Unternehmensweites Datenschutzmanagement

Günter Karjoth, Matthias Schunter und Michael Waidner
IBM Research, Forschungslaboratorium Zürich,
8803 Rüschlikon, Schweiz
{gka,mts,wmi}@zurich.ibm.com
http://www.research.ibm.com/privacy

Zusammenfassung

Die IBM Enterprise Privacy Architecture (EPA) ermöglicht Unternehmen ihren Kunden einen umfassenden und wohldefinierten Grad an Datenschutz anzubieten. EPA besteht aus den folgenden vier Grundelementen. Die Datenschutzregulierungsanalyse (privacy regulation analysis) identifiziert und strukturiert die anzuwendenden Bestimmungen. An Hand des Managementreferenzmodells kann das Unternehmen seine Datenschutzstrategie sowie die daraus resultierenden Datenschutzpratiken herleiten. Das datenschutzorientierte Geschäftmodell beschreibt eine Methodik, um Unternehmensabläufe unter Berücksichtigung von Datenschutzanforderungen neu zu strukturieren. Sie generiert ein detailliertes Modell der relevanten Parteien und Aktivitäten sowie der hierauf anzuwendenden Datenschutzpolitiken. Das vierte Element ist die technische Referenzarchitektur, welche die für die Implementierung notwendigen Technologien bereitstellt.

Die Platform for Enterprise Privacy Practices (E-P3P) stellt eine weitere Verfeinerung der technischen Referenzarchitektur dar: Unternehmen sammeln personenbezogene Daten und versprechen ihren Kunden faire Datenschutzpraktiken bei der Verarbeitung dieser Daten. Dank E-P3P können Unternehmen diese Versprechungen automatisiert durchsetzen, indem E-P3P gesammelte Daten mit der formalisierten Datenschutzpolitik, welcher der einzelne Nutzer zugestimmt hat, verknüpft.

1 Einführung

Der Schutz von Kundendaten gewinnt immer stärker an Bedeutung. Besonders im Bereich e-Commerce ist Datenschutz ein kritisches Problem. Auch im herkömmlichen Handel wächst dessen Bedeutung. Unternehmen sind sich dieser Problematik bewusst. Deshalb veröffentlichen Unternehmen Datenschutzpolitiken, welchen einen fairen Umgang mit gesammelten Daten versprechen. Trotzdem sind folgende Probleme oft ungelöst:

- Geschäftsabläufe werden ohne Berücksichtigung von Datenschutzaspekten entworfen. Als Konsequenz sammeln Unternehmen personenbezogene Daten (personally identifiable information (PII)) auf Vorrat statt nur die Daten zu erfassen, welche für einen spezifischen Geschäftsablauf nötig sind.
- Bestehende Dienste setzen eine Benutzeridentifizierung auch dann voraus, wenn die Identität des Benutzers nicht nötig wäre. Datensparsame und anonymisierende Sicherheitstechnologie wird nur selten eingesetzt.
- Unternehmen sammeln und speichern verschiedenste Arten von personenbezogenen Daten. In größeren Unternehmen besteht u.U. nur ungenügende Kenntnis darüber, welche personenbezogenen Daten gesammelt werden und wo sie gespeichert sind.
- Unter Umständen ist unbekannt, ob und welches Einverständnis zur Verwendung der Daten vom Kunden erklärt wurde. Ebenso sind die anwendbaren rechtlichen Bestimmungen oft unklar.

In Kapitel 2 stellen wir die IBM Enterprise Privacy Architecture (EPA) vor. EPA beschreibt einen Weg, welcher Unternehmen ermöglicht o.g. Probleme zu lösen. EPA ist eine Methodik mit der Unternehmen seinen Kunden einen verbesserten und wohldefinierten Grad an Datenschutz bieten kann. Es wird im Datenschutz-Consulting der IBM eingesetzt.

In Kapitel 3 wird die Platform for Enterprise Privacy Practices (E-P3P) beschrieben. E-P3P erlaubt Unternehmen Datenschutzpolitiken zu definieren, zu formalisieren, und automatisch durchzusetzen sowie die datenschutzrelevanten Einverständniserklärungen der Kunden zu verwalten.

2 IBM Enterprise Privacy Architecture

Die IBM Enterprise Privacy Architecture (EPA) ermöglicht einem Unternehmen maximalen Nutzen aus personenbezogenen Daten unter Berücksichtigung der Datenschutzbedenken der Kunden sowie der relevanten Bestimmungen zu ziehen. EPA beschreibt ein umfassendes Datenschutzmanagementsystem, welches spezifisch auf die Gesamtheit der für ein Unternehmen relevanten Datenschutzbestimmungen und -möglichkeiten zugeschnitten werden kann.

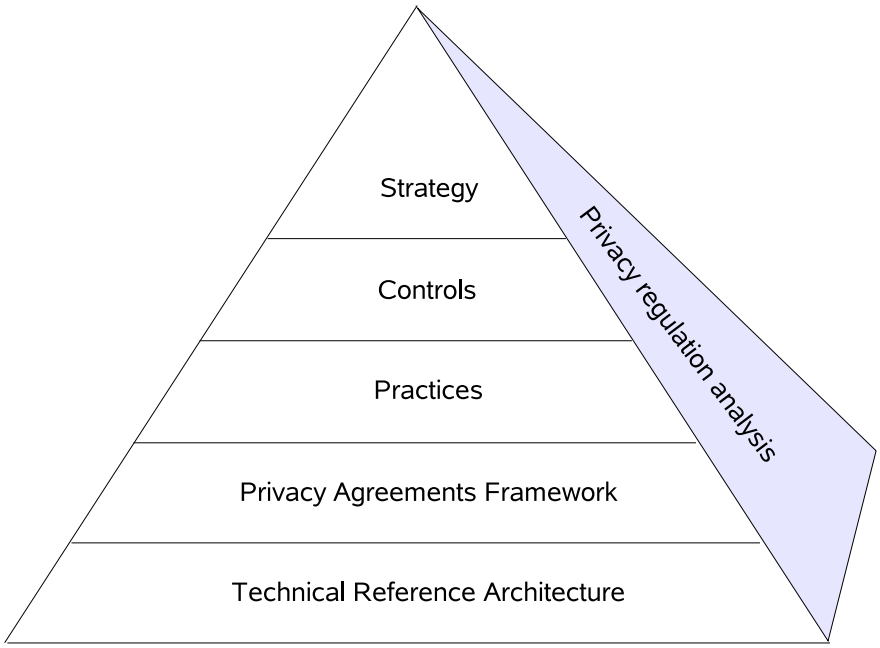

Abbildung 1. Bausteine der IBM Enterprise Privacy Architecture.

In umfassender und systematischer Weise ermöglicht EPA die Einführung und Anwendung von Datenschutzdiensten und -bewusstsein in Unternehmen. Die Spitze der EPA-Pyramide (vgl. Abb. 1) bildet das Managementreferenzmodell, welches die Datenschutzstrategien und deren Umsetzung im Unternehmen festlegt. Im datenschutzorientierten Geschäftsmodell wird beschrieben, wie Unternehmensabläufe unter Einbezug von Datenschutz restrukturiert werden können. Die unterste Ebene ist die technische Referenzarchitektur, welche die für die Umsetzung nötige Technologie zur Verfügung stellt.

Der Entwicklung von EPA lagen die folgenden Ziele zu Grunde:

- *Der Wert der Daten soll erhöht oder erhalten werden*. Das Datenmodell im technischen Referenzmodell erlaubt die Identifizierung und Katalogisierung von personenbezogenen Daten innerhalb einer Organisation und somit die Einrichtung angemessener Schutzmaßnahmen.

- *Vereinheitlichung verschiedenster Datenschutzbestimmungen und -normen*. Die Datenschutzregelanalyse unterstützt die Identifizierung der einzuhaltenden Bestimmungen und erlaubt deren einheitliche Ausformulierung. Die anwendbaren Bestimmungen werden in einer Datenschutzpolitik für das Unternehmen formalisiert, welche mit den gesammelten personenbezogenen Daten verknüpft wird

- *Aufbau und Förderung von Vertrauen am Markt*. Dank EPA behalten die Kunden die Kontrolle über ihre eigenen Daten. Das Managementreferenzmodell fördert die Sensibilisierung eines Unternehmens bezüglich der Datenschutzproblematik. Zusammen mit externen Kontrollen erhöhen diese Maßnahmen das Vertrauen der Kunden in ein Unternehmen.
- *Herausarbeitung von Gestaltungsalternativen im Bereich Datenschutzmanagement*. Die Analyse der Regeln zeigt verschiedene Alternative bezüglich deren Erfüllung auf, speziell auch hinsichtlich der Verwendung weniger sensitiver Datentypen. Des weiteren identifiziert sie Bereiche mit großem Risiko sowie datenschutzrelevante Geschäftsverbindungen.
- *Verwendung einer integren Platform für konsistentes Datenschutzmanagement*. Eine Aufgabe des Managementreferenzmodells ist es sicher zu stellen, dass Veränderungen des Umfelds kontinuierlich in das Datenschutzmanagement eines Unternehmens einfließen.

2.1.Datenschutzregelanalyse

Die Einhaltung der Bestimmungen ist eine Hauptmotivation von Datenschutzanstrengungen der Wirtschaft. Vor der Entwicklung eines Datenschutzkonzepts ist eine strukturierte Übersicht über die bestehenden Bestimmungen notwendig. Die große Herausforderung hierbei bildet die im Rechtswesen typische Sprache mit spezifischen Ausdrucksweisen und Begriffen.

EPA strukturiert die relevanten Regulierungen in zwei Tabellenarten: Die erste Tabellenart enthält einen Überblick über die relevanten Vorschriften unter Verwendung einheitlicher Begriffe. Die zweite Tabellenart formalisiert diese in Form von Verhaltensregeln zur Verwendung gesammelter Daten. Die letzteren Tabellen sind unternehmensspezifisch und formaler als erstere. Jeder Eintrag beschreibt, welche Operationen welche Partei mit welchen Daten ausführen darf sowie welche Datenschutzbestimmungen dabei zu beachten sind. Des weiteren enthalten die Einträge entsprechende Querverweise auf die rechtlichen Bestimmungen. Hierbei werden datenschutzrelevante Geschäftsvorgänge in die Phasen Sammeln, Speichern, Bearbeiten und Verwenden untergliedert (engl. collection, retention, processing and use, oder kurz „CRPU“).

2.2.Das Managementreferenzmodell

Das EPA Managementreferenzmodell befasst sich mit den für ein umfassendes Datenschutzmanagement notwendigen Prozessen innerhalb eines Unternehmens. Diese Prozesse sind so strukturiert und vernetzt, dass sie alle Aspekte von der strategischen Übersicht bis zur Implementierung der Datenschutzmassnahmen umfassen (siehe Abbildung 1).

Die **Strategie** beschreibt die Datenschutzphilosophie, die übergeordneten Regeln und identifiziert die anwendbaren Bestimmungen. Sie stellt die höchste Ebene des Datenschutzmanagements eines Unternehmens dar und verkörpert dessen Philosophie, Grundsätze und anzuwendenden Bestimmungen. Ergebnis der Strategie sind die Datenschutz- und die Sicherheitsstrategie. Beide zusammen definieren, welche Anstrengungen ein Unternehmen bereit ist für Datenschutz und Sicherheit zu leisten.

Kontrolle definiert die allgemeinen Kontrollen, welche für das Durchsetzen der Grundsätze notwendig sind. Sie setzt sich aus folgenden Komponenten zusammen: ein Inventar der Datenschutzanforderungen, eine Klassifizierung und Kontrolle von Datenquellen, eine Routine zur Kontrolle der Einhaltung dieser Regelungen, die Definition der organisatorischen Rolle und Verantwortungsbereiche sowie ein Mitarbeiterschulungsprogramm.

In den **Praktiken** wird die Umsetzung der Grundsätze in die Unternehmensabläufe beschrieben. Hier wird das Datenschutzprogramm eines Unternehmens in die zu implentierenden Datenschutzverbindlichkeiten für Verfahren, Programme und Aktivitäten umgesetzt. Die einzelnen Komponenten sind eine Datenschutzdeklaration des Unternehmens, ein Programm, welches Kunden die Möglichkeit gibt, ihre Präferenzen (opt-in, opt-out) zu bestimmen, ein Prozess, der es Kunden erlaubt, die von ihnen vorhanden Daten einzusehen, ein Schlichtungsverfahren, ein Kommunikationsprogramm, welches die Datenschutzanstrengungen des Unternehmens extern bekannt macht, sowie Programme, welche den Zugriff auf Informationen kontrollieren, um die Daten und Ressourcen des Unternehmens zu schützen.

2.3.Das datenschutzorientierte Geschäftsmodell

Das datenschutzorientierte Geschäftsmodell (privacy agreement framework) beschreibt das Datenschutzmanagement auf Ebene der einzelnen Geschäftsvorgänge, welche personenbezogene Daten verarbeiten. Solche Vorgänge finden zwischen Kunden und dem Unternehmen, zwischen Mitarbeitenden und Abteilungen innerhalb des Unternehmens sowie mit kooperierenden Unternehmen statt. Dank diesem Modell lassen sich die zwischen den verschiedenen Parteien notwendigen Datenschutzvereinbarungen identifizieren. Die Hauptbestandteile dieses Modells sind die betroffenen Parteien, die bearbeiteten Daten und die Datenschutzregeln.

Das **Parteienmodell** beschreibt die Parteien, welche personenbezogene Daten verarbeiten. Es wird zwischen Kunde (data subject, die Personen, über die Daten gesammelt werden) und Nutzern (data user, Parteien welche diese Daten verwenden) unterschieden. Für die Beschreibung der Parteien, ihrer Datenverarbeitung sowie der Beziehungen verwendet das Par-

teienmodell eine objektorientierte Modellierung. Das Ergebnis wird in UML [1] in Form von Klassen- und Kollaborationsdiagrammen dargestellt.

Das **Datenmodell** spezifiziert die für einen Geschäftsvorgang notwendigen Daten. Zusätzlich zur Identifizierung der Felder eines Formulars klassifiziert es die Daten in mindestens drei Kategorien:

- Personenbezogene Daten stellen die kritischsten Daten dar, welche direkt einer Person zugeordnet werden können. Beispiele hierfür sind Familienname oder die Kreditkartennummer.
- Depersonalisierte Daten sind personenbezogene Daten, bei denen die identifizierende Information durch ein Pseudonym ersetzt wurde. Dadurch werden Daten unkritischer, können aber nach Verarbeitung wieder repersonalisiert werden, indem das Pseudonym durch die entsprechenden Daten ersetzt wird. Ein Beispiel für De- und Repersonalisierung ist die Bestellverarbeitung nach Kundennummer.
- Anonymisierte Daten enthalten weder Identifizierungsinformationen noch Pseudonyme. Somit stellen sie die unkritischste Kategorie dar. Daten werden dann als anonymisiert betrachtet, wenn aus ihnen grundsätzlich kein Rückschluss auf die Identität des Kunden mehr gezogen werden können. Beispiele hierzu sind der Wohnort oder die alleinige Altersangabe, d.h. ohne weitere Angaben, welche Rückschlüsse auf die Identität der Person ermöglichen würden.

Im **Regelmodell** werden die Regeln erfasst, welche die Nutzung von Daten durch die Parteien und die erlaubten Handlungen festlegen. Also, welche Handlungen vom für welchen Zweck vorgenommen werden dürfen. Zusätzlich können Regeln auch Vorbedingungen sowie aus einem Zugriff resultierende Verpflichtungen festlegen. Beispiele für Vorbedingung und Verpflichtung sind, dass Daten nur gelesen werden dürfen, falls der Kunde volljährig ist und dass der Kunde nach einem Zugriff von diesem Zugriff in Kenntnis gesetzt werden muss.

2.4.Technische Referenzarchitektur

Um sicher zu stellen, dass ein Unternehmen seinen Kunden einen adäquaten Datenschutz gewährt, muss Datenschutz unternehmensweit umgesetzt werden. Bei jeder Verwendung von personenbezogenen Daten muss das Einhalten der vereinbarten Bestimmungen gesichert sein. Die Datenschutzsysteme eines Unternehmens bestehenaus mindestens drei Komponenten (siehe Abbildung 2).

Abbildung 2: Die Komponenten des Datenschutzsystems eines Unternehmens.

Mittels dem **policy management system** kann der Administrator die Datenschutzpolitik definieren, ändern und anpassen. Gleichzeitig verteilt es die relevanten Bestimmungen an das Kontrollsystem.

Das **privacy enforcement system** erzwingt den Schutz sensitiver Daten bei jeder Operation. Es erhält die anzuwendenden Datenschutzbestimmungen vom policy management system und sendet Logfiles an die audit console. Normalerweise besteht es neben dem zu schützenden System aus zwei Teilen:

Jedes zu schützende System (Datenbank, CRM-System, etc.) benützt einen entsprechenden systemspezifischen **resource monitor**, welcher das System vor unberechtigten Zugriffen abschirmt. Jede ankommende Anfrage wird in eine Anfrage an den authorization director umgewandelt. Dieser systemunabhängige authorization director wertet die gegebene Datenschutzpolitik aus und entscheidet, ob ein Operation gewährt wird oder nicht. Nur wenn dieser den Vorgang genehmigt, wird die Anfrage an das geschützte System weitergeleitet. Neben der Abschirmung sendet der resource monitor Logfiles an die audit console.

Mittels der **audit console** überwacht der Datenschutzbeauftragte die Kontrolldaten in des privacy enforcement system sowie die vom policy management system verteilten Bestimmungen.

3 Die E-P3P-Plattform für datenschutzfreundliches Datenmanagement

Die Platform for Enterprise Privacy Practices (E-P3P) ist eine Verfeinerung der EPA Referenzarchitektur für unternehmensweites Datenschutzmanagement. Sie setzt die Einhaltung der unternehmensinternen Datenschutzbestimmungen durch, welche vom entsprechenden Geschäftmodell[1] abgeleitet wurden.

E-P3P besteht aus mehreren, unabhängigen Schritten:

Identifizierung von PII-Daten. Vor der Einführung eines Datenschutzanagementsystems muss ein Unternehmen ein Inventar der Systeme, die personenbezogene Daten verarbeiten, erstellen. Dieses bestimmt den Anwendungsbereich des Datenschutzmanagementsystems in einem Unternehmen und ist ein Resultat des datenschutzorientierten Geschäftsmodells.

[1] Diese Bestimmungen können mit P3P formuliert werden [2]. Man beachte, dass P3P grobkörniger als die Datenschutzpraktiken von E-P3P sind: Während z.B. P3P sagt, „wir geben keine Daten weiter," können unter E-P3P die exakten, in einem Unternehmen zugelassenen Datenflüsse definiert werden.

Formalisierung der **Datenschutzrichtlinien**. Für personenbezogene Daten erzeugt das datenschutzorientierte Geschäftsmodell eine natursprachliche Beschreibung der relevanten Datenschutzpolitik, welche sowohl die rechtlichen Bestimmungen wie auch die Erwartungen von Kunden und Unternehmen erfüllen muss (z.B. abhängig vom Verwendungszweck oder den Ort, an dem solche Daten in ein Unternehmen gelangen). Damit in E-P3P diese Politik automatisch umgesetzt werden kann, bedarf es einer Formalisierung in einer maschinenlesbaren Sprache. Den Kunden wird dann die natursprachliche Version zur Einverständniserklärung präsentiert, während die maschinenlesbare Version der automatischen Umsetzung dient.

Auflistung und Formalisierung von Optionen. Um ein möglichst breites Kundenspektrum abzudecken, kann die Datenschutzpolitik verschiedene wählbare Optionen beinhalten, welche nach der Art der erfassten Daten unterscheiden (z.B. Daten von Kindern, Erwachsenen, etc.). Dank diesen Optionen kann ein Unternehmen eine umfassende Datenschutzstrategie verfolgen und dennoch einzelne Kundenwünsche berücksichtigen.

Verwaltung der Kundeneinverständniserklärungen. Eine Datenschutzstrategie kann als ein Vertrag zwischen dem einzelnen Kunden und dem Unternehmen betrachtet werden. Somit muss der Kunde den anzuwendenden Bestimmungen inklusive der gewählten Optionen zustimmen. Die entsprechenden Einverständniserklärungen sind jeweils für jeden Kunden einzeln zu speichern.

Überprüfbarkeit. Der Umgang mit personenbezogenen Daten sollte die Datenschutzbestimmungen auf überprüfbare Art und Weise erfüllen, um spätere Überwachung durch den Datenschutzbeauftragen zu ermöglichen.

Datenschutzdienstleistungen für die Kunden. Ein korrekter Umgang mit personenbezogenen Daten umfasst auch gewisse Zusatzdienstleistungen für den Kunden, welche durch die vorhandenen Datenschutzbestimmungen gefordert werden. Ein Kunde sollte die Möglichkeit haben, die gespeicherten Daten sowie die Zugriffsprotokolle auf die Daten einzusehen und zu kontrollieren und die Daten gegebenenfalls zu aktualisieren. Zusätzlich kann ein Unternehmen auch die Möglichkeit anbieten, personenbezogene Daten zu löschen.

1.1. Regeln und Gewaltentrennung zwischen den beteiligten Parteien

In einem Unternehmen umfassen Datenschutz und Autorisierungen mindestens vier Arten von Parteien.

- **Kunden** deren personenbezogene Daten erfasst werden.
- **Benutzer** innerhalb der beteiligten Unternehmens, welche die gesammelten Daten verwenden. Diese Verwendung geschieht durch das Ausführen von Arbeitsschritten der installierten Anwendungen, welche ihrerseits auf Teilbereiche der gesammelten Daten zugreifen.

- Der **Datenschutzbeauftragte** (privacy officer oder PO) regelt den Datenschutz eines Unternehmens.
- Der **Sicherheitsbeauftragte** (security officer oder SO) regelt die Zugriffsberechtigungen eines Unternehmens.

E-P3P führt folgende Abstraktionen und die entsprechenden Teile einer Datenschutzpolitik ein (siehe Abb. 3):

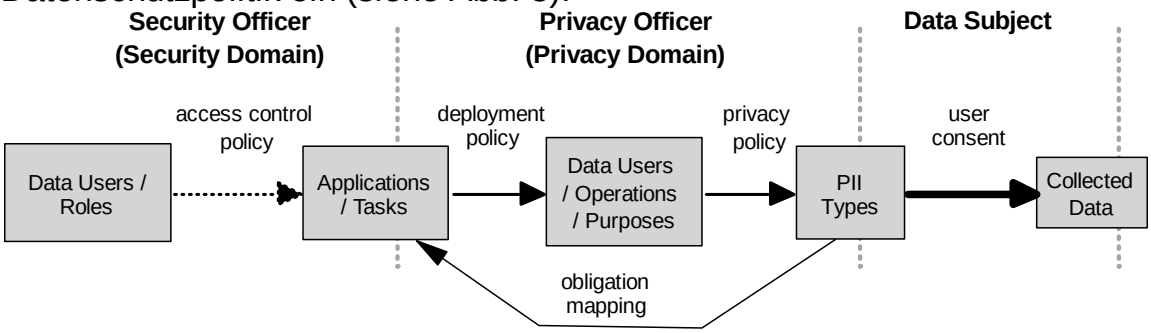

Abbildung 3: Gewaltentrennung zwischen Sicherheits-, Datenschutzbeauftragter und Kunde.

1. *Personenbezogene Daten werden in Feldern gesammelt, welche in Formularen gruppiert werden.* Ein Formular verknüpft die Felder, welche aus Kundensicht zusammengehören. So kann ein Kundenformular z.B. die Felder Name, Straße und Ort verknüpfen. Weitere Beispiele sind Formulare für bisherige Bestellungen oder für Finanzdaten.
2. *Der PO definiert die Datenschutzpolitik (privacy policy).* Die Datenschutzpolitik legt fest, welche Daten für welche Operationen von welchem Benutzer für welchen Zweck verwendet werden darf. Ein Beispiel ist „Die Abteilung für Marktforschung darf die Daten zum Zwecke des e-mail Marketings einsehen". Zudem können weitere Bedingungen und Verpflichtungen an die Datenverwendung geknüpft werden, wie z.B., dass die Daten nach 30 Tagen zu löschen sind, falls keine Zustimmung eines Elternteils vorliegt.
3. *PO und SO definieren die anwendungsspezifische Integration (deployment policy).* Diese ordnen jedem Arbeitsschritt jeder Anwendung eine datenschutzrelevante Operation und einen Zweck zu. Diese Zuordnung ist unternehmensspezifisch. So kann z.B. ein Unternehmen ein CRM-System, welches Newsletters versendet, und ein Drucker für Massensendungen die Operation „lesen" zum Zwecke der „Marktforschung“ zuordnen. Ein anderes Unternehmen verwendet eine andere Anwendung welche ebenso auf „lesen“ für „Marketing“ abgebildet wird.

4. *Der PO erzeugt einen Katalog der gesammelten Daten.* Der Katalog beinhaltet die Datenquellen und definiert für jede Quelle die erfassten Daten, deren Typ und die anzuwendende Datenschutzpolitik. Diese Informationen werden einem Formular für diese Quelle zugeordnet.
5. *Der PO beschreibt die Implementierung der Datenschutzverpflichtungen (deployment mapping).* Diese legt fest, wie Verpflichtungen bei den vorgegebenen Systemen umgesetzt werden. Die Umsetzung von „löschen“ kann bei einem CRM System bedeuten, dass der Benutzer von einer Mailingliste gelöscht wird. Bei einer Datenbank hingegen kann es sich um direktes löschen handeln.
6. *SO gibt die Zugriffskontrollregeln (access control policy) vor.* Diese Regeln definieren innerhalb eines Unternehmens die Rollen und Benutzer sowie welche Benutzer oder Funktionen welche Arbeitschritte welcher Anwendung ausführen dürfen.

Nachdem diese Vorgaben festgelegt wurden, kann ein geschütztes System (c.f. 2.4) die erfassten Daten eines Kunden speichern und verarbeiten: Der Kunde gibt die geforderten Daten in ein vorgegebenes Formular ein. Der Kunde hat die Möglichkeit vorgegebenen Optionen zu wählen und stimmt der Datenschutzpolitik mit den gewählten Optionen zu oder lehnt sie ab. Bei Zustimmung wird das Formular mit den gewählten Optionen, der Datenschutzpolitik und den Datenfelder und deren Typen für die Weiterverarbeitung gespeichert.

3.1.Erteilung oder Verweigerung der Zugriffserlaubnis

Die Entscheidung, ob ein Zugriff auf personenbezogene Daten erlaubt oder verweigert werden soll, wird mittels der im Formular enthaltenen Datenschutzpolitik gefällt. Diese Entscheidung erfolgt auf zwei Ebenen. Während die Zugriffskontrolle (engl.: access control) sich mit der Einschränkung des Zugriffs der Mitarbeiter auf Anwendungen einschränkt, beschränkt die Datenschutzkontrolle (engl.: privacy control) den Zugang einer Anwendung zu den erfassten Daten.

Zugriffskontrolle: Als Benutzer mit gewissen Rollen möchte ein Mitarbeiter einen Arbeitsschritt einer Anwendung ausführen. Mittels der Zugriffskontrollpolitik wird geprüft, ob der Benutzer oder eine dessen Rollen autorisiert ist, diesen Arbeitsschritt auszuführen. Wenn ja, wird der Arbeitsschritt der Anwendung gestartet. Diese Zugriffskontrolle ist unabhängig von der Autorisierung auf der Datenschutzebene

Datenschutzkontrolle: Verlangt ein Arbeitsschritt einer gestarteten Anwendung den Zugriff auf bestimmte Datenfelder, werden die Datenschutzregeln im entsprechenden Formular ausgewertet, um die Zugriffserlaubnis zu erteilen oder zu verweigern:

1. Das Datenschutzsystem erhält die Anfrage mit den Angaben zum gewünschten Arbeitsschritt der Anwendung und den benötigten Datenfeldern.
2. Das Datenschutzsystem ordnet dem Arbeitsschritt mittels der anwendunsspezifischen Integration eine datenschutzrelevante Operation und einem Zweck zu.
3. Aufgrund der Datenschutzpolitik und der gewählten Optionen wird entschieden, ob die gewünschte Operation zu diesem Zweck zulässig ist oder nicht. Im Falle der Nichtzulässigkeit wird der Zugriff auf diese Daten verwehrt. Wird der Zugriff zugelassen, so werden der Zugriff gewährt sowie evtl. von der Datenschutzpolitik vorgegebenen Datenschutzverpflichtungen ausgeführt.

3.2.Verwaltung von Einverständniserklärungen

Ein wichtiger Aspekt dieses Datenmanagementsystems ist die Verwaltung der Einverständniserklärungen der Kunden. Diese bestehen aus der Zustimmung zum Umfang der gesammelten Daten, der Datenschutzpolitik im Allgemeinen, wie auch den jeweiligen gewählten Optionen.

Kernstück unseres Modells ist das sog. "sticky policy paradigm": Über das Formular werden sowohl Datenschutzpolitik wie auch Optionen mit den Daten dauerhaft verknüpft. Dies gilt auch, wenn die Daten an ein anderes Unternehmen weitergegeben werden.

Man beachte, dass eine Verwaltung von Einverständniserklärungen pro Benutzer notwendig ist, wenn Daten in verschiedenen Kontexten gesammelt aber gemeinsam gespeichert werden. Beispiele hierfür sind die Verwaltung verschiedener Versionen der Datenschutzpolitik oder Benutzern aus Ländern mit unterschiedlichen Rechtssystemen, z.B. europäisches und amerikanisches Recht.

4 Danksagung

Wir bedanken uns bei Kathy Bohrer, Nigel Brown, Jan Camenisch, Calvin Powers und Els Van Herrenweghen für konstruktive Kommentare sowie bei allen Mitgliedern des EPA-Teams für ihre produktive Zusammenarbeit.

5 Literatur

[1] Grady Booch: Object Oriented Analysis and Design. Benjamin Cummings, 1994.

[2] The Platform for Privacy Preferences (P3P), W3C Candidate Recommendation, http://www.w3.org/TR/2000/CR-P3P-20001215, 2000.