einverständnis zur Weitergabe seiner personenbezogenen Daten oder zur Nutzung der Daten für spezielle Zwecke des Data Warehousings oder für Direktmarketingmassnahmen sein.

Insgesamt verfolgt E-P3P das sogenannte Sticky Policy Paradigm demzufolge alle Wünsche des Kunden im Hinblick auf den Schutz seiner Privatsphäre dauerhaft mit seinen personenbezogenen Daten verbunden werden. Dieser Grundsatz erstreckt sich bis einschliesslich der Weitergabe der Daten an Dritte.

Übertragen auf das Data Warehousing ist somit denkbar, die Kundenwünsche im Hinblick auf den Schutz der Privatsphäre zusammen mit den Kundendaten zu erheben und so verbunden zum gegebenen Zeitpunkt in das Data Warehouse zu überführen. In der in Abschnitt 4.1.4 geschilderten Analysephase liesse sich auf diese Weise die Übereinstimmung des Analysezwecks mit den Kundenwünschen direkt überprüfen.

Als einheitliche Datenschutzplattform führt E-P3P schliesslich eine Synchronisierung zwischen den verschiedenen erhobenen personenbezogenen Daten durch. Dies ist notwendig, wenn Daten von einem Kunden zu verschiedenen Zeitpunkten von unterschiedlichen Stellen erhoben werden, da ein und derselbe Kunde prinzipiell unterschiedliche Wünsche im Hinblick auf den Schutz seiner Privatsphäre äussern kann.

Für das Data Warehousing ist dies ebenfalls relevant, da die Daten und somit auch ihre Verwendungszwecke integriert werden und daher konsistent sein sollten.

4.3.3 Datenschutzmanagement im Data Warehousing nach SWIFT

Nach SWIFT erfolgt die Berücksichtigung des Datenschutzes im Data Warehousing mittels vier Komponenten. Zunächst muss das logische Datenmodell vollständig ausgebaut werden, um möglichst weitgehend die gesetzlichen und kundenorientierten Datenschutzanforderungen abbilden zu können. Darauf aufbauend werden sogenannte Privacy Views definiert, die den Datenschutzanforderungen entgegen kommen, die der Kunde mittels eines feingranularen Optierungssystems festlegen kann. Dritter Baustein für umfassenden Datenschutz im Data Warehousing ist nach SWIFT die Bereitstellung einer interaktiven Dienstleistungsschnittstelle, die es dem Kunden ermöglicht, auf seine personenbezogenen Daten zuzugreifen. Abgerundet wird der Datenschutz durch die Möglichkeit zur Generierung von Berichten aus Logfiles und Metadaten, mit deren Hilfe es dem Datenschutzbeauftragten ermöglicht wird, die Einhaltung der Datenschutzpolitik des Unternehmens zu überprüfen.

Ausbau des logischen Datenmodells

Zu Beginn des Ausbaus des logischen Datenmodells werden sämtliche personenbezogenen Daten identifiziert. Dabei werden folgende Daten unterschieden:

- *Identifizierende Daten*, z. B. Kundennummer, Name, Adresse und Telefonnummer,

- *Daten, die personenbezogene Informationen bereitstellen*, z. B. Alter, Geschlecht, Status, Kinderzahl, geschätztes Einkommen, Schuhgrösse, Zahlungsgewohnheiten,
- *Daten, die besonders schützenswerte Informationen abbilden*,

unterschieden.

Im Anschluss an die Identifikation personenbezogener Daten werden mögliche zusätzliche Daten ermittelt, deren Erfassung sinnvoll wäre. Z. B. könnte die o. g. Schuhgrösse um die Marke und den Typ ergänzt werden.

Um dem Datenschutz aktiv entgegenzukommen wird das nachhaltig vervollständigte logische Datenmodell um Opt-out-Spalten ergänzt, d. h. jedes Kundenprofil ggf. sogar jedes personenbezogene Datum wird um die Information ergänzt, ob der Kunde dem jeweiligen Verarbeitungszweck zustimmt oder nicht. Verarbeitungszwecke, die in einem solchen Opt-out-System erfasst werden können, sind das Einverständnis des Kunden zur Verwendung seiner personenbezogenen Daten für

- das Direktmarketing,
- automatisierte Einzelentscheidungen,
- die Verwendung besonders schützenswerter Daten,
- die Bekanntgabe seiner personenbezogenen Daten an Tochtergesellschaften sowie
- die Bekanntgabe seiner personenbezogenen Daten an sonstige Dritte.

Insbesondere im Hinblick auf das Direktmarketing sowie die Bekanntgabe von Daten sind weitere feingranulare Abstufungsschritte denkbar.

Verwendung von Anonymisierungs- und Opt-out-Verfahren sowie Datenschutz-Views zur Beschränkung des Zugriffs

Auf der Basis der als personenbezogen, besonders schützenswert bzw. als identifizierend klassifizierten Daten sowie des definierten Opt-out-Profils des Kunden können für verschiedene Benutzerklassen Views auf die Datenbestände definiert werden, die das Bedürfnis des Kunden nach Schutz seiner Privatsphäre berücksichtigen.

SWIFT unterscheidet dabei grob fünf Views. Eine grössere Vielfalt an bedarfsgerechten Views lässt sich durch die Verfeinerung des Optierungssystems erreichen.

- Standard View: Beschränkter Zugriff auf personenbezogene Daten.
- View auf personenbezogene Daten: Voller Zugriff auf personenbezogene Daten.
- Anonymisierter View: Zugriff auf anonymisierte personenbezogene Daten.
- Opt out View: Ausschliesslicher Zugriff auf Datensätze, die nicht mit Opt-out-Flag gekennzeichnet sind.

- Selektiv anonymisierter View: Zugriff auf selektiv anonymisierte personenbezogene Daten.

Neben der Klassifizierung der personenbezogenen Daten findet eine Klassifizierung der Data-Warehouse-Anwendungen statt. Dabei können grob folgende Anwendungen unterschieden werden:

- Analytische Anwendungen
- Handlungsorientierte Anwendungen (z. B. für Direktmarketing)
- Anwendungen zur Bekanntgabe personenbezogener Daten
- Spezielle administrative Anwendungen
- Sonstige Anwendungen

Für analytische Anwendungen ist nach SWIFT eine generelle Anonymisierung mittels anonymisierter Views denkbar. Für handlungsorientierte Anwendungen stellt sich die Berücksichtigung des Kundenbedürfnisses komplexer dar. So kann der Kunde beispielsweise über das Direktmarketing-opt-out veranlassen, von Direktmarketingmassnahmen ausgeschlossen zu bleiben. Darüber hinaus signalisieren jedoch auch die Opt-out-Flags, die die automatisierte Verarbeitung personenbezogener Daten oder die Verwendung besonders schützenswerter Daten ausschliessen, dass der Kunde kein Direktmarketing wünscht.

Was Anwendungen zur Bekanntgabe personenbezogener Daten angeht, so sollten die Daten laut SWIFT selektiv anonymisiert werden. Zumindest sollten aber die Opt-out-Flags berücksichtigt werden, die die Verarbeitung besonders schützenswerter personenbezogener Daten oder die Bekanntgabe beliebiger personenbezogener Daten nicht vorsehen.

Spezielle administrative Anwendungen sollten auf sämtliche personenbezogenen Daten zugreifen können, während alle anderen Anwendungen nur beschränkte Zugriffsmöglichkeiten haben sollten.

Abb. 4-5 zeigt die verschiedenen Views bzw. Bekanntgabeebenen für die verschiedenen Klassen von Anwendungen.

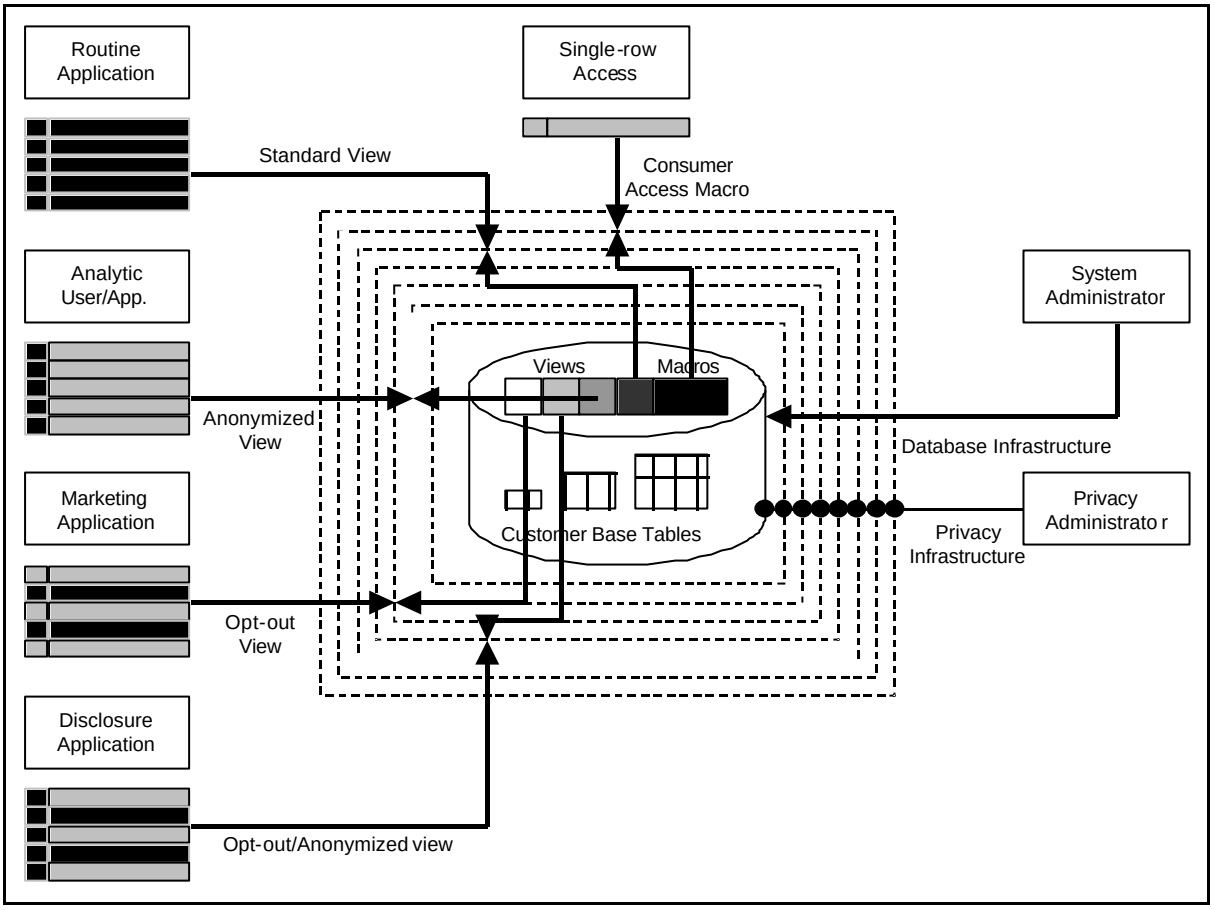

Abb. 4-5: Bereitstellung einer interaktiven Kunden Dienstleistungsschnittstelle für die persönliche Datenverwaltung

Für den Kunden sieht SWIFT eine Schnittstelle vor, über die er seine personenbezogenen Daten einsehen, aktualisieren und ggf. berichtigen kann. Zudem sollte es ihm möglich sein, über diese Schnittstelle seine Datenschutzbedürfnisse darzulegen, die dann mit Hilfe von Datenschutzregeln gemäss der Datenschutzpolitik des Unternehmens verarbeitet werden.

Generierung von Berichten aus Logfiles und Metadaten

Zur Überprüfung, ob das Unternehmen seinen Datenschutzgrundsätzen genüge tut, können Berichte über die Zugriffsaktivitäten bereitgestellt werden, die auf der Basis von Metadaten und Logfiles über die Zugriffsaktivitäten generiert werden. Die Berichte zielen meist entweder auf die Beschreibung der Datenschutzinfrastruktur des Unternehmens oder auf die Darstellung der Datenschutzbemühungen. Letztere enthalten in der Regel Hinweise auf mögliche Datenschutzverstösse. Je nach Zielsetzung sind im ersteren Details zum logischen Datenmodell, zum Datenbankschema, zu verschiedenen Datenschutzsichten und damit verbundenen Privilegien zu finden. Eine Auflistung der Anwendungen, die personenbezogene Daten verarbeiten, sowie eine Übersicht über alle Benutzer, die auf das Data Warehouse und seine peripheren Applikationen Zugriff haben, runden solche Berichte ab.

Ausser zu Zwecken der Selbstkontrolle können die Berichte auch unabhängigen Einrichtungen (TRUSTe, BBB Online, CPA WebTrust) oder Regierungsstellen zur Überprüfung und Zertifizierung vorgelegt werden, wodurch das Unternehmen ein gewisses Mass an Aussenwirkung erreichen kann.

4.3.4 Zusammenfassung

Die in Abschnitt 4.3 vorgestellten Ansätze berücksichtigen in hohem Mass die individuellen Bedürfnisse des Kunden nach dem Schutz seiner Persönlichkeit. Insbesondere wird dies durch folgende Elemente realisiert:

- *Feingranulare Optierungssysteme*: Der Kunde wählt für seine personenbezogenen Daten, insbesondere die besonders schützenswerten, aus einer Menge von Verarbeitungszwecken aus, zu welchen seine Daten durch das Unternehmen oder Dritte verarbeitet werden dürfen.
- *Maschinenlesbare Datenschutzerklärungen*: Das Unternehmen strukturiert seine natürlichsprachliche Datenschutzerklärung beispielsweise gemäss den Prinzipien einer für den Datenaustausch geeigneten Sprache wie XML[6] (Extended Markup Language). Auf diese Weise ist die Datenschutzerklärung für den Browser des sich im Web bewegenden Kunden verständlich. Formuliert der Kunde seine Datenschutzbedürfnisse ebenfalls in dieser strukturierten Form, kann die Erfassung der Datenschutzbedürfnisse des Kunden sowie deren Abgleich mit der Datenschutzpolitik des Unternehmens weitgehend automatisiert werden.
- *Kundenzugriff*: Über eine Kundenschnittstelle gibt das Unternehmen dem Kunden die Möglichkeit, auf seine personenbezogenen Daten zuzugreifen und für diese Änderungen, Sperrungen oder Löschungen durch das Unternehmen zu beantragen.

Insgesamt basieren die kundenbeziehungsorientierten Massnahmen in hohem Mass auf dem datenschutzrechtlichen Grundprinzip, dass mittels der Einwilligung des Kunden in bestimmte Verarbeitungsverfahren bezogen auf eine bestimmte Menge seiner personenbezogenen Daten, diese eine Rechtsgrundlage haben und somit zulässig sind.

Den Verfahren wohnt somit ein hohes Mass an Kundenorientierung inne, so dass die eingangs in Abschnitt 2.1.1 genannten Interessen des Kunden weitgehend erfüllt werden können. Dem gegenüber bleibt jedoch das Bestreben des Unternehmens, personenbezogene Daten weitgehend uneingeschränkt im Rahmen des Data Warehousings zu nutzen, unerfüllt.

Einzig die Möglichkeit, dass die Berücksichtigung des individuellen Kundenbedürfnisses dazu führen kann, dass der Kunde dazu neigt, dem Unternehmen auf dieser Vertrauensbasis umfassendere personenbezogene Daten zu überlassen, als er es sonst tun würde [Swift 2001,

S. 239], gibt Anlass zu der Annahme, dass Unternehmen, die auf Rechtssicherheit bedacht sind und Kundendaten ausschliesslich auf dem ordnungsgemässen und dem Willen des Kunden entsprechenden Weg erheben und verarbeiten, über eine qualitativ höherwertigere Datenbasis verfügen werden.

Zur weiteren Erhöhung der Motivation des Kunden, seine personenbezogenen Daten preiszugeben, können flankierende Anreizsysteme in Form von Werbegeschenken, finanziellen Beteiligungen an der Nutzung personenbezogener Daten o. ä. zum Einsatz kommen.

[6] Insbesondere im Zusammenhang mit dem elektronischen Datenschutzstandard P3P (Platform for Privacy Preferences) spielt die Formulierung von Datenschutzerklärungen in XML eine besondere Rolle.

5 Zusammenfassung, Fazit und Ausblick

5.1 Zusammenfassung

Ausgehend von der Erkenntnis, dass der Umgang mit personenbezogenen Daten weitreichende Konsequenzen sowohl für die Betroffenen als auch für die datenverarbeitenden Stellen haben kann, wurde die Rolle des Data Warehousings im Bereich der Verarbeitung personenbezogener Daten identifiziert. Dabei wurde festgestellt, dass bereits die Prinzipien des Data Warehousings nur eingeschränkt im Einklang mit den vielfältigen Datenschutzgesetzgebungen und -leitlinien stehen.

Da die pauschale Umsetzung von Grundprinzipien des Datenschutzes jedoch weder im Interesse der Unternehmen noch seiner Kunden bzw. Arbeitnehmer liegt, wurden die verschiedenen Interessenlagen ausgehend von der Geschäftsbeziehung zwischen Unternehmen und ihren Kunden bzw. den Rechten und Pflichten, wie sie zwischen Arbeitgeber und Arbeitnehmer bestehen, analysiert. Dabei wurden die wirtschaftlichen sowie die datenschutzorientierten Interessen von Unternehmen und ihren Kunden bzw. Arbeitgebern und ihren Angestellten gegenübergestellt.

Die Betrachtung ergab, dass die Interessenlage innerhalb der Kundschaft eines Unternehmens eine hohe Bandbreite aufweisen kann, angefangen von Kunden, die ihre Privatsphäre uneingeschränkt geschützt sehen möchten bis hin zu Kunden, die dazu neigen, ihre personenbezogenen Daten dem Unternehmen vollständig zur Verfügung zu stellen. Im Hinblick auf die Arbeitnehmer eines Unternehmens konnte festgestellt werden, dass ebenfalls nicht von einem homogenen und exklusiven Interesse der Angestellten hinsichtlich ihrer Privatsphäre am Arbeitsplatz ausgegangen werden kann. Dies ist auf das besondere Verhältnis zwischen Arbeitgeber und Arbeitnehmer zurückzuführen, das v. a. hinsichtlich der positiven wirtschaftlichen Entwicklung des Unternehmens hochgradige Synergien aufweist. Da die adäquate Einplanung von Mitarbeitern hierbei ein mitbestimmender Faktor ist, existieren durchaus – wenn auch in verschiedenem Mass je Mitarbeitergruppe – Motive seitens der Arbeitnehmer, dem Arbeitgeber weiterreichende personenbezogene Daten zur Verfügung zu stellen.

Da im CC DW2 sowohl Unternehmen aus der Schweiz als auch der Bundesrepublik Deutschland vertreten sind, wurde in Kapitel 3 ein Abgleich der Begrifflichkeiten zur Beschreibung des Umgangs mit personenbezogenen Daten zwischen den beiden Rechtsräumen vorgenommen. Dabei hat sich gezeigt, dass die Begrifflichkeiten und ihre semantischen Abhängigkeiten differieren, jedoch sämtliche Bereiche ihre jeweilige Entsprechung haben. Um die Datenschutzproblematik im Data Warehousing genauer analysieren zu können, wurden schliesslich die Grundprinzipien des Datenschutzes skizziert, die in beiden Rechtsräumen weitgehend übereinstimmen.

In Abschnitt 4.1 wurden anhand der Referenzarchitektur des Data Warehousings, wie sie im CC DW2 verwendet wird, mögliche Konflikte zwischen dem Datenschutz und der Verarbeitung personenbezogener Daten im Data Warehousing dargestellt. Diese manifestieren sich hauptsächlich in der Änderung des Vertragszwecks bei der Übernahme personenbezogener Daten aus den operativen Systemen ins Data Warehouse, um sie dort Analyseverfahren zu unterziehen, deren Zweck kaum ex ante festgelegt werden kann. Weitere zentrale Konfliktmöglichkeiten bieten die Tatsache, dass personenbezogene Daten in grossem Umfang erhoben und langfristig gespeichert werden sowie ihre Nutzung durch Mitarbeiter nicht generell auf ein Mindestmass festgelegt ist.

Die Abschnitte 4.2 und 4.3 stellen mögliche Massnahmen vor, um sich der Datenschutzkonformität im Data Warehousing mit personenbezogenen Daten zu nähern. Abschnitt 4.2 geht dabei von Massnahmen aus, die eher im formaljuristischen Sinn zu Datenschutzkonformität führen, jedoch den individuellen Grad an Datenschutz je Kunde bzw. Mitarbeiter weitgehend unberücksichtigt lassen.

Die Massnahmen in Abschnitt 4.3 stellen das Kundeninteresse in den Mittelpunkt und können somit ein Ansatz sein zur erhöhten Vertrauensbildung zwischen Kunden und Unternehmen und somit zu grösserer Bereitschaft des Kunden, seine personenbezogenen Daten für die Verarbeitung im Data Warehousing zur Verfügung zu stellen. Die Betrachtung von Mitarbeiterdaten wurde an dieser Stelle unterlassen, da die eng gefassten gesetzlichen Massnahmen zum Mitarbeiterdatenschutz kaum Spielräume zur Berücksichtigung des individuellen Mitarbeiterwillens lassen.

5.2 Fazit und Ausblick

Der vorliegende Arbeitsbericht zeigt auf, dass jegliche Massnahmen, die das Bedürfnis des Kunden bzw. Mitarbeiters nach Schutz der persönlichen Daten aufgreifen, die Möglichkeiten des Unternehmens einschränken, Data Warehousing mit personenbezogenen Daten mit einem maximalen Grad an Vollständigkeit zu betreiben. Es muss daher davon ausgegangen werden, dass Datenschutz und Data Warehousing gemeinsam nur suboptimal realisiert werden können, sofern nicht – gleich einem Kompromiss – der Wille des einzelnen Kunden bzw. Mitarbeiters in den Mittelpunkt der Verarbeitung personenbezogener Daten gestellt wird.

Dies ist im Bereich des Mitarbeiterdatenschutzes aufgrund der in Unternehmen installierten Gesamtinteressenvertretungen von Mitarbeitern kaum möglich. Aus diesem Grund sollte der Arbeitgeber in Verhandlungen mit den Arbeitnehmervertretungen grundsätzlich auf das gemeinsame Interesse am wirtschaftlichen Wohlstand des Unternehmens abheben, das u. a. durch die exakte Personalplanung auf der Basis eines umfassenden Wissens über den einzelnen Mitarbeiter realisiert werden kann.

Im Hinblick auf Kundendaten kann die generelle Bereitschaft zu Einschränkungen bei der Verarbeitung personenbezogener Daten durch Unternehmen vielfältige Gründe haben, so

z. B. die Exklusivität der Kundschaft, die Sensibilität der zu verarbeitenden Daten oder die Annahme, dass sich Datenschutz zum Wettbewerbsbestandteil weiterentwickelt. Ist diese generelle Bereitschaft gegeben, so empfiehlt es sich für Unternehmen, datenschutzfreundliche Massnahmen einzusetzen, die das individuelle Datenschutzbedürfnis des Kunden in den Mittelpunkt stellen (siehe Abschnitt 4.3).

Ob sich der Einsatz datenschutzfreundlicher Massnahmen im Data Warehousing zum oben erwähnten künftigen Wettbewerbsfaktor entwickelt und somit die datenschutzfreundlichen Massnahmen auch wirtschaftlich gerechtfertigt sind, muss die gesellschaftliche, politische und wirtschaftliche Entwicklung zeigen.

Die Betrachtung der wirtschaftlichen Entwicklung zeigt, dass bisherige Kernleistungen von Unternehmen aufgrund der technischen Entwicklung und der damit verbundenen Standardisierung zu gewöhnlichen Leistungen werden [Heinrich 2002, S. 47 ff.], so z. B. eine einem Kreditinstitut in Auftrag gegebene Überweisung oder eine Telefonverbindung durch ein Telekommunikationsunternehmen. Auf diese Weise geht das produktbezogene Differenzierungspotenzial von Unternehmen verloren [Heinrich 2002, S. 51], was durch Zusatzleistungen [Meffert/Bruhn 2000, S. 19 ff.] kompensiert werden muss. Denkbar ist, dass Datenschutz zu einer solchen Zusatzleistung und somit zum Auswahlkriterium des Kunden bei der Anbietersuche wird. Vom heutigen Standpunkt aus fehlt es an Indikatoren, die für diese Vermutung sprechen. Vielmehr überwiegt wohl die Auffassung, dass Datenschutz kaum über das nötige Potenzial verfügt, auf den Wettbewerb Einfluss zu nehmen.

Zum einen fehlt es Behörden an einer umfassenden Ausstattung, um datenschutzrechtliche Sachverhalte initial verfolgen zu können, zum anderen sind die in Abschnitt 3.5 angeführten Sanktionen wohl zu gering, als dass sie den Nutzen des Data Warehousings aufwiegen könnten.

Weitere Faktoren, die bei der Entscheidung eines Unternehmens über das adäquate Mass an datenschutzfreundlichen Massnahmen eine Rolle spielen, sind das weitgehend nicht vorhandene Bewusstsein bei Kunden und Mitarbeitern, dass gerade ihre personenbezogenen Daten – wenn auch in legaler Weise – für Direktmarketingmassnahmen oder Leistungsanalysen verwendet werden. In Fällen, wo das Bewusstsein entsprechend geschärft ist, fällt es Unternehmen jedoch nicht schwer, den Zusatznutzen, den die analytische Verarbeitung personenbezogener Daten im Allgemeinen mit sich bringt, insbesondere der Kundschaft zu kommunizieren. Auf diese Weise wird diese kaum ausschliesslich ihre Persönlichkeitsrechte fokussieren.

Nicht zuletzt wiegt sich der Kunde bzw. Mitarbeiter in der Sicherheit des Rechtsstaates, aufgrund derer er pauschal vom einwandfreien Umgang mit seinen personenbezogenen Daten sowohl durch öffentliche als auch private Stellen ausgeht. Dieser Status wird wohl anhalten, solange keine umfassend dokumentierten, das öffentliche Aufsehen erregenden Datenschutzvorfälle mit weitreichenden Konsequenzen auftreten.

Zusammenfassend erscheint es angesichts der oben geschilderten Faktoren für Unternehmen derzeit kaum angebracht, umfassend in datenschutzfreundliche Massnahmen zu investieren. Jedoch sollte die politische und gesellschaftliche Entwicklung neben der wirtschaftlichen aufmerksam beobachtet werden. Insbesondere die politische Entwicklung stellt sich derzeit als ambivalent dar. Einerseits werden Forderungen nach dem Schutz der Konsumenten lauter, was für eine Verschärfung des Datenschutzes spricht, andererseits bestehen Anzeichen, dass die Sicherheit des Staates und seiner Bürger durch Massnahmen der Überwachung und uneingeschränkten Verarbeitung personenbezogener Daten weiter verbessert werden kann. Ausschlaggebend für diese Fragestellung werden sicherlich politische Mehrheitsverhältnisse sein, die die Haltung der Gesellschaft, jedoch in letzter Konsequenz nicht die des Einzelnen, zum Schutz personenbezogener Daten widerspiegeln. Die Haltung des Einzelnen zur Verarbeitung personenbezogener Daten durch Unternehmen kann sich v. a. daran orientieren, ob es den Unternehmen gelingt, den Zusatznutzen, den die Verarbeitung personenbezogener Daten für den einzelnen Kunden stiftet, transparent darzulegen und zu kommunizieren.

Hierin kann die Wirtschaftsinformatik insbesondere im Rahmen ihrer Bemühungen um die konzeptionelle Ausgestaltung des Customer bzw. Employee Relationship Managements (CRM bzw. ERM) ihren Beitrag leisten, indem anhand von zu entwickelnden Metriken untersucht wird, inwiefern das Recht auf informationelle Selbstbestimmung ausschlaggebend für die Qualität einer Beziehung ist.

Nach WINTER [Winter 2000, S. 278] ist davon auszugehen, dass gelungene Kundenbeziehungen ohne den Schutz der Privatsphäre kaum realisierbar sind. Aufgrund des besonderen Abhängigkeitsverhältnisses zwischen Arbeitgeber und Arbeitnehmer kann diese Annahme auch auf den Arbeitnehmerdatenschutzes ausgedehnt werden.

Aus diesem Grund sollten Entwicklungen weiterverfolgt werden, wie sie in Abschnitt 4.3 dargestellt wurden. Die Ansätze der Enterprise Privacy Architecture (EPA) bzw. E-P3P von IBM oder der Ansatz zum Datenschutzmanagement im Data Warehousing nach SWIFT, wo Konzepte entwickelt werden, die Datenschutzregelungen weitgehend technisch abbilden und so zu einem hohen Mass an Automatisierung des Datenschutzes beitragen, sollten weiter verfeinert und operationalisiert werden.

Schliesslich sollte das Unternehmen im Rahmen seiner Informationslogistik bestrebt sein, Kunden- und Mitarbeiterdaten im Unternehmen redundanzfrei zu speichern und zu verarbeiten, um über geeignete Schnittstellen [Swift 2001, S. 255] dem Kunden bzw. Mitarbeiter zu jedem Zeitpunkt Einblick in seine persönlichen Daten gewähren zu können. Auf diese Weise kann der Betroffene selbständig über das Mass entscheiden, in dem er persönliche Daten dem Unternehmen zur Verfügung stellt. In Kombination mit einem entsprechenden Anreizsystem, das die Bereitstellung von persönlichen Daten honoriert, wäre dies ein wichtiger Beitrag in Richtung eines wettbewerbsorientierten Datenschutzes.

Literatur

[Amazon 2002]

Amazon.de: Ihre Privatsphäre und der Schutz Ihrer persönlichen Daten (Datenschutz), URL: http://www.amazon.de/exec/obidos/tg/browse/-/504968/ref%3Dcs%5Fnav%5Fbn%5F3%5F2/302-3693669-4319259, 22.10.2002.

[Anonymizer 2002]

Anonymizer.com: About the Standard Privacy Toolbar Settings and Features, URL: http://www.anonymizer.com/toolbar_help/about_settings.shtml, 09.09.2002.

[Arbeitskreis gegen Überwachung 2002]

Arbeitskreis gegen Überwachung Kamen: Wer sonst noch überwacht? – Überwachung durch Unternehmen, URL: http://mitglied.lycos.de/kein1984/wirtschaft.html, 31.10.2002.

[ArGV3]

Verordnung 3 zum Arbeitsgesetz (Gesundheitsvorsorge, ArGV 3) vom 18. August 1993 (Stand: 1. Februar 2000); URL: http://www.admin.ch/ch/d/sr/8/822.113.de.pdf, 30.10.2002.

[Auth/von Maur/Helfert 2002]

Auth, G.; von Maur, E.; Helfert, M.: A Model-based Software Architecture for Meta-data Management in Data Warehouse Systems, in: Proceedings of Fifth International Conference on Business Information Systems (BIS '02), Poznan, Poland, 2002, S. 34-40.

[Bach/Gronover/Schmid 2000]

Bach, V.; Gronover, S.; Schmid, R. E.: Customer Relationship Management: Der Weg zur profitablen Kundenbeziehung, in: Österle, H.; Winter, R. (Hrsg.): Business Engineering, Springer Verlag, Berlin et al., 2000.

[Baeriswyl 2001]

Baeriswyl, B.: E-Recht, in: Vorlesung „Security & E-Recht“ im SS 2001 an der Hochschule Rapperswil, URL: www.ita.hsr.ch/Downloads/unterlagen/seb/4-E-Recht.pdf, 14.08.2001.

[BDSG 2001]

Bundesdatenschutzgesetz, URL: http://jurcom5.juris.de/bundesrecht/bdsg_1990/htmltree.html, 09.09.2002.

[BetrVG 2001]

Betriebsverfassungsgesetz in der Fassung der Bekanntmachung des Gesetzes vom 25. September 2001 (BGBl. I S. 2518), geändert durch das Gesetz vom 10. Dezember 2001 (BGBl. I S. 3443), 2001, URL: http://www.bma.bund.de/doc/doc_request.cfm?D2A8C19785CA4EC8A8CE721CB2DCADAF, 29.10.2002.

[BMA 2000]

Bundesministerium für Arbeit und Sozialordnung: Übersicht über das Arbeitsrecht, Stand: 01.01.2000, URL: http://www.bma.bund.de/download/Uebersicht_Arbeitsrecht/KAP2.pdf, 29.10.2002.

[Botschaft DSG 1988]

Botschaft zum Bundesgesetz über den Datenschutz vom 23. März 1988, URL: http://www.datenschutz-zug.ch/pdf/dsg_botschaft.pdf, 22.10.2002.

[BSI 2002]

Bundesamt für Sicherheit in der Informationstechnik: M 2.8 Vergabe von Zugriffsrechten, in: Bundesamt für Sicherheit in der Informationstechnik: IT-Grundschutzhandbuch, URL: http://www.bsi.de/gshb/deutsch/m/m2008.htm, 09.09.2002.

[Büllesbach 2001]

Büllesbach, A.: Datenschutz als Wettbewerbsvorteil für Unternehmen, in: Symposium on Privacy and Security, Zürich, 2001.

[Büllesbach 2002a]

Büllesbach, A.: Datenschutz im Data Warehouse – Eine ungeliebte Fragestellung, in: Siebtes Data-Warehouse-Forum, St. Gallen, 2002.

[Büllesbach 2002b]

Büllesbach, A.: Premium Privacy, in: Bäumler, H.; von Mutius, A. (Hrsg.): Datenschutz als Wettbewerbsvorteil, Verlag Vieweg, Braunschweig, Wiesbaden, 2002, S. 45-57.

[Bundesverfassungsgericht 1983]

Bundesverfassungsgericht 65, 1: Volkszählung – Urteil des Ersten Senats vom 15. Dezember 1983 auf die mündliche Verhandlung vom 18. und 19. Oktober 1983 – 1 BvR 209, 269, 362, 420, 440, 484/83 in den Verfahren über die Verfassungsbeschwerden, URL: http://www.datenschutz-berlin.de/gesetze/sonstige/volksz.htm, 09.09.2002.

[Cranor et al. 2002]

Cranor, L.; Langheinrich, M.; Marchiori, M.; Presler-Marshall, M.; Reagle, J.: The Platform for Privacy Preferences 1.0 (P3P1.0) Specification – W3C Recommendation 16 April 2002, URL: http://www.w3.org/tr/p3p, 10.09.2002.

[Dittrich/Vavouras 2001]

Dittrich, K. R.; Vavouras, A.: Data Warehousing aus technischer Sicht, in: Baeriswyl, B.; Rudin, B.; Hämmerli, B.; Oppliger, R.; Schweizer, R. (Hrsg.): digma – Zeitschrift für Datenrecht und Informationssicherheit, Schulthess Juristische Medien AG, Zürich, 2001, S. 116-122.

[DSG 1992]

Bundesgesetz über den Datenschutz (DSG) vom 19. Juni 1992 (Stand am 7. Juli 1998).

[EDSB 1994]

Der Eidgenössische Datenschutzbeauftragte: Leitfaden für die Bearbeitung von Personendaten im Arbeitsbereich – Bearbeitung durch private Personen, Bern, 1994.

[EU-DSRL 1995]

Richtlinie 95/46/EG des Europäischen Parlaments und des Rates vom 24.10.1995 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten und zum freien Datenverkehr, URL: http://www.ad.or.at/office/recht/eu.htm, 09.09.2002.

[Forum Recht Redaktion 2001]

Forum Recht Redaktion: Überwachung in der digitalen Welt, in: Forum Recht – Das rechtspolitische Magazin für Uni und soziale Bewegungen, Freiburg, 2001, URL: http://www.forum-recht-online.de/301/301seite2.htm, 31.10.2002.

[Gentsch 2001]

Gentsch, P.: Tante Emma im Internet?, in: IT Fokus – Magazin für technisches Informationsmanagement, IT Verlag für Informationstechnik, Höhenkirchen, 2001, S. 80-84

[Grundgesetz 1994]

Grundgesetz für die Bundesrepublik Deutschland (GG) vom 23. Mai 1949 (BGBl. S. 1), URL: http://www.rewi.hu-berlin.de/jura/proj/dsi/Gesetze/gg.html, 09.09.2002.

[Helfert/Herrmann/Strauch 2001]

Helfert, M.; Herrmann, C.; Strauch, B.: Datenqualitätsmanagement – Arbeitsbericht Nr. BE HSG/CC DW2/02, Institut für Wirtschaftsinformatik, Universität St. Gallen, 2001.

[Heinrich 2002]

Heinrich, B.: Methode zur wertorientierten Analyse und Gestaltung der Kundeninteraktion – Zur Rolle des Service Integrators im Privatkundengeschäft von Kreditinstituten, Copy & Druck Shop, Augsburg, 2002

[Hinrichs 2001]

Hinrichs, H.: Transformationskomponente, in: Bauer, A.; Günzel, H.: Data Warehouse Systeme, dpunkt.verlag, Heidelberg, 2001, S. 49-50.

[Höller 2002]

Höller, R.: Vertrauen ist doch besser als Kontrolle, in: Kommunikation & Management online, Verlag für die Deutsche Wirtschaft, Bonn, 2002, URL: http://www.komma-net.de/news/archiv3.asp?DB=news6&ID=288, 02.11.2002.

[Hoess/Kloss/Sweat 2001]

Hoess, M.; Kloss, K.; Sweat, J.: Brauchen Daten Schutz?, in: Informationweek 24/2001, CMP-WEKA, Poing, 2001, URL: http://www.informationweek.de/print.php3?/channels/channel35/012416.htm, 22.10.2002

[HSID 2000]

HSID forum: Mängel bei Schufa-Einträgen, URL: http://geld.guenstiger.de/zinsen/Maengel_bei_Schufa_Eintraegen.html, 22.10.2002.

[Inmon 1996]

Inmon, W.: Building the Data Warehouse, Wiley Computer Publishing, New York, 1996.

[International Labour Office 1993]

International Labour Office: Workers privacy, Part II: Monitoring and surveillance in the workplace, Conditions of work digest, Band 12, Genf, 1993.

[Jung/Winter 2000]

Jung, R.; Winter, R.: Data Warehousing: Nutzungsaspekte, Referenzarchitektur und Vorgehensmodell, in: Jung, R.; Winter, R. (Hrsg.): Data Warehousing Strategie, Springer Verlag, Berlin et al., 2000, S. 3-20.

[Karjoth/Schunter/Waidner 2002]

Karjoth, G.; Schunter, M.; Waidner, M.: Unternehmensweites Datenschutzmanagement bei IBM, in: Bäumler, H.; von Mutius, A. (Hrsg.): Datenschutz als Wettbewerbsvorteil, Verlag Vieweg, Braunschweig, Wiesbaden 2002, S. 68-79.

[Köhntropp 2000]

Köhntropp, M.: Identitätsmanagement – Anforderungen aus Nutzersicht, in Sokol, B. (Hrsg.): Datenschutz und Anonymität, Düsseldorf 2000, S. 43-55.

[Königshofen 2002]

Königshofen, T.: Das Datenschutzkonzept der Deutschen Telekom, in: Bäumler, H.; von Mutius, A. (Hrsg.): Datenschutz als Wettbewerbsvorteil, Verlag Vieweg, Braunschweig, Wiesbaden 2002, S. 58-67.

[LDA Brandenburg 2000]

Der Landesbeauftragte für den Datenschutz Mecklenburg-Vorpommern, der Landesbeauftragte für den Datenschutz und für das Recht auf Akteneinsicht Brandenburg: Anlage 2 zu „Data-Warehouse und Datenschutz“, Schwerin; Kleinmachnow, 2000, URL: http://www.brandenburg.de/land/lfdbbg/tb_info/tb/tb9/anlage2.pdf, 28.10.2002.

[Meffert/Bruhn 2000]

Meffert, H.; Bruhn, M.: Dienstleistungsmarketing, 3. vollständig überarbeitete Auflage, Gabler, Wiesbaden, 2000.

[MWG 2000]

Bundesgesetz über die Information und Mitsprache der Arbeitnehmerinnen und Arbeitnehmer in den Betrieben (Mitwirkungsgesetz) vom 17. Dezember 1993 (Stand am 27. Juni 2000), URL: http://www.admin.ch/ch/d/sr/8/822.14.de.pdf, 02.11.2002

[OR 2002]

Bundesgesetz betreffend die Ergänzung des Schweizerischen Zivilgesetzbuches (Fünfter Teil: Obligationenrecht) vom 30. März 1911 (Stand am 25. Juni 2002), URL: http://www.admin.ch/ch/d/sr/2/220.de.pdf, 29.10.2002.

[Österle 2000]

Österle, H.: Geschäftsmodell des Informationszeitalters, in: Österle, H.; Winter, R. (Hrsg.): Business Engineering, Springer Verlag, Berlin et al., 2000, S. 21-42.

[Österle/Winter 2000]

Österle, H.; Winter, R.: Business Engineering, in: Österle, H.; Winter, R. (Hrsg.): Business Engineering, Springer Verlag, Berlin et al., 2000.

[Oppliger 1997]

Oppliger, R.: IT-Sicherheit – Grundlagen und Umsetzung in der Praxis, Verlag Vieweg, Braunschweig, Wiesbaden, 1997.

[Quadri 2001]

Quadri, P.: Privacy in a global company – a management viewpoint, in: Symposium on Privacy and Security, Zürich, 2001.

[Rossnagel/Pfitzmann/Garstka 2001]

Rossnagel, A.; Pfitzmann, A.; Garstka, H.: Modernisierung des Datenschutzrechts, Berlin, 2001, URL: http://www.bmi.bund.de/downloadde/11659/Download.pdf , 22.10.2002.

[Scheer 1998]

Scheer, A.-W.: Wirtschaftsinformatik: Referenzmodelle für industrielle Geschäftsprozesse, Studienausgbe, 2. durchges. Auflage, Springer Verlag, Berlin et al., 1998.

[Scheja 2001]

Scheja, G.: Datenschutz im Unternehmen, in: 3. CC DW2-Workshop, Augsburg, 18.-20. September 2001, Institut für Wirtschaftsinformatik, Universität St. Gallen, 2001.

[Schiek 2001]

Schiek, S.: Verdrängungsstrategie – Kameraüberwachung auf dem Vormarsch, in: Forum Recht – Das rechtspolitische Magazin für Uni und soziale Bewegungen, Freiburg, 2001, URL: http://www.forum-recht-online.de/301/301schiek.htm, 31.10.2002.

[Schmid/Bach/Österle 2000]

Schmid, R. E.; Bach, V.; Österle, H.: Mit Customer Relationship Management zum Prozessportal, in: Bach, V.; Österle, H. (Hrsg.): Customer Relationship Management in der Praxis, Springer Verlag, Berlin et al., 2000. S. 3-55.

[Schweizer 1999]

Schweizer, A.: Data Mining, Data Warehousing – Datenschutzrechtliche Orientierungshilfen für Unternehmen, Orell Füssli, 1999.

[Schweizer 2001]

Schweizer, A.: Data Mining – ein rechtliches Minenfeld, in: Baeriswyl, B.; Rudin, B.; Hämmerli, B.; Oppliger, R.; Schweizer, R. (Hrsg.): digma – Zeitschrift für Datenrecht und Informationssicherheit, Schulthess Juristische Medien AG, Zürich, 2001, S. 108-115.

[StGB 2002]

Schweizerisches Strafgesetzbuch vom 21. Dezember 1937 (Stand am 8. Oktober 2002), URL: http://www.admin.ch/ch/d/sr/3/311.0.de.pdf, 24.10.2002.

[Swift 2001]

Swift, R. S.: Accelerating Customer Relationships, Prentice Hall, Upper Saddle River, 2001.

[TDG-Germany 2002]

Die totale Überwachung auch im Büro, in: Tilly, B.: Marktanzeiger-News 21/2002, TDG-Germany, 2002, URL: http://www.marktanzeiger.de/newsletter/maznews021031.html, 02.11.2002.

[VDSG 1993]

Verordnung zum Bundesgesetz über den Datenschutz (VDSG) vom 14. Juni 1993.

[Weichert 2002]

Weichert, T.: Den Kunden im Blickfeld, in: Bäumler, H.; von Mutius, A. (Hrsg.): Datenschutz als Wettbewerbsvorteil. Verlag Vieweg, Braunschweig, Wiesbaden, 2002, S. 27-37.

[Winter 2002]

Winter R.: Ganzheitliches Kundenbeziehungsmanagement für Finanzdienstleistungen, in: Leist, S.; Winter, R. (Hrsg.): Retailbanking im Informationszeitalter, Springer Verlag, Berlin et al. 2002, S. 270-287.