Diplomarbeit

P3P und dessen Erweiterungsmöglichkeiten
-
Abgleich von Datenschutzpraktiken/ -präferenzen am Beispiel des Lufthansa AG Intranets

Bhakti Meyer
Fachbereich Informatik
Johann Wolfgang Goethe-Universität
Frankfurt am Main

01. August 2002

Erklärung

Hiermit versichere ich, dass ich die vorliegende Diplomarbeit selbständig gefertigt und keine anderen als die in der Arbeit angegebenen Hilfsmittel und Quellen verwendet habe.

Heppenheim, 01. August 2002

Vorwort

Zur Formulierung und Veröffentlichung von Datenschutzmassnahmen im Internet existieren bestimmte Tools. Mit dieser Arbeit sollte geprüft werden, inwieweit diese Hilfsmittel auch für die Nutzung bzgl. des Intranets einsetzbar sind. Dies wurde exemplarisch für das Intranet der Lufthansa AG dargestellt. Während dieser Untersuchung hat sich herausgestellt, dass es möglich ist, das exsistierende Standardvokabular durch eigene Formulierungen zu ergänzen und so das Vokabular zu erweitern und Intranet-fähig zu machen.

Es blieb zu untersuchen, wie userseitig auf diese Erweiterungen reagiert wird. Falls sie nicht verstanden würden, wäre solch eine erweiterte Formulierung nicht sinnvoll. Damit wären auch die Tools zur Veröffentlichung von Datenschutzmassnahmen, die auf das Internet abgestimmt sind, für das Lufthansa Intranet nicht anwendbar.

Herrn Dipl.-Math. Jürgen Weber der Lufthansa AG möchte ich für die Ausschreibung und Begleitung dieser interessanten Diplomarbeit danken.

Herrn Prof. Dott.-Ing. R. Zicari von der Universität Frankfurt danke ich, dass er mir die Erstellung dieser Arbeit unter seiner Professur für “Datenbanken und Informationssysteme“ ermöglicht hat. Besonderen Dank gilt hierbei Herrn Dipl.-Math. Karsten Tolle für die interessanten Diskussionen und wertvollen Anregungen.

Meinen Kindern und meinem Mann danke ich, da sie während der Abschlussphase meines Studiums besondere Entbehrungen hinnehmen mussten und mich immer wieder unterstützt haben. Desweiteren danke ich auch all denjenigen, die mir im Laufe des Studiums und während der Erstellung der Diplomarbeit immer wieder Mut und Geduld zugesprochen haben.

Inhaltsverzeichnis

Abbildungsverzeichnis

Tabellenverzeichnis

Kapitel 1

Einleitung

Web-Browser sind keine Einbahnstrassen, die nur Daten und Informationen aus dem Internet anfordern und präsentieren. Jede Nutzung des Internets löst in der Regel einen Austausch von Informationen aus, bei dem auch der Nutzer bewusst oder unbewusst Daten von sich preisgibt. So werden beim Zugriff auf einen Web-Server Informationen über den Nutzer und den angewählten Web-Seiten in Protokolldateien (Logfiles) abgelegt. Im Einzelnen können auf Web-Servern die IP-Adresse und das Betriebssystem des zugreifenden Rechners, der verwendete Browser-Typ, die URI der angeforderten Seite sowie Datum und Uhrzeit des Zugriffs festgehalten werden. Zusätzlich können Web-Server noch abfragen, von welcher Web-Seite die aktuelle Seite angefordert wurde.

Für die Web-Server ist das einzige Wiedererkennungsmerkmal eines Nutzers seine IP-Adresse. Allerdings ist die Zurückführung der IP-Adresse auf eine Person nicht ohne weiteres möglich, da sich viele Nutzer über einen Internet-Provider ins Netz einklinken und dabei jedes Mal nur eine temporäre IP-Adresse erhalten. Um weitere Informationen über ihre Besucher zu sammeln, gibt es für Web-Anbieter zum einen die Möglichkeit, die benötigten Informationen direkt vom Nutzer abzufragen, z.B. in Form eines Formulars, welches vom Nutzer selbst oder durch bereit gestellte Daten automatisch ergänzt wird, oder sie setzten die Cookie-Technik ein.

Dies kann als Grund für zunehmende Bedenken der Internet-Nutzer gegenüber diesem Medium aufgefasst werden. Durch den allgemeinen Informationsbedarf kann der Nutzer nicht mehr nachvollziehen, wer im einzelnen was, wo und wie mit seinen Daten anstellt. Abgesehen vom Risiko der Vermarktung personenbezogener Daten an Dritte besteht auch die Gefahr eines individuellen Verlustes der Privatsphäre. Angst vor Missbrauch persönlicher Daten sowie fehlendes Vertrauen im Internet-Shopping-Verfahren und Zahlungssysteme könnten sich jedoch als Hindernis für die Entwicklung des *Electronic Commerce* erweisen. Um so bedeutender ist deshalb der Datenschutz im Internet.

Seit 1997 arbeitet das *World Wide Web Consortium* (W3C) an einem offenen Standard zur Wahrung der Privatsphäre im Internet. An dieser Initiative, die unter dem Namen *Platform for Privacy Preferences Project* (P3P) läuft, beteiligten sich Firmen wie Microsoft, AT&T und IBM. Im Rahmen von P3P soll der Nutzung eines Internets-Dienstes eine Einigung über Datenschutzprinzipien zwischen Anbieter und Nutzer vorausgehen. Diensteanbieter haben

hierbei die Möglichkeit, ihre Geschäftspraktiken bzgl. personenbezogener Daten als maschinenlesbares Dokument (XML-Dokument) zu formulieren. Analog dazu kann der Web-Benutzer seine Datenschutzpräferenzen in einem XML-Dokument festlegen. Beim Besuch einer Web-Seite vergleicht der Browser des Nutzers oder ein auf dem Computer des Nutzers installierter P3P User Agent die Datenschutzpraktiken mit den Präferenzen des Nutzers. Stimmen die Praktiken mit den Präferenzen überein, so kann der Nutzer den Besuch auf der Web-Seite fortsetzten, ansonsten wird der Besuch nicht gestattet bzw. der Nutzer kann manuell in das Geschehen eingreifen und auf einer Site-by-Site Basis den Zugriff auf die nötigen Daten zum Anzeigen der Web-Seite gestatten.

Ausgangspunkt dieser Arbeit war der Web-basierte Zugriff der Lufthansa Mitarbeiter auf die erforderlichen IT-Systeme, die zur Erledigung ihrer Aufgaben notwendig sind. Die Mitarbeiter greifen dabei über Mitarbeiterportale des Inter- bzw. Intranets auf diese IT-Systeme zu. Die Nutzung dieser Systeme unterlagen bisher konzerninternen Regeln der Betriebsvereinbarungen, die sich auf Deutschland bezogen. Da jedoch auch Mitarbeiterdaten auf Servern außerhalb Deutschlands gehalten und verarbeitet werden und es so zur Vernetzung dieser verschiedenen Systeme kommt, galt es, diese zu vereinheitlichen. Dies zog nach sich, dass „Verhaltensregeln“ bzgl. der Verarbeitung von Mitarbeiterdaten aufgestellt wurden, die konzernweit gelten sollten. Diese sogenannten „Codes of Conduct“ sind verabschiedet worden. Die Lufthansa AG hat in diesem Zusammenhang sogenannte „Lufthansa Privacy Principles“ formuliert, die sich auf den Umgang und die Verarbeitung von personenbezogenen Daten beziehen. Grundlage zur Formulierung dieser Principles waren die Principles der *Organisation for Economic Co-Operation and Development* (OECD). Die OECD hat in diesem Zusammenhang einen Generator entwickelt, der bei der Formulierung von Privacy Statements behilflich sein soll, die dann als Datenschutzmassnahmen im Internet veröffentlicht werden können. Zu prüfen war, ob dieser Generator für die Formulierung von Privacy Statements für das Lufthansa Intranet benutzt werden kann oder nicht. Falls nicht sollte ursprünglich eine Anpassung des Codes erfolgen, was jedoch nicht möglich war, da der Code nur für öffentliche Stellen und nicht für Privatunternehmen zugänglich ist. Als nächstes sollte geprüft werden, ob das vom W3C entwickelte Standardvokabular in den P3P Spezifikationen ausreicht, um für das Lufthansa Intranet maschinenlesbare Datenschutzmassnahmen zu formulieren. Gleichzeitig sollten auch die sich auf dem Markt befindlichen Tools zur Erstellung des XML-Dokumentes für die Datenschutzmassnahmen auf Lufthansa-Tauglichkeit überprüft werden.

Kapitel 2 befasst sich zunächst mit dem Bundesdatenschutzgesetz (BDSG), um die grundsätzlichen Notwendigkeit von Datenschutz und den im BDSG verankerten Vorschriften hierzu aufzuzeigen. Im Anschluss werden die Arbeitsrichtlinien der Lufthansa AG, die sich auf die Verarbeitung von personenbezogenen Daten beziehen, dem BDSG gegenübergestellt.

Im dritten Kapitel werden die OECD Privacy Principles mit denen der Lufthansa AG verglichen, um den Gebrauch des OECD Privacy Statement Generators grundsätzlich zu klären. Die Benutzung des Generators wird anhand des Lufthansa Projektes „my Travel ex“ verdeutlicht. Neben der Benutzungsauswertung wird auch ein Vorschlag zur Änderung des Fragenkataloges des Generators aufgeführt, um den Generator für Intranetzwecke benutzen zu können.

Kapitel 4 behandelt die Grundlagen zur Formulierung eines maschinenlesbaren Privacy Statements. Gleichzeitig wird neben dem P3P Vokabular, das sich auf die Ausdrucksweise von Datenschutzmassnahmen bezieht, auch die Sprache eingeführt, mit der der Nutzer seine Datenschutzpräferenzen ausdrücken kann. Diese Sprache APPEL (*A P3P Preference*

Exchange Language) ist auch ein Standard des W3C, der sich allerdings noch in einem Entwurfstadium befindet. In diesem Abschnitt wird außerdem das P3P-Element „extension“ eingeführt, womit das P3P-Vokabular erweitert werden kann. Es findet auch eine userseitige Untersuchung dieses Elementes statt.

Die zur Erreichung der maschinenlesbaren Privacy Statements und Privacy Preferences auf dem Markt befindlichen Tools und ihre Funktionsweise werden in Kapitel 5 vorgestellt. Im Rahmen dieser Diplomarbeit wird anhand des P3P-Elementes „extension“ das P3P Vokabular für die Lufthansa AG beispielhaft erweitert. Im Anschluss daran werden die User Agents vorgestellt. Diese führen den Vergleich von Datenschutzpraktiken und Userpräferenzen durch. Von besonderer Bedeutung ist dabei die Handhabung eines Extensions in einer Präferenz bzw. in einem Privacy Statement durch diese User Agents.

Kapitel 6 beinhaltet einen zusammenfassenden Ausblick bzgl. der Verwendungsmöglichkeit der vorgestellten Standards und Tools für das Lufthansa Intranet.

Kapitel 2

Bundesdatenschutzgesetz (BDSG)

2.1 Die Notwendigkeit von Datenschutz

Um in der heutigen Zeit ihre Aufgaben bewältigen zu können, müssen sowohl der Staat als auch die Wirtschaft Informationen bzw. Daten über einzelne Personen sammeln, die zur Aufgabenerfüllung nicht nur gespeichert, sondern auch aufbereitet werden müssen. Dabei kann es passieren, dass der Einzelne nicht mehr nachvollziehen kann, wer wo was über ihn speichert und ggf. weiterverarbeitet, da oft die Datenerhebung in einem Hintergrundprozess abläuft. Durch den immer höher werdenden Informationsbedarf und der verschiedensten Datenzusammensetzung, die benötigt werden, kann der Einzelne leicht den Überblick verlieren, was die über ihn sich im Umlauf befindlichen Daten angeht. Er verliert nicht nur die Kontrolle über seine Daten sondern auch einen Teil seiner Selbstständigkeit und seiner Mündigkeit.

Um sowohl das Recht auf informationelle Selbstbestimmung des Einzelnen als auch dem Informationsbedarf des Staates bzw. der Wirtschaft gerecht zu werden, müssen Regelungen über den Umgang mit personenbezogenen Daten getroffen werden. Diese Regelungen sind im Bundesdatenschutzgesetz (BDSG) verankert.

Aufgabe des Datenschutzes ist es, dass der Einzelne Kontrollmöglichkeiten bekommt und unabhängige Stellen die Einhaltung der Regelungen überwachen. Gleichzeitig muss aber auch der Informationsbedarf der Wirtschaft bzw. des Staates berücksichtigt werden.

Im BDSG wird geregelt, ob und wie mit personenbezogenen Daten umgegangen werden darf. Im folgenden werden die grundlegenden Regelungen des BDSG kurz dargestellt [1].

2.2 Vorschriften des BDSG

Die einzelnen Vorschriften des BDSG umfassen folgende Bereiche:

- Zulässigkeit der Datenerhebung, -verarbeitung und -nutzung,
- die Rechte des Betroffenen,
- Durchführungs- und Sicherungspflichten der Stellen, die mit personenbezogenen Daten umgehen,
- Folgen von Gesetzesverletzungen, insbesondere Straf- und Bußgeldvorschriften und
- Kontrolle des Umgangs mit personenbezogenen Daten.

Das BDSG bezieht sich bei der Zweckdefinierung des Datenschutzes in §1 Abs. 1 BDSG auf das Grundgesetz, wonach die Würde des Menschen, und damit ist auch seine Selbstständigkeit gemeint, unantastbar ist. Gleichzeitig sollten aber auch die Gesellschaft und das Gemeinwohl beachtet werden.

In § 1 BDSG sind zunächst der Zweck und die Anwendung des Gesetzes dargelegt. Es geht dabei um den Schutz des Einzelnen vor der Beeinträchtigung des Persönlichkeitsrechts durch den Umgang mit personenbezogenen Daten.

Gibt es andere Rechtsvorschriften des Bundes bzgl. personenbezogener Daten, so gehen diese vor. Auch bleiben Geheimhaltungspflichten vom BDSG unberührt. Die Datenerhebung muss zu jeder Zeit rechtlich einwandfrei sein.

Zulässigkeit der Datenerhebung, -verarbeitung und -nutzung

Grundsätzlich ist die Verarbeitung und Nutzung personenbezogener Daten verboten, es sei denn, das BDSG bzw. eine andere Rechtsvorschrift oder der Betroffene selbst erlaubt es. Sobald eine Rechtsvorschrift vorliegt, bedarf es keiner Erlaubnis des Einzelnen (§ 4 BDSG). Bei einer Zustimmungspflicht des Einzelnen bedarf es der Schriftform. Bevor der Betroffene sein Einverständnis für den Umgang mit seinen personenbezogenen Daten gibt, muss ihm erläutert werden, welchen Umfang die Erhebung hat und was mit seinen Daten geschieht. Auf Verlangen ist auch zu erklären, was geschieht, wenn er nicht einwilligt.

Für die Erhebung gilt grundsätzlich, dass sie nach Treu und Glauben und ohne Heimlichkeit und Täuschung erfolgt. Das heißt, dass die Erhebung praktisch auf die Mitwirkung des Betroffenen angewiesen ist. Eine Nötigung zur Freigabe von Daten ist nicht erlaubt.

Bzgl. des Speicherns, Veränderns und Übermittelns erlaubt der BDSG es in folgenden Bereichen:

1) Es besteht ein Vertrags- oder Vertrauensverhältnis mit Zweckbestimmung der Daten mit dem Betroffenen.

2) Die Erforderlichkeit der speichernden Stelle steht fest, bzw. es besteht kein schutzwürdiges Interesse des Betroffenen an der Verweigerung zur Nutzung und Verarbeitung seiner Daten.

3) Die Daten stammen aus allgemeinzugänglichen Quellen.

4) Die wissenschaftlichen Zwecke überwiegen.

Die Übermittlung und Nutzung ist zulässig, falls:

- es zur Wahrung der Interessen Dritter erforderlich ist bzw. ein öffentliches Interesse vorliegt,
- es sich um in Listen zusammengefasste Daten über eine Personengruppe handelt und die Angaben auf folgendes beschränken sind:
    - Gruppenzugehörigkeit des Betroffenen
    - Name
    - Titel
    - Akademischer Grad
    - Anschrift
    - Geburtsjahr

(§ 28 BDSG).

Geschäftsmäßiges Speichern zum Zwecke der Übermittlung ist dann zulässig, wenn:

- kein schutzwürdiges Interesse bzgl. des Betroffenen besteht,
- die Daten aus allgemeinzugänglichen Quellen stammen.

Die Übermittlung ist zulässig, falls:

- der Empfänger glaubhaft machen kann, dass er berechtigtes Interesse an den Daten hat,
- es sich um in Listen zusammengefasste Daten zwecks Werbung oder Markt- und Meinungsforschung handelt,
- kein schutzwürdiges Interesse bzgl. des Betroffenen besteht.

Eine geschäftsmäßige Datenspeicherung zum Zwecke der Übermittlung in anonymisierter Form ist zulässig, wenn

- die Identifikationsmerkmale gesondert gespeichert werden,
- kein schutzwürdiges Interesse bzgl. des Betroffenen besteht,
- die Daten aus allgemeinzugänglichen Quellen stammen.

Die Daten müssen gelöscht werden, wenn

- die Speicherung unzulässig ist, etwa weil schon die Erhebung unzulässig war, oder
- es sich um Daten über gesundheitliche Verhältnisse, strafbare Handlungen, Ordnungswidrigkeiten sowie religiöse oder politische Anschauungen handelt und die speichernde Stelle deren Richtigkeit nicht beweisen kann, oder
- geschäftsmäßig zum Zweck der Übermittlung verarbeitete Daten aufgrund einer am Ende des fünften Kalenderjahres nach der ersten Speicherung vorzunehmenden Prüfung nicht mehr erforderlich sind.

Daten sind zu Sperren, wenn einer Löschung besondere Gründe entgegenstehen, wie etwa:

- gesetzlich, satzungsmäßig oder vertraglich festgelegte Aufbewahrungsfristen,
- schutzwürdige Interessen des Betroffenen, oder
- ein unverhältnismäßig hoher Aufwand wegen der besonderen Art der Speicherung.

In § 5 BDSG wird festgelegt, dass es Personen, die in der Datenverarbeitung beschäftigt sind, untersagt ist, unbefugt personenbezogene Daten zu verarbeiten oder zu nutzen. Diese Personen sind auf das Datengeheimnis zu verpflichten. Diese Pflicht besteht auch noch nach dem Ausscheiden aus dem Unternehmen.

Unabdingbare Rechte des Betroffenen

Jeder hat grundsätzlich das Recht auf Auskunft, Berichtigung, Löschung oder Sperrung bzgl. der über ihn gespeicherten Daten (§ 6 BDSG).

Er kann verlangen, dass ihm mitgeteilt wird, welche Daten zu welchem Zweck gespeichert werden und an wen sie ggf. regelmäßig übermittelt werden. Er muss dabei seine Anfrage gezielt stellen und sich legitimieren. Diese Auskunft ist grundsätzlich kostenlos, es sei denn, der Arbeitsaufwand übersteigt das Normalmass.

Die Auskunft kann verweigert werden, wenn es keine Benachrichtigungspflicht gibt. Dies bedarf dann jedoch einer Begründung. Bei Teilauskünften muss darauf hingewiesen werden, dass die Angaben unvollständig sind.

Benachrichtigungspflicht besteht bei der erstmaligen Speicherung bzw. Übermittlung. Dabei ist anzugeben, um welche Daten und um welchen Zweck es sich handelt. Der Betroffene braucht nicht benachrichtigt werden, falls

- er schon von woanders über die Speicherung und Übermittlung seiner Daten erfahren hat,
- die Löschung wegen gesetzlicher, satzungsmäßiger oder vertraglicher Vorschriften nicht möglich ist,
- es sich um eine vorübergehende Speicherung handelt und die Löschung innerhalb von drei Monaten erfolgt.

Klagt ein Betroffener auf Schadensersatz, weil ihm seiner Meinung nach durch die Speicherung seiner Daten Schaden entstanden ist, so liegt die Beweislast bei der speichernden Stelle, d. h. sie muss beweisen, dass sie unschuldig am Schaden des Betroffenen ist. Kann sie dieses nicht, so haftet sie (§ 8 BDSG).

Der Betroffene kann sich an die Aufsichtsbehörde des jeweiligen Landes, in dem sich der Firmensitz befindet, wenden. Diese geht dann dem Sachverhalt nach und unterrichtet den Betroffenen vom Ergebnis.

Durchführungs- und Sicherungspflichten der Stellen, die mit personenbezogenen Daten umgehen

Um die Erfüllung des Gesetzes zu gewährleisten, wird in § 9 BDSG darauf hingewiesen, dass diesbezüglich technische und organisatorische Maßnahmen ergriffen werden müssen, soweit ihr Aufwand im angemessenen Verhältnis zum Schutzzweck ist.

Die Einrichtung eines automatisierten Verfahrens zum Abruf personenbezogener Daten ist zulässig, solang das Verfahren für beide Seiten – Betroffeneninteresse und Geschäftszweck – angemessen ist. Dabei muss gewährleistet werden, dass die Zulässigkeit des Abrufverfahrens kontrolliert werden kann. Dazu muss folgendes schriftlich festgelegt werden:

- Anlass und Zweck des Abrufverfahrens,
- Datenempfänger,
- Art der zu übermittelnden Daten,
- nach § 9 erforderliche technische und organisatorische Maßnahmen (§ 10 BDSG).

Die Verantwortung bzgl. der Zulässigkeit des Abrufs trägt dabei der Empfänger. Diese Bestimmungen gelten allerdings nur für nicht-allgemeinzugängliche Datenbestände.

Bei der Verarbeitung an anderer Stelle ist der Auftraggeber für die Einhaltung des Gesetzes verantwortlich.

Ab 5 Mitarbeitern besteht die Pflicht zur Bestellung eines Datenschutzbeauftragten innerhalb eines Monats nach Aufnahme der Tätigkeit. Er muss direkt der Leitung unterstellt sein und besitzt Weisungsfreiheit. Aufgabe des Datenschutzbeauftragten ist es, die Einhaltung des BDSG und anderer Datenschutzvorschriften zu überwachen. Schwerpunkte sind dabei:

- Zulässigkeit des Umgangs mit Daten,
- Überwachung der ordnungsgemäßen Programmanwendung,
- Unterrichtung von Mitarbeitern über die Anforderungen des Datenschutzes.

Dabei muss ihm eine Übersicht der Daten und auch der eingesetzten Datenverarbeitungsanlagen zur Verfügung gestellt werden. Auch in jeder anderen Hinsicht muss er unterstützt werden. Es müssen technische und organisatorische Massnahmen getroffen werden, die zur Ausführung der Vorschriften des Gesetzes erforderlich sind.

Die Massnahmen müssen z. B. geeignet sein, um

- Unbefugten den Zugang zu Datenversarbeitungsanlagen zu verwehren (Zugangskontrolle),
- zu verhindern, dass Datenträger unbefugt gelesen, kopiert, verändert oder entfernt werden können (Datenträgerkontrolle),
- eine unbefugte Dateneingabe zu verhindern (Speicherkontrolle),
- eine Benutzerkontrolle zu gewährleisten,
- eine Zugriffskontrolle zu ermöglichen,
- eine Übermittlungskontrolle durchzuführen,
- eine Eingabekontrolle zu machen,
- eine Auftragskontrolle zu unterstützen,
- eine Transportkontrolle zu bestehen,
- die behördliche oder innerbetriebliche Organisation so zu gestalten, dass sie den besonderen Anforderungen des Datenschutzes gerecht wird (Organisationskontrolle).

2.3 Arbeitsrichtlinien der Lufthansa AG von 1995

In ihrer Arbeitsrichtlinie von 1995 hat die Lufthansa AG Massnahmen festgelegt, wie Personen, die personenbezogene Daten verarbeiten, mit diesen umzugehen haben. Grundlage der Arbeitsrichtlinie ist dabei das BDSG.

Zweck der Richtlinie ist es die Vorschriften des BDSG einheitlich in die Praxis umzusetzen und zu gewährleisten, dass sie eingehalten werden. Verantwortlich für die Umsetzung und Einhaltung der Richtlinie sind dabei die Führungskräfte der Abteilungen, in denen

personenbezogene Daten verarbeitet oder genutzt werden. Verbindlich ist sie außerdem auch für den Konzern-Datenschutzbeauftragten und für alle Organisationseinheiten, die ihn zur Erfüllung seiner Aufgaben unterstützen.

Da die Einhaltung und Umsetzung des BDSG und des Bundesverfassungsgerichtes sehr komplex ist, arbeitet der Konzern-Datenschutzbeauftragte mit verschiedenen Abteilungen und Organisationseinheiten zusammen. Er hat dabei ein Informationsrecht hinsichtlich der datenschutzrelevanten Systeme, Planung/Projekte und Vorkommnisse. Dies entspricht einer Informationspflicht der Geschäftsfelder, Fachbereiche und Zentralstellen.

Um seine Aufgaben zu erfüllen, hat der DS-Beauftragte ein vollständiges Zugriffs- und Nutzungsrecht in Bezug auf Dateien.

Zu den Aufgaben des DS-Beauftragten zählen:

- Beratung bei Personalauswahl
- Initiierung von Datenschutz-Schulungen
- Koordination von Auskünften und Massnahmen, die eingeleitet werden müssen, falls Anfragen von Behörden vorliegen,
- Ausarbeitung neuer Richtlinien,
- Prüfungspflicht (Stichproben) auf Einhaltung der Richtlinien.

Er ist zu informieren über:

- Neugestaltung, Übernahme oder Änderung bestehender Datenverarbeitungsaufgaben,
- bauliche und organisatorische Veränderungen,
- Systemfehler oder -störungen und
- Datenschutz- und Datensicherungsverstöße von Mitarbeitern.

Es existieren diverse Organisationseinheiten die den Konzern-Datenschutzbeauftragten auf verschiedene Weise unterstützen:

Organisationseinheit	**Aufgaben**
Personaldateninspektion	Überwachung der Durchführung und Einhaltung der Betriebsvereinbarungen für die automatisierte Verarbeitung personenbezogener Daten
Konzernrevision	Prüfung der ordnungsgemäßen Anwendung der Richtlinien sowie die Einhaltung der gesetzlichen Regeln zum Datenschutz
Rechtsabteilung	Ansprechpartner bei Rechtsfragen
Personalliniendienste	Unterstützung der Organisationseinheiten/Projekte bei der Durchführung ihrer datenschutzrelevanten Aufgaben
Lokales Informationsmanagement	Unterstützung bei bereichsspezifischen Realisierung des Datenschutzes
Bereich Informatik	Hilfestellung insbesondere bei der Planung und Implementierung von Datensicherungs-massnahmen
Werkschutz	Schutz und Sicherung datenschutzrelevanter Objekte

Tabelle 2.1: Unterstützung des DS-Beauftragten durch die Organisationseinheiten

Um den Datenschutz realisieren zu können, hat die Lufthansa AG für folgende Bereiche in ihrer Arbeitsrichtlinie Pflichten und Verfahren zur Erfüllung der gesetzlichen Vorschriften entwickelt:

- Zulässigkeitsprüfung von Vorhaben zur Verarbeitung oder Nutzung personenbezogener Daten,
- Datensicherung,
- Dokumentation,
- Rechte des Betroffenen,
- Verpflichtung auf das Datengeheimnis,
- Schulung und
- Regelung von Sonderfällen.

Damit kommt sie ihren Pflichten gegenüber dem Gesetz nach.

2.4 Zusammenfassung & Gegenüberstellung

Neben den im Gesetz geforderten Pflichten und Massnahmen hat die Lufthansa AG in der Betriebsvereinbarung für Bodenpersonal Deutschland noch zusätzliche Vorschriften eingebracht. Diese sind:

1) Klassifizierung der EDV-Anwendungen nach folgenden Gesichtspunkten; damit gehen auch unterschiedliche Regelungen bei der Handhabung einher:

    - personaldatenverarbeitende EDV-Anwendungen,
    - betriebsdatenverarbeitende EDV-Anwendungen und
    - sonstige EDV-Anwendungen.

2) Die Dokumentation von EDV-Anwendungen umfasst pro Anwendung:

   - Datenkatalog,
   - Schlüsselverzeichnis
   - Ausgabenkatalog
   - Schnittstellenverzeichnis und
   - Berechtigungskatalog

   Zugriffsberechtigungsänderungen, -vergabe und -löschung werden protokolliert.

3) Es gibt Verwendungseinschränkungen bzgl. personenbezogener Daten, die elektronisch gespeichert werden, es sei denn es bestehen einvernehmliche Regelungen:

   - Profilabgleiche sind nicht erlaubt.
   - Es dürfen keine umfänglichen beruflichen Biografien erstellt werden.
   - Es dürfen keine zur Beurteilung von Arbeitnehmer dienenden Daten gespeichert werden.

4) Die Auswertung der Benutzer- und Bearbeiterkennzeichen über das erbrachte Arbeitsvolumen und die Arbeitsqualität ist unzulässig.

5) Es darf keine Auswertung der durch die Systemsoftware aufgezeichneten Benutzerkennzeichen erfolgen.

6) Falls es sich um tragbare PC´s handelt und sie zu den personal- bzw. betriebsdatenverarbeitenden EDV-Anwendungen gehören, so sind sie mit Sicherheitssoftware auszustatten, welche die Aktivitäten des Nutzers protokolliert.

Kapitel 3

OECD Privacy Statement Generator

Die Grundsätze des Bundesverfassungsgerichts und das BDSG sehen eine Reihe von Vorschriften zum Schutze des Einzelnen vor dem Missbrauch seiner Daten durch die Verarbeitung und Nutzung personenbezogener Daten durch den Staat bzw. die Wirtschaft vor. Neben dem Recht auf informationelle Selbstbestimmung soll der Einzelne nachvollziehen können, wer wo was bei welcher Gelegenheit erfährt. Er muss seine Einwilligung geben und über Zweck und Umfang der Datenverarbeitung unterrichtet werden. Es sollt auch dargelegt werden, was geschieht, falls er seine Einwilligung nicht gibt.

Um diesen Pflichten gerecht zu werden, erscheint es sinnvoll, Privacy Principles aufzustellen und sie dem Betroffenen zugänglich zu machen. Gleichzeitig besteht so auch die Möglichkeit das Vertrauen des Einzelnen zu stärken. Gerade im e-Business-Bereich ist das Misstrauen groß.

Da die Formulierung von Privacy Statements sehr schwierig ist, hat die OECD – *Organisation for economic co-operation and development* – in Zusammenarbeit mit Industrie, Privacy Experten und Verbraucherorganisationen den OECD Privacy Policy Statement Generator entwickelt [3], [4], [5].

Mit Hilfe des Generators können Privacy Principles formuliert werden, die eindeutig und unverfänglich sind. Dazu muss vorab die eigene Vorgehensweise in Bezug auf personenbezogene Daten überprüft werden. Mit Hilfe eines Fragebogens werden die Praktiken geprüft und am Ende ein Formulierungsvorschlag offeriert. Dieser bedarf eventuell noch einer Überarbeitung.

Da Lufthansa verschiedene Unternehmenszweige besitzt und demzufolge jedes Unternehmen unterschiedliche Vorgehensweisen in Bezug auf personenbezogenen Daten verfolgt, erscheint es sinnvoll den Unternehmenszweigen solch einen Generator zur Verfügung zu stellen, so dass jeder seine Principles selbst generieren kann und sie trotzdem einer einheitlichen konzernkonformen Formulierung unterliegen.

3.1 Privacy Principles der OECD

Die OECD hat in diesem Zusammenhang Richtlinien in Zusammenarbeit mit ihren Mitgliedsländern entwickelt. Im wesentlichen sind acht Prinzipien ausgearbeitet und formuliert worden:

1) Collection Limitation Principle,
2) Data Quality Principle,
3) Purpose Specification Principle,
4) User Limitation Principle,
5) Security Safeguards Principle,
6) Openness Principle,
7) Individual Participation Principle und
8) Accountability Principle.

Diese Principles [6] werden im folgenden näher erläutert. Sie überschneiden sich in einigen Punkten und bedingen sich auch gegenseitig.

Collection Limitation Principle

Dieses Principle besagt, dass die Sammlung/Speicherung personenbezogener Daten begrenzt werden sollte. Eine Expertengruppe des OECD hat dabei versucht, Daten einer gewissen Sensibilität zuordnen. Diese Abgrenzung ist ihr aber leider nicht einheitlich gelungen.

Daher ist dieses Prinzip sehr allgemein gehalten. Die Grenzen, die letztendlich vom jeweiligen Gesetzgeber gesetzt werden sollten, sollten folgende Aspekte beachten:

- Datenqualität; es sollte möglich sein, Informationen hoher Qualität aus den gesammelten Daten herauszuziehen,
- zweckgebundene Datensammlung; nur die für den Zweck dienlichen Daten sollten gesammelt werden,
- Kennzeichnung bestimmter sensitiver Daten gemäß den Gesetzten und Traditionen des jeweiligen Mitgliedlandes,
- Beschränkung der Befugnisse von Datenschutzbeauftragten und
- Bürgerrechte.

Außerdem befasst sich dieses Principle auch mit der Datenerhebung selbst. Die Daten sollten auf rechtmäßige und faire Weise erlangt werden und wo notwendig mit dem Wissen oder der Einwilligung des Betroffenen. Die Einschränkung „wo notwendig“ ist ein Zugeständnis z.B. an die Verbrechensbekämpfung.

Data Quality Principle

Die personenbezogenen Daten sollten für den Grund, für den sie benutzt werden, wichtig sein. Daten, die z.B. Meinungen wiedergeben, sind in einem anderem Zusammenhang eventuell falsch. Die Daten sollten korrekt und vollständig sein. Außerdem sollten sie aktuell sein.

Purpose Specification Principle

Der Grund der Datenerhebung sollte nicht später als zum Zeitpunkt der Erhebung selbst bekannt gemacht werden. Sollte der Grund sich zu einem späteren Zeitpunk ändern, muss dies auch bekannt gemacht werden. Ausserdem sollten die Daten, wenn sie keinem Grund mehr dienen, vernichtet/gelöscht werden. Dies ist wichtig, da eventuell die speichernde Stelle die Kontrolle über nicht mehr gebrauchte Daten verliert und so evtl. Datendiebstahl oder Datenkopien ermöglicht werden.

Use Limitation Principle

Dieses Principle beschäftigt sich mit den verschiedenen Benutzungsarten von Daten. Sie beinhaltet auch die Veröffentlichung von Daten. So könnten z. B. Daten von einem Computer zum anderen übertragen werden, wo sie dann unerlaubt benutzt werden können, ohne dass es eine Kontrolle gibt. Generell sollte die ursprüngliche Zweckbestimmung massgeblich sein.

Dieses Principle lässt allerdings zwei Ausnahmen zu :

1) Der Betroffenen hat seine Einwilligung gegeben, dass Daten auch anderweitig genutzt werden können.
2) Es gibt diesbezüglich Regelungen in der Gesetzgebung.

Security Safeguard Principle

Dieses Principle geht auf die Sicherheitsaspekte ein. Daten sollten in angemessener Weise vor Risiken wie unerlaubtem Zugriff, Verlust, Beschädigung, Veränderung oder auch Veröffentlichung geschützt werden. Dabei sind vor allem technische und organisatorische Massnahmen gemeint.

Openness Principle

Ein Betroffener sollte das Recht haben:

a) zu erfahren, ob Daten über ihn gespeichert werden,
b) in angemessener Zeit bzgl. seiner Daten benachrichtigt zu werden; Kosten sollten für ihn dabei nicht anfallen,
c) den Grund zu erfahren, weshalb sein Auskunftsbegehren abgelehnt worden ist und gegen diese Ablehnung anzugehen und
d) Einwand zu erheben und eine Löschung, Berichtigung, Vervollständigung oder Ergänzung zu bewirken.

Accountability Principle

Verantwortlich für die Einhaltung der vorherigen Principles ist der Datenschutzbeauftragte. Dazu sollten ihm geeignete Mittel zur Verfügung gestellt werden. Dies gilt auch für die Verarbeitung der Daten durch Dritte. Auch hier trägt er letztendlich die Verantwortung, das heißt, er muss gewährleisten, dass das Persönlichkeitsrecht des Betroffenen auch bei der Verarbeitung durch Dritte bestehen bleibt.

3.2 Privacy Principles der Lufthansa AG und ihre Zuordnung zu den OECD Principles

Lufthansa hat Privacy Principles entwickelt, die die konzernweite Ausrichtung im Datenschutz festlegen sollen [2]. Diese allgemeinen Datenschutzgrundsätze stellen eine interne Verpflichtung für die LH-Konzerngesellschaften bzw. ihre Mitarbeiter dar.

In den Privacy Principles der Lufthansa AG [2] werden dabei sechs datenschutzrelevante Bereiche angesprochen, die im folgenden den Principles der OECD zugeordnet werden:

Kundenorientierung

Die Wahrung des Persönlichkeitsrechtes ihrer Kunden, Aktionäre und sonstiger Geschäftspartner (Betroffene) bei der Verarbeitung und Nutzung ihrer personenbezogenen Daten ist ein wichtiges und verpflichtendes Serviceelement.

Das Persönlichkeitsrecht findet sein äquivalent in dem *Collection Limitation Principle*. Hier wird ausdrücklich auf die Einhaltung der Bürgerrechte hingewiesen. Die OECD formuliert sein Principle etwas konkreter. Sie geht außerdem noch z. B. auf die Datenqualität und die Zweckgebundenheit der Daten ein.

Transparenz

Um vertragliche und vorvertragliche Zwecke sowie um individuelle Serviceleistungen anbieten zu können, werden personenbezogene Daten verarbeitet und genutzt. Bzgl. individuellen Serviceleistungen werden die Betroffenen über die Zwecke der Verarbeitung und der Nutzung sowie ggf. über die Empfänger der Daten, sofern sie hiervon nicht bereits auf andere Art Kenntnis haben, informiert. Zu den Rechten des Betroffenen gehören außerdem:

- das Verweigerungsrecht: Der Betroffene hat das Recht, die Verarbeitung und Nutzung seiner Daten außerhalb der ursprünglichen Zweckformulierung zu untersagen.
- Auskunftsrecht: Der Betroffene darf Auskunft über die über ihn gespeicherten Daten verlangen und bei fehlerhaften Daten eine Berichtigung erwirken.
- Sicherheitsvorkehrung bei der Datenübermittlung an Dritte: Das Persönlichkeitsrecht darf bei solch einer Übertragung nicht beeinträchtigt werden.
- Vorkehrung zur Wahrung der Richtigkeit, der Aktualität und Wichtigkeit der Daten für den Zweck.

Dieser Grundsatz spiegelt sich in dem *Individual Participation Principle* und dem *Data Quality Principle* wieder.

Sicherheit

LH stellt angemessene Verfahren gegen Verlust und Missbrauch, sowie gegen unberechtigte und unbefugte Zugriffe, Offenlegung, Veränderung und Löschung von Daten bereit.

Damit genügt LH dem *Security Safeguard Principle*.

Globale Einheitlichkeit

Wem eine Dienstleistung erbracht wird, an welcher der LH-Konzern beteiligt ist, soll weltweit eine gleich wirksame Zuwendung in Hinblick auf die Wahrung seines Persönlichkeitsrechtes erhalten.

Dieser Grundsatz findet sich im *Accountability Principle* wieder.

Privacy Statements (Datenschutzerklärungen)

Lufthansa bekennt sich zu weitgehender Selbstregulierung im Datenschutz. Wesentliche Elemente dieser Selbstregulierung sind Privacy Statements der relevanten LH Geschäftsfelder. Diese Statements legen das Datenschutzverhalten gegenüber den Betroffenen konkret fest. Ihre Erarbeitung auf Basis der Privacy Principles erfolgt eigenverantwortlich durch das betroffene Geschäftsfeld. Dabei muss folgendes beachtet werden:

- Privacy Statements müssen nachvollziehbar auf die datenschutzspezifischen Besonderheiten der entsprechenden Geschäftsprozesse eingehen.
- Die Geschäftsfelder sollen bei der Abfassung der Datenschutzerklärungen offen für Anregungen von relevanten Verbraucherorganisationen sein.

Mit diesem Grundsatz trägt LH dem *Purpose Specification Principle* Rechnung.

Gesetzlich unabhängige Konfliktlösung

Bei Konflikten bzgl. der Einhaltung des Datenschutzes bietet LH dem Betroffenen die Möglichkeit, den Datenschutzbeauftragten des Konzerns auf einfache Weise einzuschalten. Die Unabhängigkeit des Datenschutzbeauftragten wird dabei durch zwingende Vorschriften des BDSG sichergestellt.

Bei dem *Individual Participation Principle* wird auf die Rechte des Betroffenen eingegangen. Diese Rechte können durch die Einbeziehung eines Datenschutzbeauftragten durch den Betroffenen bei Konfliktfällen gewahrt werden.

3.3 Fazit

Da bei der Entwicklung der LH Privacy Principles auf die Principles der OECD zurückgegriffen wurde, war eine grundsätzliche Übereinstimmung voraussehbar. Die Principles der OECD sind allerdings etwas konkreter formuliert.

In den Abschnitten bzgl. der Transparenz, der globalen Sicherheit und den Privacy Statements (Datenschutzerklärungen) werden zu einem auf die Zweckveröffentlichung der Datenerhebung, auf die Einheitlichkeit des Persönlichkeitsrechtes und zum anderen auf die Datenschutzerklärung selbst eingegangen. Es ist deutlich, dass eine Formulierung von Principles notwendig ist. Wegen der vielfältigen Verzweigung des Unternehmens sollte darauf geachtet werden, dass dies Formulierungen einheitlich sind.

3.4 Benutzung des Generators anhand des Projektes „my Travel ex“ der Lufthansa AG

Um die Vorgehensweise und die Fragen des OECD- Generators näher kennen zulernen, wurde mit Hilfe des LH-Projektes „my Travel ex“ der Generator praktisch getestet, theoretisch war eine Übereinstimmung der Principles festgestellt worden.

3.4.1 Einführung in „my Travel ex“

Die Konzernmitarbeiter sollen in die Lage versetzt werden, ihre Reisen über ein benutzerfreundliches Online-Medium komfortabel und nutzergerecht zu buchen, zu organisieren und zu kaufen. Gleichzeitig sollen diese Kunden Zugang zu ihren persönlichen Kontenbewegungen (Bestand an Buchungen, Ticketkauf, Ticketrückgabe, Versteuerung, etc.) erhalten.

Informationsabfragen, Reservierungen, etc. können über das Mitarbeiterportal vom Arbeitsplatz, dem Crew Remote Access des Mitarbeiterportals und, in Abhängigkeit vom Remote Access des Mitarbeiterportals, auch durch Bodenpersonal von zu Hause aus komfortabel und nutzergerecht vorgenommen werden.

Die Einhaltung der Reiseregeln erfolgt durch systemseitige Prüfung im Hintergrund. Fehleingaben werden durch Fehlermeldung angezeigt. Bei der Eingabe erhält der Kunde für jede Funktionalität eine Maske. Soweit für den Prozess persönliche Daten benötigt werden, wird die Maske bereits mit den benötigten Daten aus AIDA, dies ist wie VIVA ein System innerhalb des LH Intranets, und dem Metadirectory vorausgefüllt. In „my Travel ex“ selbst werden also keine Mitarbeiterdaten gespeichert. Gleichwohl wird eine PK-Nummern bezogene Liste der Passenger Name Records erstellt, auf die der Mitarbeiter ausschließlich Zugriff hat. „my Travel ex“ speichert nur ablaufbezogene Daten. Der Kunde komplettiert die Maske und sendet sie an den Hostrechner.

Als Ausgabe erhält der Kunde eine Bestätigung in einer Maske, in der die Hostantwort nutzergerecht und verständlich aufbereitet ist.

Um „my Travel ex“ benutzen zu können, muss der LH-Mitarbeiter sich ins Lufthansa Intranet eingeloggt haben. Bei dem Eintritt ins Intranet über das Mitarbeiterportal des Internets identifiziert sich der Nutzer zunächst. Danach hat er Zugang zu den Web-Seiten des Lufthansa Intranets (Abb. 3.1).

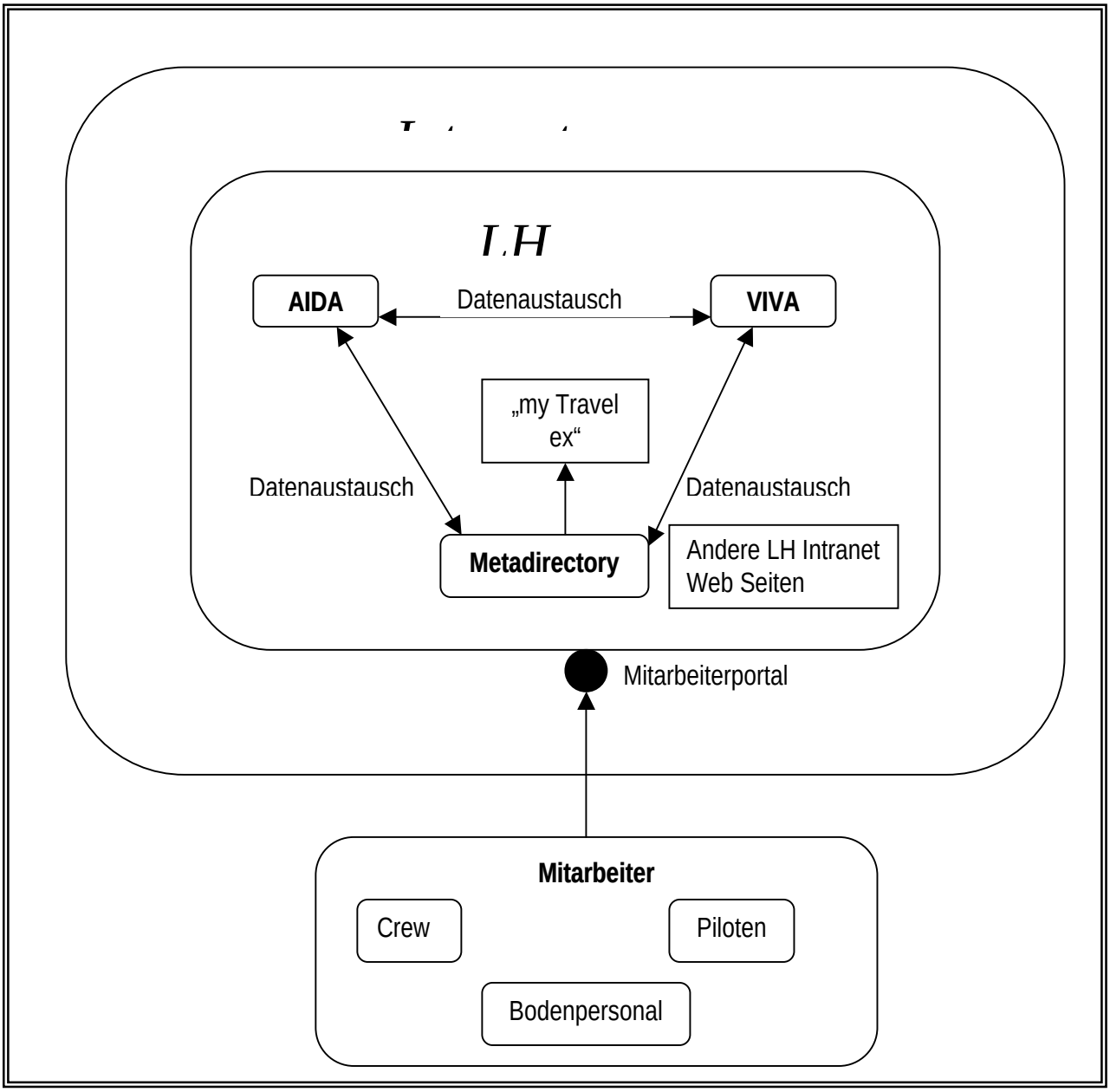

Abbildung 3.1: Schema Mitarbeiterzugang zum LH Intranet und dessen interne Web Seiten

3.4.2 Gliederung des OECD Generators und allgemeine Auswertung

Der Generator teilt seine Fragen in 11 Bereiche auf:

1) Informationen über die Organisation selbst und ihre Web Seite,
2) Möglichkeiten des anonymen Zugriffs,
3) „Verbindungscharakteristiken“ der Web Seite,
4) Automatische Sammlung von Informationen,
5) Datenerhebung und ihre Begründung,
6) Schutz des Kindes,
7) Veröffentlichung von Daten und Mitbestimmungsmöglichkeiten durch den Kunden,
8) Vertraulichkeit/Sicherheit,
9) Selbstbeteiligung des Einzelnen/ Zugriff,
10) Übereinstimmungen mit anderen Regularien und
11) Datenschutzkontrolle durch interne und externe Instanzen.

Bei der Benutzung des Generators für “my Travel ex“ hat sich herausgestellt, dass trotz der Übereinstimmung der Principles der Generator in dieser Form nicht von Lufthansa genutzt werden kann. Der Generator ist in erster Linie auf Grundlage des Internets konzipiert worden. Bei Lufthansa sollte der Generator allerdings für das Intranet eingesetzt werden. Daher waren einige Fragen nicht eindeutig oder gar nicht zu beantworten.

Auch waren einige Abschnitte zu allgemein gehalten. Sie trafen nicht direkt auf die Projektebene zu. Allerdings sollten sie nicht komplett entfallen, da sie wichtige Aspekte behandeln. Vielmehr bedarf es auf einer übergeordneten Ebene der Einarbeitung. Diese Abschnitte könnten dann schon beim Eintritt des Mitarbeiters ins Intranet erscheinen.

Grundsätzlich entspricht der Formulierungsentwurf den Anforderungen der Lufthansa AG. Aufgrund der Uneinstimmigkeiten der Fragen bzgl. der Internet/Intranet-Problematik sollte jedoch eine Anpassung der Fragen an LH-Bedürfnisse stattfinden. Dadurch würde dann auch der Formulierungsentwurf konkreter und auf das Intranet abgestimmter ausfallen.

3.4.3 Auswertung der einzelnen Abschnitte

Es folgt zunächst eine Auswertung der einzelnen Abschnitte. Falls ein Abschnitt an die Bedürfnisse von Lufthansa angepasst werden sollte, wird mit der Auswertung auch ein Änderungsvorschlag aufgeführt. In diesem Fall sind die Fragen des OECD Generators zum Vergleich mit aufgeführt. Der gesamte Fragenkatalog des Generators befindet sich in Anhang A.

Abschnitt 1: Informationen über das Projekt/Abteilung und ihre Web Seite

Dieser Abschnitt (Abb. 3.2) gibt einen allgemeinen Überblick über die formalen Daten wie Name, Adresse usw. wieder. Die Eingaben brauchen allerdings nicht so detailliert gemacht werden, da der Kontakt Lufthansa-intern mit weniger Informationen hergestellt werden kann. Es brauchen lediglich Informationen dazu bereitgestellt werden, um welche Abteilung es sich

hier handelt, wer der Ansprechpartner dieser Abteilung ist und wie die interne Co-mail lautet. Die Frage, ob dieses Statement auch für andere Abteilungen gilt, kann weggelassen werden, da jede Abteilung ihr eigenes Statement formuliert.

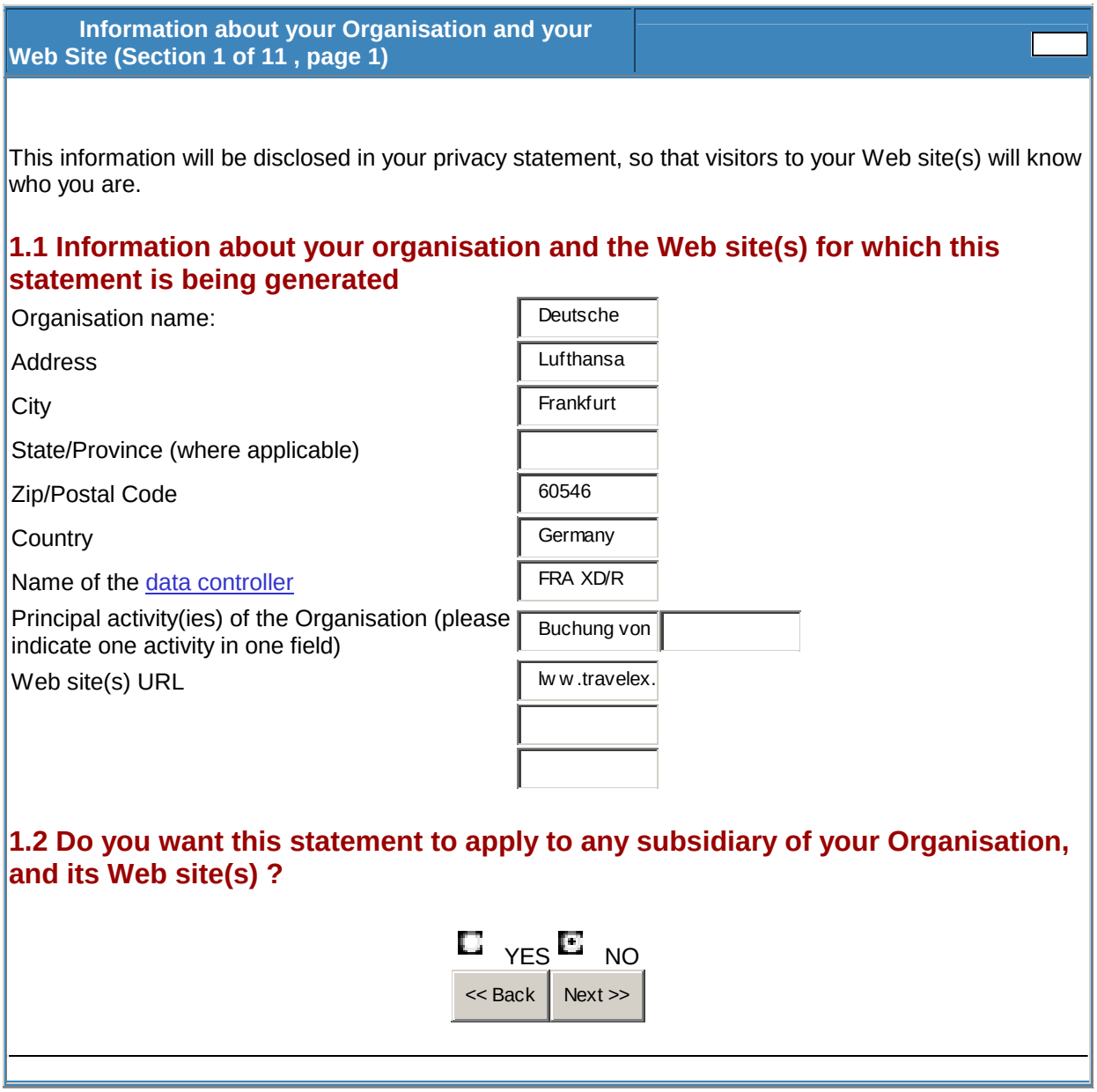

Abbildung 3.2: Fragenkatalog des OECD, Abschnitt 1

Abschnitt 2: Möglichkeiten des anonymen Zugriffs

In diesem Abschnitt wird geklärt, ob auch ein anonymer Zugriff auf die Web Seite möglich ist. Da sich jeder Mitarbeiter schon beim Eintritt ins Intranet durch seine PK-Nr. identifizieren muss, ist er im Grunde schon nicht mehr anonym. Allerdings muss er sich, um „my Travel ex“ benutzen zu können, und damit die erforderlichen Daten aus dem Metadirectory geholt werden können, erneut identifizieren. Dies kann für andere Anwendungen im Intranet nicht notwendig sein. Daher sollte die Frage übernommen werden.

Abschnitt 3: Verbindungen zu anderen Web Seiten

Abschnitt 3 (Abb. 3.3) behandelt die Verbindungen zwischen Web Sites. Oft werden persönliche Daten von Dritten gesammelt und dann von anderen Web Seiten benutzt. LH speichert die Daten seiner Mitarbeiter in einem Metadirectory. Werden diese Daten benötigt, so wird auf das Directory zugegriffen. Dies ist dann allerdings kein Dritter, da es LH-intern gespeichert ist und das Metadirectory Bestandteil von LH ist. Die Frage 3.2. ist nicht konkret zu beantworten, da zwar auf persönliche Daten aus dem Metadirectory zugegriffen wird, aber dies kein Dritter ist. Die Frage müsste entweder umformuliert oder weggelassen werden. Man sollte allerdings, um die Transparenz gegenüber dem Mitarbeiter zu wahren, die Schnittstellen zu anderen Systemen innerhalb des Intranets offen legen (Frage 3.2.1). Der Fragenabschnitt 3.2 könnte daher wie folgt geändert werden:

> 3.2. Hat Ihre Web Seite Schnittstellen zu anderen LH-IT-Systemen (z.B. das Metadirectory), die persönliche Daten über Ihre Besucher sammelt? Wenn ja, spezifizieren Sie diese Schnittstellen zu anderen Systemen bitte näher.

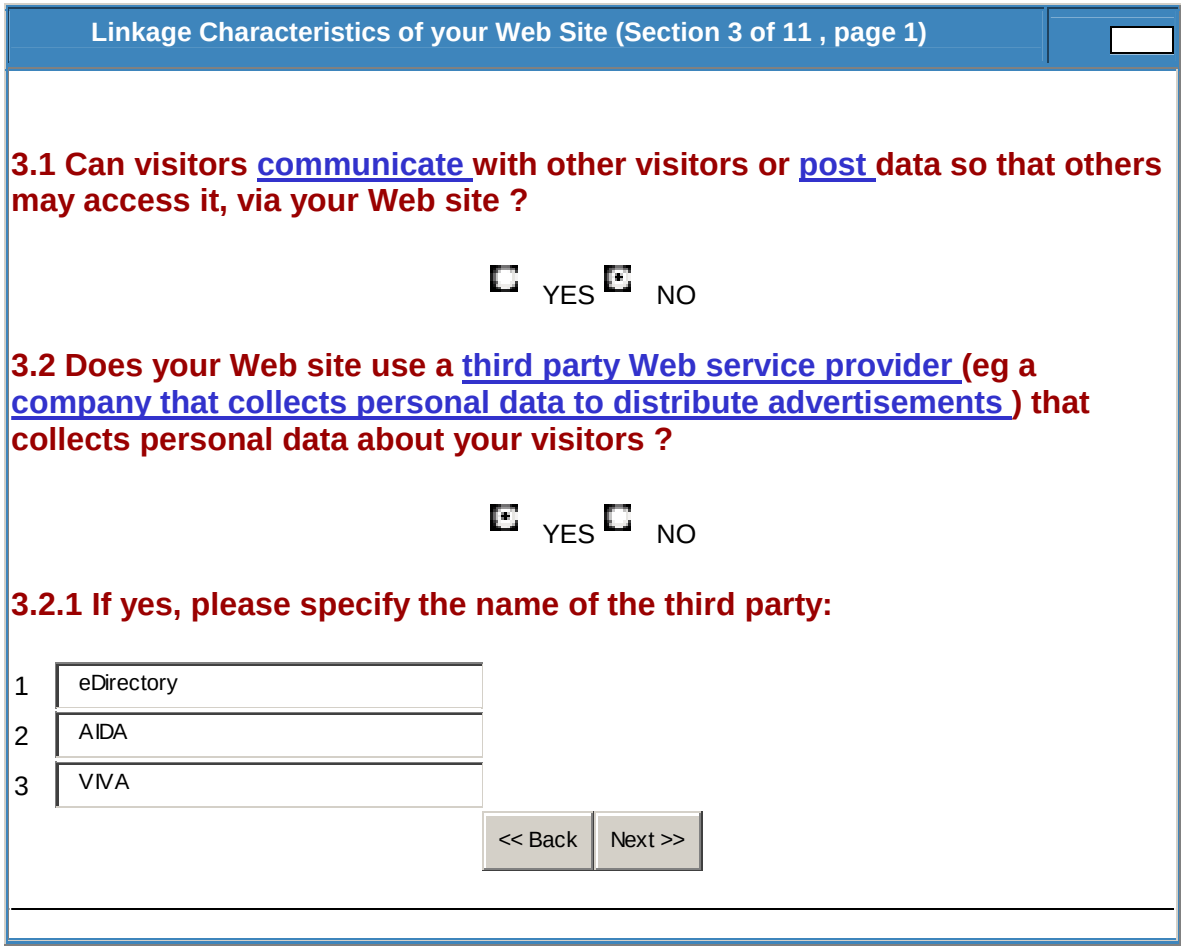

Abbildung 3.3: Fragenkatalog des OECD, Abschnitt 3

Abschnitt 4: Automatische Sammlung von Daten

Dieser Abschnitt (Abb. 3.4) beschäftigt sich mit der Art und Weise wie Daten erhoben werden. Grundsätzlich kann dieser Abschnitt übernommen werden. Um mehr Transparenz zu schaffen, sollte allerdings näher spezifiziert werden, welche andere Methoden benutzt werden, um Daten zu erlangen. Dies kann als Frage 4.2.a mit eingeführt werden.

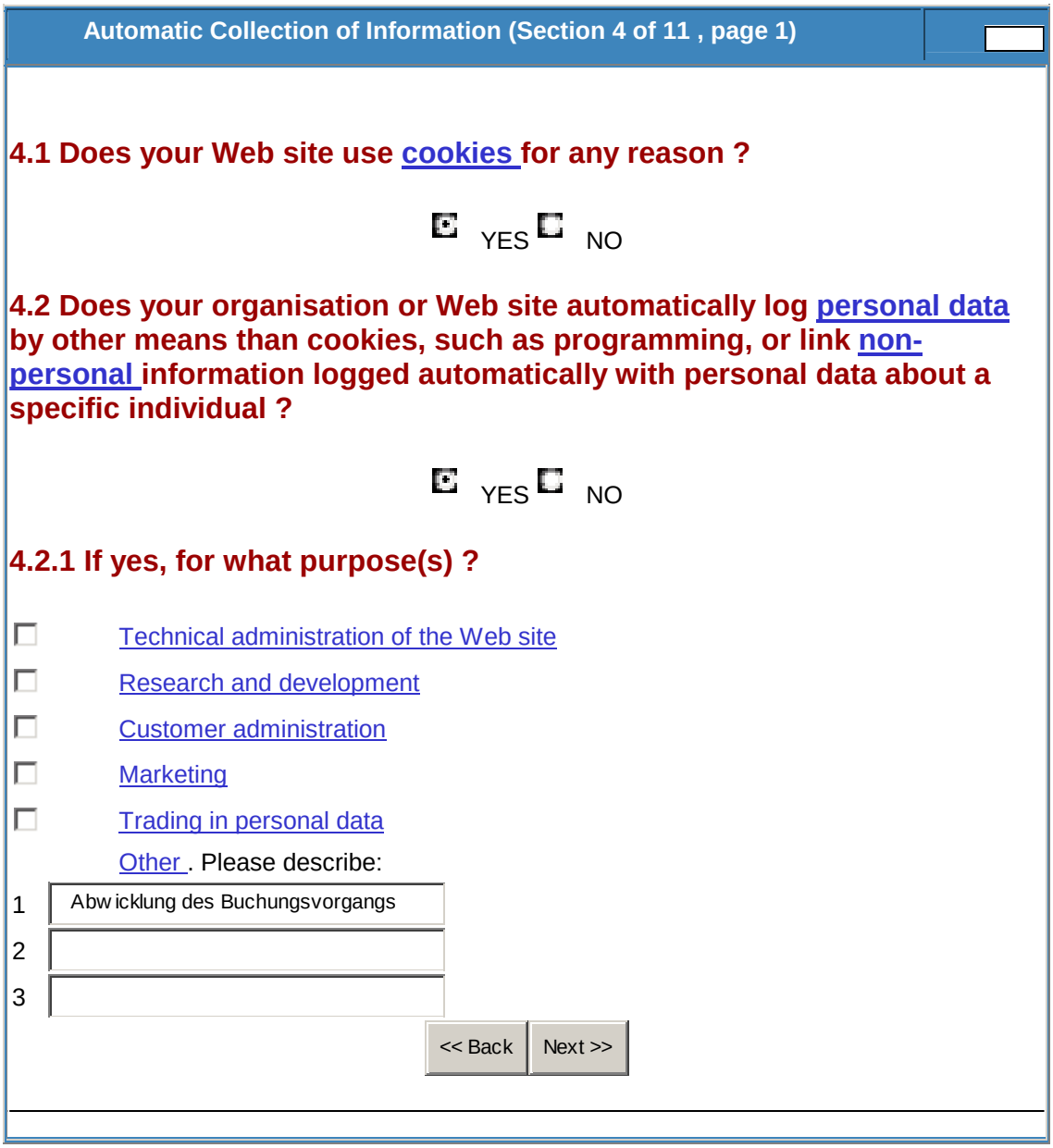

Abbildung 3.4: Fragenkatalog des OECD, Abschnitt 4

Abschnitt 5: Datenerhebung und ihre Begründung

Die Themen *Data Collection* and *Purpose Specification* werden hier bearbeitet. Frage 5.5 in Abb. 3.5 zielt auf die Mitbestimmungsmöglichkeiten des Einzelnen ab. Diese Frage ist eigentlich mit „nein“ zu beantworten. Dies wurde vom Generator jedoch nicht akzeptiert. Daher wurde die Frage mit „ja“ beantwortet. Bei „my Travel ex“ werden nur Daten zu dem Zweck der Flugpreisberechnung und Reservierung benötigt. Der Grund wird sich nicht ändern, da dies der Zweck von „my Travel ex“ ist. In anderen Bereichen kann es natürlich vorkommen, dass Daten aus einem anderen Grund erhoben werden, als zuvor angegeben. Daher ist die Frage an sich auch zu übernehmen.

Zu klären blieb, ob es sich hier um einen Programmierfehler handelt. Wenn alternative Antworten geboten werden, sollte der Generator sie auch akzeptieren und keine Fehlermeldung hervorrufen. Diesbezüglich wurde eine e-mail (Anhang C) an den OECD geschickt. Die Antwort ist auch in Anhang C nachzulesen. Anscheinend war es nicht beabsichtigt, Antworten den Generator-Nutzern aufzuerlegen.

Abschnitt 6: Schutz des Kindes

Dieser Abschnitt 6 im Fragebogen spricht ein wichtiges Thema an, das nicht vernachlässigt werden darf. Er zielt auf die Privatsphäre des Kindes ab. Es ist tatsächlich so, das bei Lufthansa Daten über Kinder gespeichert werden; jedoch nicht bei „my Travel ex“ selbst. Es werden Name und Geburtsdatum im Metadirectory festgehalten. Dies ist nötig, um z.B. bei Ticketkäufen die Buchungsart und –kosten der Reisepartner zu ermitteln. Da aber ausser dem Mitarbeiter selbst kein anderer auf seine Daten Zugriff hat, sind auch die Daten der Kinder indirekt vor fremden Zugriff geschützt. Daher ist ein Schutz der Kinder und Ihrer Daten nicht unbedingt notwendig. Hier vermischen sich die Projektebene von „my Travel ex“ mit der darüber liegenden Konzernebene von Lufthansa.

Sinnvoll wäre es, Formulierungen diesbezüglich schon gleich beim Eintritt ins Intranet über das Mitarbeiterportal bereitzustellen. Diese Formulierungen würden für alle folgenden Web Seiten gelten. Auf Projektebene kann dieser Abschnitt dann entfallen.

Abschnitt 7: Veröffentlichung und Mitbestimmungsmöglichkeiten des Nutzers

Dieser Abschnitt (Abb. 3.6) bearbeitet Aspekte, die die Offenlegung von Daten angehen. Grundsätzlich ist es wichtig für den Nutzer zu wissen, ob Daten mit anderen ausgetauscht werden. Da man sich hier innerhalb des Lufthansa Intranets befindet, sollten allerdings begriffliche Anpassungen vorgenommen werden. Frage 7.1 des Fragebogens sollte wie folgt umformuliert werden:

7.1. Gewährt Ihre Web Seite oder Ihre Organisationseinheit anderen Projekten oder Organisationseinheiten Einblick in die persönlichen Daten Ihrer Web Seiten Nutzer?

Falls eine Offenlegung stattfindet, wird zusätzlich getestet, ob der Nutzer dann die Möglichkeit hat, mitzubestimmen und in welcher Weise dies erfolgen kann. Da „my Travel

ex“ keine Daten mit anderen Einheiten teilt, wurde dieser Teilabschnitt übersprungen, der jedoch so übernommen werden kann.

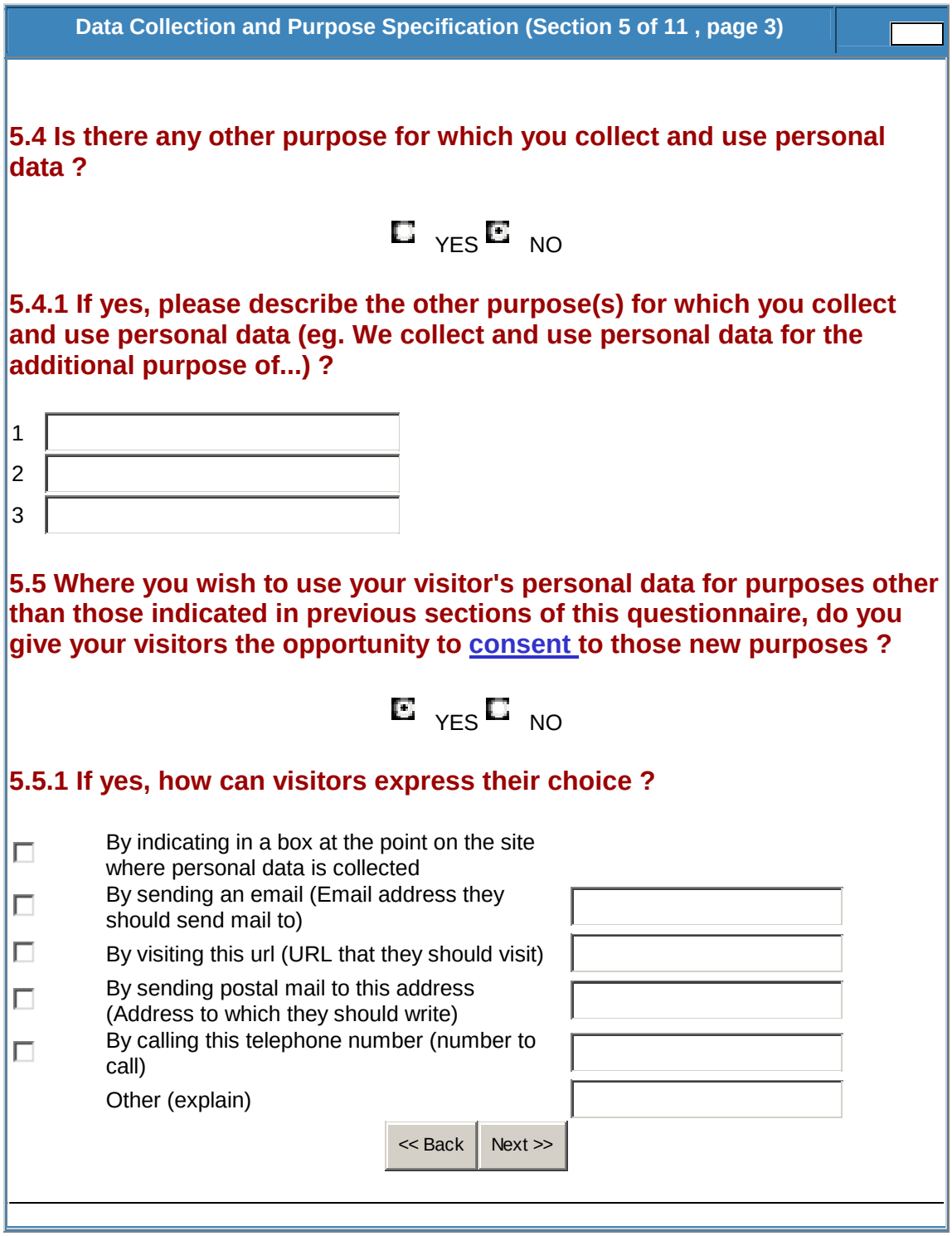

Abbildung 3.5: Fragenkatalog des OECD, Abschnitt 5

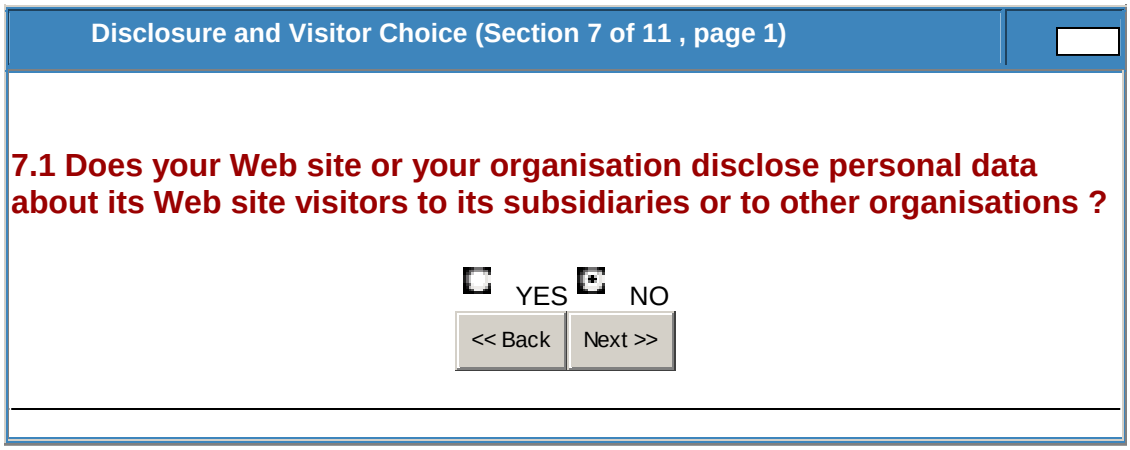

Abbildung 3.6: Fragenkatalog des OECD, Abschnitt 7

Abschnitte 8 bis 11

Abschnitt 8 (Vertraulichkeit/Sicherheit) ist zwar wichtig, aber etwas zu allgemeingehalten. Es spricht Themen an, die für das gesamte LH-Intranet relevant sind. Genauso wie Abschnitt 6 mit dem Bereich „Schutz des Kindes“ sollte dieser Bereich auf eine höhere Ebene verlagert werden und schon beim Eintritt ins Intranet formuliert sein.

In Abschnitt 9 (Selbstbeteiligung des Einzelnen/Zugriff) werden die Zugriffsmöglichkeiten des Einzelnen auf seine eigenen Daten geprüft. Es werden auch Aspekte bzgl. der Löschung, Berichtigung usw. von Daten bearbeitet und in wieweit der Einzelne Einfluss darauf nehmen kann. Da bei „my Travel Ex“ direkt keine Daten gespeichert werden, erscheint es in ersten Moment sinnvoller diesen Abschnitt eher auf der LH-Ebene anzusiedeln. Es kann aber sein, dass andere Abteilungen sehr wohl Daten speichern, die über die im Metadirectory hinausgehen, so dass der Abschnitt doch in den Generator auf Projektebene übernommen werden sollte.

Die Abschnitte 10 und 11, die die Themen „Übereinstimmungen mit anderen Regularien“ und „Datenschutzkontrolle durch interne und externe Instanzen“ beinhalten sind für das gesamte LH-Intranet relevant und sollten daher einheitlich für alle Web Seiten formuliert werden. Es wäre daher sinnvoller, dies schon auf der Metaebene Lufthansa zu berücksichtigen.

Kapitel 4

P3P & APPEL Grundlagen

Wie schon in den vorangegangenen Abschnitten deutlich wurde, ist der Datenschutz eine wichtige Maßnahme, um das Vertrauen der Nutzer zu gewinnen. Die Veröffentlichung von Datenschutzgrundsätzen ist dabei ein wesentlicher Schritt in diese Richtung. Der Nutzer kann sich vorab über Praktiken informieren und dann entscheiden, ob er mit dem Anbieter weiter in Verbindung bleiben möchte. Mit der Formulierung über einen Generator wird dabei die Eindeutigkeit der Aussagen gewährleistet, so dass es nicht zu Missverständnissen kommen kann. Die Aussagen sind klar und leicht verständlich, auch für Laien. Außerdem kann man bei der Benutzung eines Generators davon ausgehen, dass alle wichtigen Aspekte bzgl. des Datenschutzes berücksichtigt wurden. Man braucht sich nicht unbedingt selbst mit den Gesetzten und Bestimmungen auseinander setzten.

Die Formulierung von Datenschutzmaßnahmen kann allerdings nur der erste Schritt zum Vertrauen der Nutzer ins Netz sein, da der Nutzer sich im allgemeinen nicht mit dem Lesen von Maßnahmen aufhalten möchte. Für den Nutzer wäre es am einfachsten, er könnte seine Datenschutzpräferenzen in einer allgemein gebräuchlichen Form „kodieren“. Das gleiche sollten auch die Anbieter von Web-Seiten mit ihren Datenschutzpraktiken machen. Besucht nun ein Nutzer eine Webseite, könnten diese Präferenzen und Praktiken zum Beispiel durch den Browser vorab verglichen werden. Stimmt alles überein, so wird die Seite angezeigt. Wenn nicht, dann kann der Vorgang automatisch abgebrochen werden; der Nutzer kann die Seite nicht besuchen. Eine andere Möglichkeit wäre auch in diesem Fall, den Nutzer aktiv in den Vorgang mit einzubeziehen. Durch eine Fehlermeldung könnten die Unstimmigkeiten aufgezeigt und durch eine manuelle Zustimmung des Nutzers, die nur für dieses eine Mal gilt, gelöst werden.

Das oben beschriebene Szenario war Grundlage für eine Initiative des W3C (*World Wide Web Consortium*).

Mit der *Plattform for Privacy Project* (P3P) leitete 1997 das W3C eine Initiative ein, die zu mehr Sicherheit und Transparenz im Web beitragen sollte [8]. P3P ist so konzipiert, dass jeder einzelne Internet-Benutzer selbst über die Preisgabe und Verwendung seiner persönlichen Daten bestimmen kann. Die Wahrung der Privatsphäre des einzelnen Nutzers stand dabei im Vordergrund von P3P.

4.1 P3P Grundlagen

4.1.1 Konzept

Grundsätzlich ist P3P eine standardisierte Menge von Ausdruckmöglichkeiten, die alle wichtigen Aspekte bzgl. des Datenschutzes abdeckt [9]. Zusammengenommen geben sie einen Überblick darüber, wie eine Web-Seite die persönlichen Daten ihres Besuchers behandelt.

P3P-fähige Web-Seiten liefern diese Informationen auf eine standardisierte, maschinenlesbare Weise. P3P-fähige Browser können diese Informationen automatisch lesen und mit den Datenschutzpräferenzen des Benutzers vergleichen. Stimmen die Präferenzen überein, so kann der Besucher auf der Seite weiter surfen. Stimmen sie nicht überein, so kann entweder der Vorgang automatisch abgebrochen werden, oder der Benutzer bekommt eine Fehlermeldung und kann dann selbst entscheiden, ob er fortfahren möchte oder nicht (Abb. 4.1) [10].

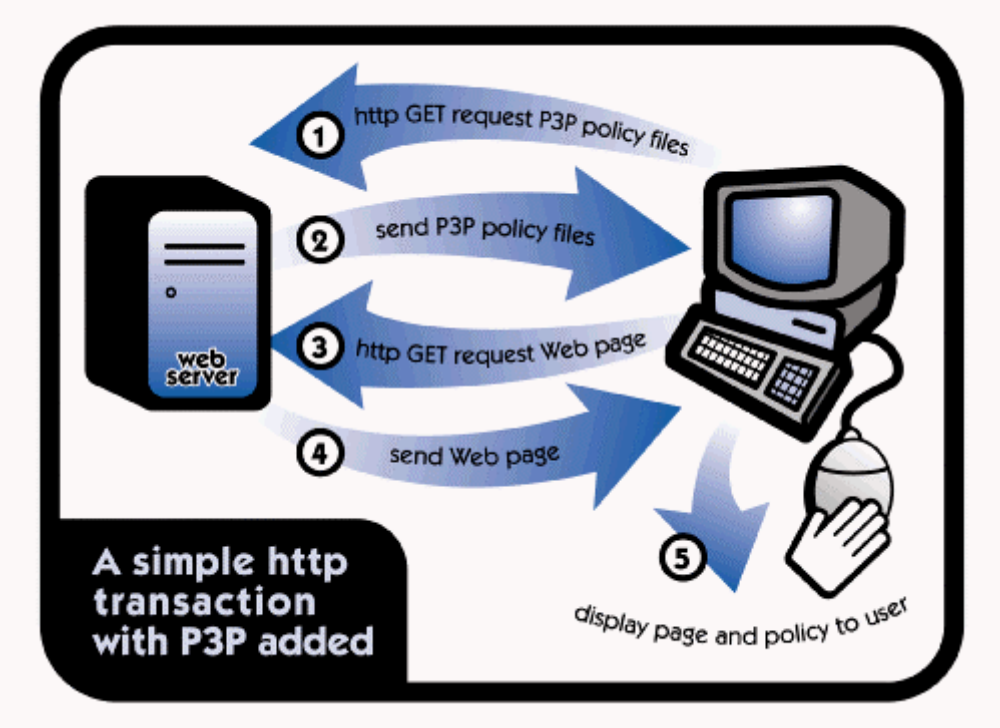

Abbildung 4.1: Transaktion mit P3P

4.1.2 Vokabular

P3P umfasst neun Aspekte im Bereich Online Privacy [13]. Fünf davon befassen sich dabei mit den Daten, die gespeichert werden:

- Wer sammelt die Daten?
- Welche Informationen genau werden gesammelt?

- Zu welchem Zweck?
- Welche Informationen werden mit anderen genutzt?
- Wer sind diese Datenempfänger?

Die verbleibenden vier Aspekte erklären die internen Datenschutzmaßnahmen:

- Können Benutzer Veränderungen bzgl. der Nutzung ihrer Daten machen?
- Wie werden Streitigkeiten gelöst?
- Welche Massnahmen werden zur Sicherung/Speicherung von Daten ergriffen?
- Wo befinden sich die Datenschutzmassnahmen in „menschenlesbarer“ Form?

P3P ermöglicht es Web-Seiten, ihre Datenschutzmaßnahmen in eine standardisiertes, maschinen-lesbares XML-Format [17] zu bringen, das durch den Browser des Benutzers automatisch gefunden und leicht ausgewertet werden kann. Dieses wird als P3P Policy bezeichnet und kann entweder manuell oder über automatische Tools erreicht werden. Diese Tools werden in Kapitel 5 vorgestellt und beschrieben.

Die P3P Spezifikation liefert unter anderem:

- ein Standardschema für Daten, die eine Web-Seite sammeln möchte; dieses Schema wird „P3P Base Data Schema“ genannt,
- eine Standardmenge zur Spezifizierung von Gebrauch, Empfänger, Datenkategorien und andere Veröffentlichungen von Privatdaten,
- ein XML Format, um Privacy Policies auszudrücken,
- ein Hilfsmittel, um Privacy Policies mit Web-Seiten und Cookies zu assoziieren (policy reference file) und
- einen Mechanismus, um P3P Policies über http transportieren zu können.

Der folgende Abschnitt 4.1.2.1 wird zunächst das Vokabular der allgemeinen Angaben, die möglich sind, einführen. Dabei ist jedem möglichen P3P Element ein bestimmter Wertebereich zugeordnet aus dem ausgewählt werden kann. In Abschnitt 4.1.2.2 wird dann das Vokabular bzgl. der erhobenen Datenmenge vorgestellt. Ein tabellarischer Kurzüberblick der wichtigsten Element und ihres Wertebereiches befindet sich am Ende von Abschnitt 4.1.2.2 (S. 37 –38).

4.1.2.1 Allgemeine Properties der Web Seite

Das **POLICY** Element

Das POLICY Element beinhaltet eine ganze P3P Policy. Jede P3P Policy muss genau in einem POLICY Element enthalten sein. Das POLICY Element muss ein ENTITY und ein ACCESS Element enthalten. Optional sind STATEMENT Elemente, ein DISPUTES-GROUP Element, ein P3P Datenschema und ein oder mehrere EXTENSIONS.

Weiterhin sind folgende Attribute enthalten:

name (Pflichtattribut) Name der Policy

discuri (Pflichtattribut) URI des menschenlesbaren Privacy Statements

opturi URI der Hinweise, denen ein Nutzer folgen kann, um der Datennutzung zu einem bestimmten Zweck zuzustimmen oder abzulehnen (opt-in oder opt-out). Dieses Attribut ist für Policies Pflicht, falls sie einen Zweck enthalten, der die Attributmenge opt-in oder opt-out benötigt.

Das **ENTITY** Element

Das ENTITY Element gibt eine genaue Beschreibung über die legale Einheit, die die Privacy Praktiken repräsentiert. Dies kann z.B. der Datenschutzbeauftragte der Firma oder ein Abteilungsleiter sein.

Diese Beschreibung umfasst die Geschäftsdatenmenge (siehe Abschnitt 4.1.2.3 Base Data Schema, business data) mit der die Kontaktinformationen wie Adresse Telefonnr., e-mail-Adresse oder andere Informationen, dargestellt werden können.

Das **ACCESS** Element

Das ACCESS Element weißt darauf hin, ob die Web-Seite Zugriff auf Informationen erlaubt. Dies gilt für Dritte als auch für den Betroffenen selber. Die Service Provider müssen einen Wert für das access Element angeben. Wie allerdings dieser Zugriff auf Daten möglich ist, wird nicht spezifiziert. Der Nutzer muss mit dem Service Provider dafür selbst in Kontakt treten.

Das ACCESS Element muss eines der folgenden Werte einnehmen:

<nonident/>
Web Seite sammelt keine identifizierbaren Daten.

<all/>
All Identified Data: Zugriff wird auf alle identifizierbare Daten erlaubt.

<contact-and other/>
Identifiable Contact Information and Other Identified Data: Zugriff wird auf identifizierbare online und auf physische Kontaktinformationen gewährt, auch auf einige andere identifizierbare Daten.

<ident-contact/>
Identifiable Contact Information: Zugriff wird auf identifizierbare online und auf physische Kontaktinformationen gewährt (z.B. Postadressen).

<other-ident/>
Other Identified Data: Zugriff ist auf bestimmte andere identifizierbare Daten möglich.

<none/>
None: Es wird kein Zugriff auf identifizierbare Daten gewährt.

Das **DISPUTES** Element

Dieses Element beschreibt, wie Streitigkeiten beigelegt werden können, falls es zu Uneinstimmigkeiten bzgl. der Privacy Praktiken kommt. Eine Policy sollte einen DISPUTES-GROUP Element beinhalten, das eine oder mehrere DISPUTES Elemente umfasst. Jedes DISPUTES Element kann wahlweise ein REMIDIES Element enthalten. Service Providers, die mehrere Möglichkeiten bzgl. der Beilegung von Streitigkeiten haben, sollten für jede Vorgehensweise ein eigenes getrenntes DISPUTES Element haben.

Folgende Attribute sind dabei ausserdem noch im DISPUTES Element enthalten:

- **resolution-type**
  (Wahlattribut) Gibt an, an wen man sich wenden kann. Es kann eines der folgenden Werte annehmen:

  Customer Service [service]
  Nutzer können sich beim Web Seiten Kundendienstrepräsentanten bzgl. der Lösung von Streitigkeiten bzgl. der gesammelten Daten melden. Die Beschreibung muss Information bzgl. der Kontaktierungsmöglichkeiten des Kundenservices beinhalten.

  Independent Organisation [independent]
  Nutzer können sich an unabhängige Stellen bei Streitigkeiten wenden. Die Beschreibung muss Informationen zu Kontaktmöglichen dieser Dritten unabhängigen Partei beinhalten.

  Court [court]
  Der Nutzer hat die Möglichkeit, eine legale Beschwerde gegen die Web Seite einzureichen.

  Applicable Law [law]
  Streitigkeiten, die in Zusammenhang mit dem Privacy Statement aufkommen, werden gemäß den Gesetzten, die in der Beschreibung referenziert werden, gelöst.

- **service**
  (Pflichtattribut) URI des Kundendienstes der Web Seite oder der unabhängigen Organisation, oder URI für die Information des zuständigen Gerichts oder des relevanten Gesetzes.

- **verification**
  URI oder Beleg, der benutzt werden kann, um Zwecke zu belegen.

- **short-description**
  Eine kurze menschenlesbare Beschreibung des anwendbaren Gesetzes oder einer unabhängigen Organisation oder die Kontaktinformation des Kundenservices, falls nicht schon spezifiziert.

- **long-description**
  Das LONG-DESCRIPTION Element beinhaltet eine lange Version der short-description.

- **img**
  Das IMG Element ist ein Bildlogo (z.B. der unabhängigen Organisation oder des zuständigen Gerichtes).

- **remidies**
  Jedes DISPUTES Element sollte ein REMEDIES Element enthalten, das darstellt, wie Probleme gelöst werden. Das REMEDIES Element muss eines oder mehrere der folgenden Elemente enthalten:

  <correct/>
  Errors und Fehler, die in Verbindung mit der Privacy Policy auftreten, werden von dem Service behoben.

  <money/>
  Falls der Service gegen seine Privacy Policy verstößt, wird dem Nutzer der in der menschenlesbaren Beschreibung aufgeführte Betrag erstattet oder der Wert des Schadens.

  <law/>
  Verstöße gegen Policy Statements werden gemäß den in der menschenlesbaren Form aufgeführten Gesetzten geregelt.

4.1.2.2 Properties der erhobenen Datenmenge

Das **STATEMENT** Element

Statements beschreiben Datenpraktiken, die auf bestimmte Daten angewandt werden. Das STATEMENT Element ist eine Art Container, das die Elemente PURPOSE, RECIPIENT, RETENTION, DATA-GROUP und wahlweise CONSEQUENCE und ein oder mehrere EXTENSIONs zusammen gruppiert. Auf alle Daten, die durch DATA-GROUP referenziert werden, werden die gleiche Datenpraktiken angewandt. Web Seiten können daher, Daten, die gleich behandelt werden, zusammen fassen und ein Statement für jede Gruppe kreieren.

Das **NON-IDENTIFIABLE** Element

Dieses Element wird nur dann benutzt, wenn keine Daten oder keine identifizierbaren Daten gesammelt werden. Daten werden dann als nicht identifizierbar eingestuft, wenn sie durch die Web Seite oder von Dritten nicht in Zusammenhang mit einer natürlichen Person gebracht werden können.

Das **CONSEQUENCE** Element

Mit diesem optionalen Element hat die Web Seite die Möglichkeit, in einer menschenlesbaren Form darzustellen, was passiert, falls ein Besucher der Web Seite einer Nutzung seiner Daten nicht zustimmt.

Das **PURPOSE** Element

Jedes STATEMENT muss ein PURPOSE Element enthalten, dass einen oder mehrer Zwecke der Datenerhebung oder Datennutzung angibt. Dabei müssen die Angaben einem oder mehreren vordefinierten Zwecken zugeordnet werden:

<current/>
Completion and Support of activity for which Data was Provided: Erfasste persönliche Daten werden zur Durchführung einer laufenden Aktivität benötigt, wie z. B.: das Aufgeben einer Online-Bestellung.

<admin/>
Web Site and System Administration: Erfasste Daten werden nur zur technischen Unterstützung der betreffenden Web Seite und des darunterliegenden System genutzt.

<develop/>
Research and Development: Erfasste Informationen werden für Marketing-Zwecke u. ä. ausgewertet.

<tailoring/>
One-time Tailoring: Informationen werden für eine Sitzung zur Anpassung oder Modifizierung des Designs oder der Inhalte einer Web-Seite verwendet.

<pseudo-analysis/>
Pseudonymous Analysis: Informationen werden benutzt, um ein Profil eines bestimmten Nutzers oder Computers zu erstellen. Diese Informationen werden mit einem pseudonymen Identifier ohne die identifizierbaren Daten verbunden.
Dieses Profil wird zu Forschungs-, Analyse- und Berichterstattungszwecken genutzt.

<pseudo-decision/>
Pseudonymous Decision: Informationen werden benutzt, um ein Profil eines bestimmten Nutzers oder Computers zu erstellen. Diese Informationen werden mit einem pseudonymen Identifier ohne die identifizierbaren Daten verbunden.
Diese Profil wird benutzt, um Entscheidung bzgl. des Nutzers zu treffen, z. B. das Web-Seiten Layout.

<individual-analysis/>
Individual Analysis: Informationen können benutzt werden, um die Gewohnheiten, Interessen oder andere Charakteristiken eines Nutzers herauszufinden und mit identifizierbaren Daten zu Forschungs-, Analyse- und Benachrichtigungszwecken zu kombinieren.

<individual-decision/>
Individual Decision: Informationen können benutzt werden, um die Gewohnheiten, Interessen oder andere Charakteristiken eines Nutzers herauszufinden und mit identifizierbaren Daten zu kombinieren, um Entscheidungen bzgl. des Nutzers zu treffen.

<contact/>
Contacting Visitors for marketing of Services or Products: Informationen werden benutzt, um mit dem Nutzer bzgl. der Promotion eines Produktes oder Services Kontakt aufzunehmen. Dies schließt die Benachrichtigung im Falle eines Updates der Web-Seite mit ein, nicht aber die direkte Antwort einer Frage oder eines Kommentars des Kundendienstes für eine einmalige Transaktion.

<historical/>
Historical Prevention: Informationen werden aufgrund eines Gesetzes oder einer Policy archiviert oder gespeichert.
Dieses Gesetz oder diese Policy muss im <DISPUTES> Element genannt werden.

<telemarketing/>
Contacting Visitors for Marketing of Services or Products Via Telephone: Informationen werden benutzt, um den Nutzer mittels Telefon bzgl. der Promotion eines Produktes oder Services zu kontaktieren.

<other-purpose>string</other-purpose>
Other Uses: Information werden zu anderen als den vordefinierten Zwecken genutzt.
Eine menschenlesbare Erklärung sollte in diesen Fällen bereitgestellt werden.

Jede Art von Zweck, außer current, kann wahlweise folgendes Attribut beinhalten:

required
besagt, dass dieser Zweck eine notwendige Maßnahme der Web-Seite ist. Dieses Attribut kann folgende Werte annehmen:

- always: Dieser Zweck ist immer gegeben; der Nutzer hat keine Entscheidungsmöglichkeit.
- opt-in: Daten können zu diesem Zweck nur genutzt werden, wenn der Nutzer seine Zustimmung dazu gibt.
- opt-out: Daten können generell zu diesem Zweck genutzt werden, außer der Nutzer erlaubt es ausdrücklich nicht

Das **RECIPIENT** Element

Jedes STATEMENT Element muss ein RECIPIENT Element, das ein oder mehrere Empfänger der gesammelten Daten angibt, beinhalten. Web-Seiten müssen ihre Empfänger in ein oder mehrere der sechs vordefinierten Klassen einordnen. RECIPIENT muss ein oder mehrere der folgenden Werte annehmen:

<ours>
Ourselves and/or our entities acting as our agents or entities for whom we are acting as an agent: Ein Agent ist in diesem Zusammenhang definiert als dritte Partei, die exklusiv für den Service Provider zur genannten Zweckerfüllung Daten verarbeitet.

<delivery>
Delivery services possibly following different practices: Legale Einheiten, die einem Zustelldienst nachgehen, könnten die Daten zu einem anderen Zweck als dem genannten nutzen. Dieser Wert sollte auch genutzt werden, falls die Praktiken des Zustelldienstes nicht bekannt sind.

<same>
Legal entities following our practices. Legale Einheiten, die die Daten auf ihre eigene Verantwortung mit gleichen Praktiken behandeln.

<other-recipient>
Legal entities following different practices: Legale Einheiten, die gezwungen durch und verantwortlich gegenüber dem Service Provider sind, aber die Daten zu einem anderen Zweck als dem vom Service Provider genannten nutzen.

<unrelated>
Unrelated third parties: Legale Einheiten, deren Datenpraktiken dem Service Provider nicht bekannt sind.

<public>
Public Fora: Öffentliche Fora wie z. B. öffentliche Direktorien oder kommerzielle CD-ROM Verzeichnisse .

Das **RETENTION** Element

Jedes STATEMENT Element muss ein RETENTION Element enthalten, das die Maßnahmen zur Erhaltung der Daten, die in diesem Statement aufgeführt werden, anzeigt. Das RETENTION Element kann dabei eines der folgenden Werte annehmen:

<no-retention/>
Informationen werden nur für den Zeitraum der Transaktion benötigt. Sie werden danach gelöscht.

<stated-purpose/>
Informationen werden zur Zweckerfüllung bewahrt und werden zum frühest möglichen Zeitpunkt gelöscht.

<legal-requirement/>
Informationen werden zur Zweckerfüllung gespeichert, allerdings länger als notwendig, da es diesbezüglich gesetzliche Vorschriften gib, die eine weitere Speicherung fordern.

<business-practices/>
Informationen werden aufgrund der genannten Geschäftpraktiken vom Service Provider gespeichert. Web-Seiten müssen hier eine Löschungszeitpunkt-Tabelle einführen.

<indefinitely/>
Informationen werden auf unbegrenzte Zeit gespeichert.

Das **DATA-GROUP** und **DATA** Element

Jedes STATEMENT Element muss mindestens ein DATA-GROUP Element enthalten, das ein oder mehrere DATA Elemente umfasst.

Mit **<DATA-GROUP>** können Daten zusammengefasst werden, auf die die gleichen Datenschutzpraktiken angewandt werden.

<DATA> beschreibt die Daten selbst, die erhoben werden /bgl. Abschnitt 4.1.2.3).

Kategorien und das **CATEGORIES** Element

CATEGORIES sind Elemente innerhalb des Data Elements, die dem User und dem User Agent Hinweise über den geplanten Gebrauch von Daten geben können. **Cathegories** sind dabei keine Datenelemente; sie geben dem User vielmehr die Möglichkeit, generellere Aussagen über Präferenzen und Regeln zu machen.

Folgende Elemente werden benutzt, um Datenkategorien zu kennzeichnen.

<phyical/>
Physical Contact Information: Informationen, mit den man mit dem Nutzer in Kontakt treten kann, wie z. B. Telefonnummer oder Adresse.

<online/>
Online Contact Information: Informationen, die für eine Onlinekontaktierung benötigt werden (e-mail-Adresse).

<uniqueid/>
Unique Identifier: Daten, die der Identifikation einer Person dienen.

<purchase/>
Purchase Information: Informationen, die durch den Kauf eines Produktes oder Dienstes generiert werden, inklusive Informationen über die Zahlungsmodalitäten.

<financial/>
Financial Information: Daten über die finanzielle Situation des Nutzers, wie z. B. Kontostand, Zahlungen oder Überziehungen, Kreditkartennummern.

<computer/>
Computer Information: Informationen über das verwendete Computersystem, wie z. B. Betriebssystem, Browsertyp oder IP-Adresse.

<navigation/>
Navigation and Click-stream Data: "Passive" Daten, die beim Browsen einer Web-Seite erzeugt werden, wie z. B. besuchte Web-Seiten oder Verweildauer auf einer Seite.

<interactive/>
Interactive Data: Daten, die ein Benutzer während eines Web-Besuchs „aktiv" eingibt, wie z.B. Anfragen in Suchmaschinen oder Einkäufe im Netz.

<demographic/>
Demographic and Socioeconomic Data: Daten zu charakteristischen Merkmalen einer Person, wie z. B. Alter, Geschlecht oder Einkommen.

<content/>
Content: Umfasst Inhalte einer Kommunikation, wie z. B. Text der E-mail.

<state/>
State Management Mechanisms: Mechanismen, die Benutzer beim Besuch einer Web-Seite identifizieren, wie z. B. Cookies.

<political/>
Political Information: Mitgliedschaft in oder Sympathien für z. B. religiöse Gruppen, Gewerkschaften usw..

<health/>
Health Information: Informationen über die Gesundheit sowohl physischer als auch mentaler Art, sexuelle Neigungen usw..

<preference/>
Preference Data: Daten über Vorlieben und Abneigungen eines Nutzer, wie z. B. Farben, Musikrichtung usw..

<location/>
Location Data: Informationen über den aktuellen Aufenthaltsort, wie z. B. GPS.

<goverment/>
Goverment-issued Identifieres: Identifieres, die von der Regierung zur eindeutigen Identifizierung des Einzelnen herausgegeben werden.

<other-category>string</other-category>
Other: Umfasst alle personenbezogenen Datenarten, die nicht durch die aufgeführten Datenkategorien abgedeckt werden; in diesem Fall muss eine menschenlesbare Erklärung gegeben werden.

Da das P3P Vokabular sehr umfangreich ist, sind in den Tabellen 4.1 und 4.2 die wichtigsten Elemente, deren Kurzbeschreibung und ihr möglicher Wertebereich zusammengefasst worden:

Element	Kurzbeschreibung	Wertebereich
ENTITY	Angaben drüber, um wen es sich handelt	Das Business Data Schema wird benutzt, um diese Angaben, wie Name, Adresse etc. zu machen
ACCESS	Können auf Daten zugegriffen werden? Wenn ja, auf welche (grobe Einstufung)?	nonident, all, contact-and-other, ident-contact, other-ident, none
DISPUTES	An wen kann man sich bei Regelverstössen wenden?	service, independent, court, law
REMEDIES	Wie werden Regelverstösse behoben?	correct, money, law
EXTENSION	Element, um das P3P Vokabular zu erweitern	

Tabelle 4.1: Übersicht allgemeiner Properties

Element	Kurbeschreibung	Wertebereich
PURPOSE	Zu welchem Zweck werden die Daten erhoben?	current, admin, develop, tailoring, pseudo-analysis, pseudo-decision, individual-analysis, individual-decision, contact ,historical, telemarketing, other-purpose
RECIPIENTS	Wer erhält diese Daten noch?	ours, delivery, same, other-recipient, unrelated, public
RETENTION	Wie lange werden die Daten gespeichert?	no-retention, stated-purpose, legal-requirement, business-practices, indefinitely
DATA-GROUP	Um welche Daten handelt es sich?	Es können entweder Werte aus dem Base Data Schema ausgewählt werden (vgl. Abschnitt 4.1.2.3) oder man gibt nur die Datenkategorie an
CATEGORIES	Unterteilung der Daten zu Kategorien	Physical, online, uniqueid, purchase, financial, computer, navigation, interactive, demographic, content, state, political, health, preference, location, goverment, other-category
EXTENSION	Element um das P3P Vokabular zu erweitern	

Tabelle 4.2: Übersicht datenspezifischer Properties

4.1.2.3 Base Data Schema

Ein Datenschema ist eine Beschreibung der Datenmenge. P3P liefert einen Weg, wodurch Dienste mit User Agents über die Daten, die sie sammeln kommunizieren können. Ein Datenschema wird durch eine Anzahl von Datenelementen, welches spezifizierte Einheiten der zu sammelnden Daten sind, aufgebaut.

Datenelemente sind in Hierarchien organisiert. Ein Datenelement „erbt“ automatisch alle Datenelemente in der Hierarchie unter ihm. P3P hat ein Datenschema definiert, das P3P *Base Data Schema*. Es beinhaltet eine Reihe von Datenelementen, die oft von Diensten benutzt werden.

Die Dienste können allerdings auch eigene, neue Datenelemente deklarieren, indem sie ein eigenes Datenschema kreieren und veröffentlichen. Dies kann mittels des <DATASCHEMA> Elementes geschehen.

Alle P3P Implementationen müssen das P3P Base Data Schema verstehen. Die einzelnen, vom Base Data Schema erfassten Elemente sehen folgendes vor:

- Informationen über den User
- Informationen über dritte Parteien
- Informationen über die Firma selbst
- Dynamische Daten

Die einzelnen Datenelemente werden dabei einzelnen Kategorien zugeordnet, um auch generelle Aussagen zu ermöglichen (z.B. es werden nur clickstream data gesammelt).

Third Party Data

Mit dieser Datenmenge können sowohl der User als auch die Geschäftseinheit Informationen Dritter bereitstellen. Beim User könnte dies z. B. bei der Bestellung eines Geschenks eine andere Lieferadresse sein.

Die Datenmenge für Third Party Data ist identisch mit dem User Data Set**.**

Business Data

Die Business Data Menge spezifiziert die Informationen über den Services selbst. Bei P3P wird diese Datenmenge in erster Linie dazu benutzt, um Informationen über die Geschäftseinheit, die für die Policy zuständig ist, zu präsentieren (Tab. 4.3).

business	**Category**	**Structure**	**Short display name**
name	Demographic and Socioeconomic Data	*unstructured*	Organization Name
department	Demographic and Socioeconomic Data	*unstructured*	Department or Division of Organization
cert	Unique Identifiers	certificate	Organization Identity Certificate
contact-info	Physical Contact Information, Online Contact Information, Demographic and Socioeconomic Data	contact	Contact Information for the Organization

Tabelle 4.3: Business Data

User Data

Die User Datenmenge beinhaltet folgende Informationen über den User:

user	**Category**	**Structure**	**Short display name**
name	Physical Contact Information, Demographic and Socioeconomic Data	personname	User's Name
bdate	Demographic and Socioeconomic Data	date	User's Birth Date
login	Unique Identifiers	login	User's Login Information
cert	Unique Identifiers	certificate	User's Identity Certificate
gender	Demographic and Socioeconomic Data	*unstructured*	User's Gender (Male or Female)
employer	Demographic and Socioeconomic Data	*unstructured*	User's Employer
department	Demographic and Socioeconomic Data	*unstructured*	Department or Division of Organization where User is Employed
jobtitle	Demographic and Socioeconomic Data	*unstructured*	User's Job Title
home-info	Physical Contact Information, Online Contact Information, Demographic and Socioeconomic Data	contact	User's Home Contact Information
business-info	Physical Contact Information, Online Contact Information, Demographic and Socioeconomic Data	contact	User's Business Contact Information

Tabelle 4.4: User Daten

Dynamic Data

Manchmal ist es notwendig, Datenelemente zu spezifizieren, die keinen festen Wert haben. Alle diese Daten werden unter der Dynamic Data Menge zusammengefasst. Darunter gibt es folgende Aufteilung:

dynamic	Category	Structure	Short display name
clickstream	Navigation and Click-stream Data, Computer Information	loginfo	Click-stream Information
http	Navigation and Click-stream Data, Computer Information	httpinfo	HTTP Protocol Information
clientevents	Navigation and Click-stream Data	*unstructured*	User's Interaction with a Resource
cookies	*(variable-category)*	*unstructured*	Use of HTTP Cookies
miscdata	*(variable-category)*	*unstructured*	Miscellaneous Non-base Data Schema Information
searchtext	Interactive Data	*unstructured*	Search Terms
interactionrecord	Interactive Data	*unstructured*	Server Stores the Transaction History

Tabelle 4.5: Dynamic Data

4.1.3 Beispiel einer P3P Policy

Um zu verdeutlichen, wie eine P3P Policy im XML-Format aussieht, ist nachfolgend ein Beispiel aus der P3P Spezifikation übernommen worden. Zunächst wird beschrieben, was ausgesagt werden soll. Danach folgt die Policy im XML-Format.

Beispiel einer Privacy Policy der fiktiven Firma „CatalogExample:

„Bei CatalogExamples wird auf Ihre Privatsphäre Wert gelegt. Wir werden nie Ihre Kreditkartennummer oder andere finanzielle Informationen an Dritten weiterleiten. Nur mit Ihrer ausdrücklichen Erlaubnis werden wir Informationen mit ausgewählten Marketing Partnern austauschen. Diese Partner entsprechen entweder Ihren Angaben in Ihrer Präferenz oder Ihrem vorangegangen Kaufverhalten. Je mehr wir über ihre Vorlieben und Abneigungen wissen, umso besser können wir Angebote auf Sie abstimmen.

CatalogExample ist Lizenzinhaber des PrivacySealExample Programmes. Das PrivacySealExample Programm sichert Ihre Privatsphäre, indem es Web Seiten Lizenzinhabern zu einem hohen Privacy Standard anhält und mit unabhängigen Revisoren die Einhaltung der Praktiken beaufsichtigt.

Bei Fragen wenden Sie sich bitte an:

CatalogExample
4000 Lincoln Ave.
Birmingham, MI 4800 USA
e-mail : catalog@example.com
Telefon: 01-248-392-6753

Falls wir auf Anfragen Ihrerseits nicht reagieren oder wir nicht zu Ihrer Zufriedenheit reagiert haben, können Sie PrivacySealExample unter http://privacyseal.org/privacyseal kontaktieren. CatalogExample wird alle Fehler oder Fehlverhalten, die in Zusammenhang mit der Privacy Policy auftreten, korrigieren.

Wenn Sie auf unserer Seite surfen, dann sammeln wir folgendes:

- Grundinformationen über Ihren Computer und Verbindungen, um sicher zu gehen, dass wir Ihnen die richtige Informationen geben und aus Sicherheitsgründen; und
- zusammengefasste Informationen darüber, auf welche Seiten unsere Besucher zugreifen oder besuchen, um unsere Seite zu verbessern.

Wenn Sie einen Artikel kaufen, werden wir Sie um zusätzliche Informationen bitten. Diese beinhalten:

- Ihren Namen und Adresse, so dass wir Ihnen Ihren Einkauf liefern können und sie in Zukunft besser kontaktieren können;
- Ihre e-mail Adresse und Telefonnummer, um sie zu erreichen;
- einen Login und Passwort, der benutzt wird, um Ihre Informationen zukünftig aktualisieren zu können;
- kontenspezifische Informationen, um Ihren Einkauf zu vervollständigen (wenn Sie wünschen, kann dies für einen zukünftigen Einkauf gespeichert werden);
- wahlweise können Sie auch andere demographische Informationen eingeben, so dass wir zukünftig den Service besser auf Sie abstimmen können.

Wir geben Ihnen auch die Möglichkeit Ihre Zustimmung dazu zu geben, ob sie e-mails, Anrufe oder Werbebriefe von CatalogExample oder von unseren ausgewählten Marketing Partnern, die ähnliche Privacy Praktiken wie wir verfolgen, erhalten wollen oder nicht. Um diese Werbemassnahmen zu erhalten, klicken Sie bitte auf das dafür vorgesehene Feld. Sie können diese Angabe jederzeit widerrufen, indem Sie Ihre Eingabe ändern.

Veränderung und Aktualisierung persönlicher Informationen
Kunden können alle Ihre persönlichen Konteninformationen ändern, indem sie auf den Preference Abschnitt von CatalogExample auf http://catalog.example.com/prferences.html gehen. Sie können sowohl Ihre Adresse, Telefonnummer, e-mail Adresse und Passwort als auch ihre Privacy Settings ändern.

Cookies
CatalogExample benutzt Cookies nur, um herauszufinden, ob Sie schon CatalogExample Kunde in der Vergangenheit waren und falls dem so ist, den Dienst Ihren Surf- und Einkaufsgewohnheiten der Vergangenheit anzupassen. Wir speichern weder persönliche Daten in Cookies, noch teilen oder verkaufen wir jegliche Informationen am Dritte oder Tochtergesellschaften.

Datenspeicherung
Wir behalten die Informationen über Sie und Ihr Kaufverhalten solange sie unser Kunde sind. Falls Sie innerhalb eines Jahres keinen Einkauf bei uns tätigen, werden Ihre Informationen aus unserer Datenbank gelöscht."

Im nachfolgenden tabellarischen Überblick soll zunächst die Aussage dieser Policy schematisiert werden. Die Policy teilt sich in zwei grobe Bereiche auf. Es gibt die allgemeinen Angaben und die datenspezifischen Angaben, welche sich noch in Unterbereiche aufteilen lassen. Zunächst die allgemeinen Properties der Policy:

P3P Element	**Beschreibung**	**Wert**	**Bemerkung/Sonstiges**
ENTITY	Wer bin ich?	CatalogExample 4000 Lincoln Ave. Birmingham, MI 48009 USA catalog@example.com 01-248-392-6753	
ACCSESS	Kann man grundsätzlich auf Daten zugreifen? Wenn ja, auf welche?	contact-and-other	Zugriff auf identifizierbare online und physische Kontaktinformationen wird erlaubt.
DISPUTES-GROUP	An wen kann man sich bei Unstimmigkeiten bzgl. der Policy wenden?	independent	Man soll sich an die unabhängige Organisation „PrivacySealExample" unter http:// www.PrivacySeal.example.org wenden.
REMEDIES	Wie werden Fehler korrigiert?	Correct	Fehler werden einfach korrigiert.

Tabelle 4.6 Schema einer Policy, allgemeine Properties

Der datenspezifische Teil der Policy gliedert sich in sechs Unterabschnitte auf, da verschiedene Datenmengen zu unterschiedlichen Zwecken gespeichert werden. Diese Bereiche gliedern sich wie folgt auf:

1. Es werden Informationen zu administrativen Zwecken gesammelt und um die Web Seite besser zu sichern und dem Kunden anzupassen. Es handelt sich hierbei um dynamische Daten. Diese Daten werden nicht weitergegeben und nur zu diesem Zweck benutzt. Sobald die Daten zu diesem Zweck nicht mehr gebraucht werden, werden sie gelöscht.
2. Bestimmte Daten werden beim Kauf eines Produktes benötigt. Sie werden nur zu diesem Zweck gebraucht und werden nicht an Dritte weitergegeben. Sobald die Daten zu diesem Zweck nicht mehr gebraucht werden, werden sie gelöscht. Es handelt sich dabei um die Adresse, Telefonnummer, e-mail-Adresse, Login und das Passwort.
3. Falls gewünscht wird, wird dem Kunden ausgewählte Werbung zugesandt. Der Kunde muss dazu ausdrücklich seine Zustimmung geben. Die Werbung wird auf ihn abgestimmt. Dritte erhalten diese Informationen nur, wenn die Zustimmung des Kunden hierzu vorliegt. Bei diesen Daten handelt es sich um die Adresse, die Telefonnummer und die e-mail-Adresse. Zu jedem Punkt soll der Kunde seine Zustimmung geben können.

4. Der Kunde hat die Möglichkeit über ein Passwort auf seine eigenen Daten zuzugreifen. Hierbei handelt es sich also um eindeutig identifizierbare Daten.
5. Falls der Kunde seine Zustimmung gibt, kann die Web Seite besser auf seine Interessen abgestimmt werden. Dazu ist das Geschlecht und das Geburtsdatum nötig.
6. Aufgrund von Informationen aus vergangenen Besuchen auf der Web Seite, kann die Seite besser auf den Kunden abgestimmt werden. Herzu werden dynamische Daten verwandt.

Diese sechs Aussagen können schematisiert wie folgt dargestellt werden.

State-ment Nr.	PURPOSE	RECIPIENT	RETENTION	DATA-GROUP	CATE-GORIES	Son-stige
1	admin, develop	ours	stated-purpose	dynamic.clickstream, dymanic.http.useragent		
2	current	ours	stated-purpose	user.name, user.home-info.postal user.home-info.telecom.telephone user.business-info.postal, user.business-info.telecom.telephone user.home-info.online.email, user.login.id, user.login.password, dynamic.miscdata	purchase	
3	contact, individual-decision, tailoring	ours, same	stated-purpose	user.name, user.home-info.postal user.home-info.telecom.telephone user.business-info.postal, user.business-info.telecom.telephone user.home-info.online.email		opt-in,
4	individual-decision	ours	stated-purpose	dynamic.miscdata	uniqueid	opt-in
5	pseudo-decision, tailoring	ours	stated-purpose	user.bdate.ymd.year, user.gender		opt-in
6	tailoring, develop	ours	stated-purpose	1) dynamic.cookies 2) dynamic.miscdata	1) state 2) pre-ference	

Tabelle 4.7: Schema einer Policy, datenspezifische Properties

Die dazugehörige P3P-Formulierung ist in Abbildung 4.2 dargestellt.

```
POLICIES xmlns="http://www.w3.org/2002/01/P3Pv1">
 <POLICY name="forShoppers"

  discuri="http://www.catalog.example.com/Privacy/PrivacyPracticeShop
          ping.html"
  opturi="http://catalog.example.com/preferences.html"
          xml:lang="en">
  <ENTITY>
   <DATA-GROUP>
    <DATA ref="#business.name">CatalogExample</DATA>
    <DATA ref="#business.contact-info.postal.street">4000 Lincoln
                  Ave.</DATA>
    <DATA ref="#business.contact-info.postal.city">Birmingham</DATA>
    <DATA ref="#business.contact-info.postal.stateprov">MI</DATA>
    <DATA ref="#business.contact-info.postal.postalcode">48009</DATA>
    <DATA ref="#business.contact-info.postal.country">USA</DATA>
    <DATA ref="#business.contact-
                  info.online.email">catalog@example.com</DATA>
    <DATA ref="#business.contact-
                  info.telecom.telephone.intcode">1</DATA>
    <DATA ref="#business.contact-
                  info.telecom.telephone.loccode">248</DATA>
    <DATA ref="#business.contact-
                  info.telecom.telephone.number">3926753</DATA>
   </DATA-GROUP>
  </ENTITY>
  <ACCESS><contact-and-other/></ACCESS>
  <DISPUTES-GROUP>
   <DISPUTES resolution-type="independent"
     service="http://www.PrivacySeal.example.org"
     short-description="PrivacySeal.example.org">
    <IMG src="http://www.PrivacySeal.example.org/Logo.gif"
         alt="PrivacySeal's logo"/>
    <REMEDIES><correct/></REMEDIES>
   </DISPUTES>
  </DISPUTES-GROUP>
  <STATEMENT>
   <CONSEQUENCE>
     We record some information in order to serve your request
     and to secure and improve our Web site.
   </CONSEQUENCE>
   <PURPOSE><admin/><develop/></PURPOSE>
   <RECIPIENT><ours/></RECIPIENT>
   <RETENTION><stated-purpose/></RETENTION>
   <DATA-GROUP>
    <DATA ref="#dynamic.clickstream"/>
    <DATA ref="#dynamic.http.useragent"/>
   </DATA-GROUP>
  </STATEMENT>
  <STATEMENT>
   <CONSEQUENCE>
     We use this information when you make a purchase.
   </CONSEQUENCE>
   <PURPOSE><current/></PURPOSE>
   <RECIPIENT><ours/></RECIPIENT>
   <RETENTION><stated-purpose/></RETENTION>
   <DATA-GROUP>
    <DATA ref="#user.name"/>
    <DATA ref="#user.home-info.postal"/>
    <DATA ref="#user.home-info.telecom.telephone"/>
    <DATA ref="#user.business-info.postal"/>
    <DATA ref="#user.business-info.telecom.telephone"/>
    <DATA ref="#user.home-info.online.email"/>
```

```
   <DATA ref="#user.login.id"/>
   <DATA ref="#user.login.password"/>
   <DATA ref="#dynamic.miscdata">
    <CATEGORIES><purchase/></CATEGORIES>
   </DATA>
  </DATA-GROUP>
 </STATEMENT>
 <STATEMENT>
  <CONSEQUENCE>
    At your request, we will send you carefully selected marketing
    solicitations that we think you will be interested in.
  </CONSEQUENCE>
  <PURPOSE>
   <contact required="opt-in"/>
   <individual-decision required="opt-in"/>
   <tailoring required="opt-in"/>
  </PURPOSE>
  <RECIPIENT><ours/><same required="opt-in"/></RECIPIENT>
  <RETENTION><stated-purpose/></RETENTION>
  <DATA-GROUP>
   <DATA ref="#user.name" optional="yes"/>
   <DATA ref="#user.home-info.postal" optional="yes"/>
   <DATA ref="#user.home-info.telecom.telephone" optional="yes"/>
   <DATA ref="#user.business-info.postal" optional="yes"/>
   <DATA ref="#user.business-info.telecom.telephone" optional="yes"/>
   <DATA ref="#user.home-info.online.email" optional="yes"/>
  </DATA-GROUP>
 </STATEMENT>
 <STATEMENT>
  <CONSEQUENCE>
    We allow you to set a password so that you
    can access your own information.
  </CONSEQUENCE>
  <PURPOSE><individual-decision required="opt-in"/></PURPOSE>
  <RECIPIENT><ours/></RECIPIENT>
  <RETENTION><stated-purpose/></RETENTION>
  <DATA-GROUP>
   <DATA ref="#dynamic.miscdata">
    <CATEGORIES><uniqueid/></CATEGORIES>
   </DATA>
  </DATA-GROUP>
 </STATEMENT>
 <STATEMENT>
  <CONSEQUENCE>
    At your request, we will tailor our site and
    highlight products related to your interests.
  </CONSEQUENCE>
  <PURPOSE>
    <pseudo-decision required="opt-in"/>
    <tailoring required="opt-in"/>
  </PURPOSE>
  <RECIPIENT><ours/></RECIPIENT>
  <RETENTION><stated-purpose/></RETENTION>
  <DATA-GROUP>
   <DATA ref="#user.bdate.ymd.year" optional="yes"/>
   <DATA ref="#user.gender" optional="yes"/>
  </DATA-GROUP>
 </STATEMENT>
 <STATEMENT>
  <CONSEQUENCE>
    We tailor our site based on your past visits.
  </CONSEQUENCE>
  <PURPOSE><tailoring/><develop/></PURPOSE>
```

```
   <RECIPIENT><ours/></RECIPIENT>
   <RETENTION><stated-purpose/></RETENTION>
   <DATA-GROUP>
    <DATA ref="#dynamic.cookies">
     <CATEGORIES><state/></CATEGORIES>
    </DATA>
    <DATA ref="#dynamic.miscdata">
     <CATEGORIES><preference/></CATEGORIES>
    </DATA>
   </DATA-GROUP>
  </STATEMENT>
</POLICY>
```

Abbildung 4.2: Beispiel einer P3P Policy

4.1.4 P3P und Erweiterungsmöglichkeiten

P3P liefert einen flexiblen Mechanismus, um seine Syntax und Semantiken zu erweitern. Dies geschieht mittels des EXTENTION Elementes. Mit diesem Element können Teile einer Policy gekennzeichnet werden, die zu einer Erweiterung gehören. Die Bedeutung von EXTENTION erklärt sich selbst.

optional

Dieses Attribut gibt an, ob die Erweiterung Pflicht oder wahlweise angewandt werden kann. Eine Pflichterfüllung wird durch den Wert „no“ ausgedrückt. Dies bedeutet, dass Anwendungen, die diese Erweiterung nicht verstehen, auch die gesamte Policy nicht verstehen werden. Wird der Wert mit „yes“ besetzt, so kann die Policy auch ohne ein Verständnis der Erweiterung verstanden werden. Der Inhalt von EXTENTION kann einfach ignoriert werden.

Das optional Attribut muss nicht angegeben werden, sein Wert ist in diesem Fall „yes“.

4.14.1 Beispiel einer Erweiterung

Abbildung 4.3 zeigt den XML-Code eines EXTENSIONs. Bei diesem Beispiel soll ausgedrückt werden, in welchem Land sich der Server der Firma CatalogExample befindet. Dies könnte durch eine Erweiterung, das mit optional=“YES“ belegt ist, da die restliche Policy auch ohne diese Erweiterung nachvollziehbar ist, wie folgt ausgedrückt werden:

```
<POLICY>
<EXTENSION optional="yes">
<ORIGIN xmlns="http://www.catalog.example.com/P3P/origin"
country="USA"/>
</EXTENSION>
...
</POLICY>
```

Abbildung 4.3: Beispiel einer EXTENSION Formulierung

Das xmlns Attribut ist dabei von besonderer Bedeutung, da es den Namensraum zur Interpretation der Elemente und Attribute, die in diesem EXTENSION benutzt werden, spezifiziert [17]. Die URI des Namensraumes ist dabei die eindeutige Identifikation für die

XML-Elemente, die in dem EXTENSION benutzt werden. Service Provider können ausserdem eine Beschreibung des EXTENSIONs in der zugehörigen URI einbinden.

4.2 APPEL Grundlagen

Nachdem im vergangenen Kapitel aufgezeigt wurde, inwieweit serviceseitige Datenschutzpraktiken mittels des P3P-Vokabulars darstellbar sind, soll in diesem Abschnitt die userseitige Möglichkeit zur Darstellung von Datenschutzpräferenzen beschrieben werden.

Genauso wie es für eine Policy ein bestimmtes Vokabular gibt, muss es für die Präferenzen des Users auch ein Vokabular geben, mit dem er einerseits seine Präferenzen ausdrücken kann und das anderseits für einen Wertevergleich bei der Überprüfung auf Übereinstimmungen zwischen Service und User Einstellungen, verstanden wird.

Das W3C hat hierzu in ihrem Working Draft vom 26 Februar 2001 **APPEL** 1.0 (*A P3P Preference Exchange Language 1.0*) vorgestellt [14]. Dieses Dokument stellt eine Ergänzung zu den P3P Spezifikationen dar; es befindet sich allerdings noch im Entwurfsstadium. Mit dieser Sprache kann der User seine Präferenzen mittels einer Menge von Präferenz-Regeln, dem sogenannten *Ruleset*, ausdrücken. Diese können dann benutzt werden, um automatische oder halb-automatische Entscheidungen bzgl. der Akzeptanz von maschinenlesbaren Privacy Policies von P3P-fähigen Web Seiten zu treffen.

Vom W3C wird dabei primär davon ausgegangen, dass der User die von unabhängigen Organisationen vordefinierten Rulesets importiert und benutzt, da es schwierig sein wird, anspruchsvolle Präferenzen zu erstellen.

4.2.4 Konzept

Bei der Konzipierung wurden folgende Anforderungen an APPEL gestellt:

- APPEL Regeln sollten in der Lage sein, alles was auch mit P3P ausgedrückt werden kann, auszudrücken.
- APPEL sollte in der Lage sein, auch Situationen, in denen keine P3P Policy vorliegt, aufzufangen.
- APPEL Regeln sollten folgende Verhalten unterstützen: r*equest, don´t request* und *limit request* (vgl. S. 50). Ausserdem sollten auch zusätzliche Verhalten definierbar sein.

Dabei wurde auch der Umfang von APPEL festgelegt:

- APPEL Regeln sollten keine anspruchvollen Formulierungen aufgrund von komplexen Datenelementen innerhalb einer P3P Policy erlauben (z.B. eine Regel, die es nur erlaubt Postleitzahlen zu speichern, wenn auch der ganze Name gespeichert wird).
- APPEL braucht nicht in der Lage sein, ein Ranking bei mehreren möglichen Policies vorzunehmen. Vielmehr sollten nötige Regeln ausgedrückt werden können, die für verschiedene Policies ein bestimmtes Verhalten auslösen. Falls mehrere P3P Policies

vorhanden sind, sollten diese einzeln an den *Rule Evaluator* (vgl. S. 50) übermittelt werden.

- APPEL braucht nicht in der Lage sein, Verhandlungsstrategien zwischen User und Service auszudrücken.

4.2.2 Grundbegriffe

Zunächst werden Begriffe eingeführt, die vom W3C in seinem Working Draft [14] spezifiziert werden und auch in dieser Arbeit benutzt werden.

Begriffe (in alphabetischer Reihenfolge)

behavior
: Aktivität, die aufgrund eines erfolgreichen Matches bzgl. eines Rules vorgenommen werden sollte. APPEL unterstützt sowohl drei Standardbehaviors (request, limited und block, vgl. S. 50) als auch einen optionalen prompt Parameter.

connective
: Ein Attribut zu einem Ausdruck, der angibt wie *conntained expressions* in APPEL verglichen werden. Es unterstützt sechs *connectives*: or, and, non-or, non-and, or-exact und and-exact (VGL: S. 53)

evidence
: Eine P3P Anwendung liefert einem APPEL Rule Evaluator mit einem APPEL *Ruleset* und verschiedenen Teilen von *evidence*. Dieses *evidence* kann z. B. die URI und eine P3P Policy des Services beinhalten.

expression
: Dies ist eine Komponente eines Regel, das zu TRUE oder FALSE im Bezug auf ein *evidence* ausgewertet wird. Ein Expression beinhaltet:

    1. einen Element Identifier (Element Name)
    2. keinen oder mehrere attribute Expressions
    3. keinen oder mehrere contained Expressions
    4. ein optionales Connective

expression, attribute
: Ein Attribut-Werte Paar in einem *expression*. Sie können benutzt werden, um Werte, zweier Strings, die von Anführungszeichen umgeben sind, zu vergleichen, oder um das Vorhandensein oder die Abwesenheit von einem bestimmten Attribut zu testen, ohne den wirklichen Wert dessen zu überprüfen (z. B. bei Wildcards). Wildcards („*“) können benutzt werden, um Matches über eine Reihe von Werten durchzuführen (z. B. <DATA name=“User.*“, d. h. alle Nachfolgerknoten von dem Oberknoten „User“ sind gemeint)

expression, contained
: Ein Ausdruck, der in einem anderen Ausdruck enthalten ist. Damit ein Ausdruck zu einem erfolgreichen Match führt, müssen einige oder auch alle seine *contained expression* erfolgreich matchen.

expression, degenerate
: Ein Ausdruck, der immer zu TRUE ausgewertet wird (vgl. S. 53).

rule
: Der formale Ausdruck für die Präferenzen des Users. *Rules* drücken die Präferenzen des Users aus, die dann mit der P3P Policy des Service verglichen werden. Durch das *behavior* eines *rules* wird das bei einem erfolgreichem Match resultierende Verhalten definiert.

rule evaluator
: Prozess, der für den Vergleich von User Präferenzen mit einer P3P Policy verantwortlich ist.

ruleset
: Eine Menge von r*ules*, die alle User Präferenzen definiert.

user agent
: Ein Programm, das anstelle des Users agiert. Er vergleicht die Präferenzen des Users mit der Policy und handelt entsprechend der Präferenz des Users.

4.2.3 Vorgehensweise

Bei der Auswertung von Policy und Präferenzen wird ein *rule evaluator* (vgl. S. 48) benutzt. Dieser wird durch die P3P Applikation aktiviert. Es versorgt den *evaluator* mit verschiedenen Teilen der P3P Policy, dem sogenannten *evidence* (vgl. S. 48), und einem *ruleset* (vgl. S. 48), um diese zu bearbeiten.

Nach der Auswertung der Eingabe gibt der *evaluator* das geforderte Verhalten der zutreffenden Präferenz und eine Kopie der zutreffenden Policy zurück. Dabei muss die Policy nicht identisch mit der original Policy sein, da optionale Elemente eventuell herausgenommen worden sind.

Falls ein *rule* eine Übereinstimmung in einem Policy findet, so liefert es für dieses Regel ein bestimmtes Verhalten zurück. Es gibt drei Verhaltensregeln. Anwendungen sollten dabei das Verhalten wie folgt interpretieren:

- „***request***“: Die Policy ist akzeptabel. Falls eine URI angeben ist, sollte auf sie zugegriffen werden.
- „***limited***“: Die Policy ist einigermaßen akzeptabel. Falls eine URI angegeben ist, sollte auf sie zugegriffen werden. Allerdings sollte der Zugriff begrenzt sein, d. h. alle bis auf die absolut notwendigen Headers sollten unterdrückt werden.
- „***block***“: Die Policy ist nicht akzeptabel. Falls eine URI angegeben ist, sollte nicht auf sie zugegriffen werden. Hierbei muss beachtet werden, dass eventuell schon auf die URI zugegriffen wurde, um auf die Policy zuzugreifen. In diesen Fällen muss das aufrufende Programm entscheiden, welche Informationen dem User präsentiert werden.

Zusätzlich gibt es noch ein *prompt* Attribut, dass wie folgt von Anwendungen interpretiert werden sollte:

- prompt = „no“: Das Verhalten sollte ohne Verzögerung ausgeführt werden, d. h. der User braucht nicht mit in die Entscheidungsfindung einbezogen werden. Nichtsdestoweniger können Anwendungen Hinweise bzgl. der Auswertung eines *rules* liefern, die allerdings keine Aktion des Users erfordern.
- prompt = “yes“: Der User sollte bei einer Entscheidung bzgl. des Verhaltens, das aufgrund eines zutreffenden *rules* ausgelöst wird, mit einbezogen werden.

Grundsätzlich werden Regeln in Zusammenhang mit Policies ausgewertet. Eine Regel wird mit *True* ausgewertet, wenn alle in ihm befindlichen Ausdrücke Übereinstimmungen in der Policy finden.

Dabei werden die Regeln in der Reihenfolge ihres Vorkommens abgearbeitet. Daher ist die Reihenfolge der Regeln wesentlich, damit auch alle Regeln beachtet werden und nicht schon vorher Aktionen veranlasst werden.

4.2.4 Vokabular

Da APPEL *Rulesets* Präferenzen bzgl. P3P Policies ausdrücken sollen, sind die Syntax und Semantik von APPEL von der P3P Spezifikation beeinflusst. Das Vokabular bzgl. der einzelnen Elemente, die gesetzt werden können, und ihre möglichen Werte sind dabei mit dem der P3P Spezifikation identisch. Es werden aber noch einige andere Element gebraucht, um die Präferenzen auszudrücken.

Das **<appel:RULESET>** Element

Mit diesem Element wird ein APPEL File eingegrenzt. Es beinhaltet ein oder mehrere Regeln. Für jedes Regel wird ein Verhalten (*behavior*, vgl. S. 47)) angegeben, das dem aufrufenden Programm zurückgeben wird, falls alle Ausdrücke in dieser Regel zu *TRUE* ausgewertet werden. Außerdem können noch folgende Attribute besetzt werden:

crtdby
: Name oder ID des Rulesetautors

crtdon
: Zeit und Datum der Ruleset Kreierung

description
: Eine kurze menschenlesbare Erklärung, die ausgeben werden kann, falls dieses *ruleset* (vgl. S. 48) ausgewählt wird.

Das **<appel:RULE>** Element

Dieses Element beinhaltet die Bedingungen, unter denen ein bestimmtes Verhalten vom aufrufenden Programm ausgeführt werden soll. Es sind folgende Attribute möglich:

behavior
: (Pflichtattribut) Verhalten, das vom aufrufenden Programm ausgeführt werden soll, falls die Ausdrücke mit dem *evidence* übereinstimmen.

crtdby
Name oder ID des Rulesetautors

crtdon
Zeit und Datum der Ruleset Kreierung

description
Eine kurze menschenlesbare Erklärung, die vom User Agent (vgl. S. 48) ausgegeben werden kann, wenn ein *rule* (vgl. S. 48) ausgeführt wird.

prompt
Gibt an, ob eine Hinweisausgabe für den User ausgegeben werde sollte. Wenn dieses Attribut nicht präsent ist, wird auch keine Prompt-Meldung angezeigt.

persona
Falls der User Agent mehrere Userverzeichnisse unterstützt, gibt dieser String an, welches Datenverzeichnis bei dem Zugriff auf eine Resource benutzt werden soll. Falls hier keine Angabe gemacht wird, werden die User Agents Default Werte benutzten.

promptmsg
Eine kurze menschenlesbare Erklärung kann vom User Agent ausgegeben werden, wenn der User für eine Entscheidung hinzugezogen werden soll.

Mit dem <appel:REQUEST> Element innerhalb des <appel:Rule> Elements besteht außerdem die Möglichkeit, für bestimmte URIs ganz bestimmte Regeln anzugeben. Details zum <appel:REQUEST> Element werden in folgenden behandelt.

Falls Matches mit Seiten stattfinden sollen, die keine Policy haben, so sollten die non-or oder non-and Verknüpfungen im <apple:RULE> Element mit dem <POLICY> Element benutzt werden (connectives und ihre Bedeutung bzw. Anwendung werden auf Seite 53 näher erläutert).

Das **<appel:REQUEST>** Element

Wie schon angegeben, kann mit diesem Element eine Regel kreiert werden, das nur für eine bestimmte Resource oder Domain gilt. Das einzige Attribut ist:

uri
(Pflichtattribut) URI der für diese Rule geforderten Resource, hier ist nicht die URI der Policy gemeint.

Eine Regel, die nur <POLICY> Elemente aus dem P3P Vokabular enthält aber kein <appel:REQUEST> wird versuchen, diese Regel bei allen Web Seiten auf Übereinstimmung zu prüfen. Eine Regel, die sowohl <POLICY> Elemente als auch das <appel:REQUEST> Element enthält wird nur bei Policies auf Seiten mit der angegebenen URI im <appel:REQUEST> Element überprüft. Sind andererseits keine <POLICY> Elemente angeben sondern nur das <appel:REQUEST> Element, so wird es immer zu einem Match kommen, sobald die angegebene URI aufgerufen wird, auch wenn diese URI gar keine Policy hat.

Um hier verschiedene URIs anzugeben, können die einzelnen URIs in einem <appel:REQUEST-GROUP> Element zusammengefasst und mit den *connectives* or oder or-exact verbunden werden.

Das <appel:OTHERWISE> Element

Dies ist das sogenannte „degenerate-expression“, das immer mit TRUE ausgewertet wird. Es kann benutzt werden, um alle Fälle, die nicht von den anderen Regeln repräsentiert werden, aufzufangen. <appel:OTHERWISE> ist dabei der einzige Ausdruck in einer Regel. Ein *ruleset* sollte nur ein Regel mit dem *degenerate expression* beinhalten. Dieses sollte die letzte Regel im *ruleset* sein, da die Regeln der Reihe nach abgearbeitet werden und der *rule evaluator* ansonsten frühzeitig die Überprüfung abbricht und die nachfolgenden Regeln nicht mehr auf Übereinstimmung prüft.

Um möglichst alle Fälle aufzugreifen, wird folgende Reihenfolge der Regeln vorgeschlagen:

1. Exceptions (für alle möglichen behaviors)
2. Request Rules
3. Limited Rules
4. Block Rules

Das **<appel:connective>** Attribut

Während *attribute expressions* (vgl. S. 48) immer mit „and“ verbunden werden, d. h. alle aufgeführten Attribute müssen immer zutreffen, können *contained expressions* (vgl. S. 48) mit einem *connective* verknüpft werden, wobei der Match dann aufgrund des jeweiligen *connectives* stattfindet.

Es existieren dabei sechs *connectives*:

or
: Übereinstimmung, falls ein oder mehrere *contained expressions* im *evidence* (vgl. S. 48) gefunden werden. Falls *evidence* Elemente enthält, die nicht in der Regel aufgeführt sind, werden diese ignoriert. Bei diesem *connective* muss mindestens eins der in der Regel aufgeführten Element im *evidence* auftauchen.

and
: Übereinstimmung, falls alle *contained expressions* im *evidence* auftauchen. Falls im *evidence* Elemente auftauchen, die nicht in der Regel aufgelistet sind, so werden diese ignoriert. Falls kein *connective* angegeben ist, wird immer mit and verbunden.

non-or
: Übereinstimmung, falls keins der *contained expressions* im *evidence* gefunden werden kann. Falls im *evidence* Elemente enthalten sind, die nicht in der Regel aufgelistet sind, werden sie ignoriert.

non-and
: Übereinstimmung, falls nicht alle *contained expression* im *evidence* gefunden werden können. Falls im *evidence* Elemente aufgeführt sind, die nicht in der Regel enthalten sind, so werden diese ignoriert.

or-exact

Übereinstimmung, falls ein oder mehrere *contained expressions* im *evidence* gefunden werden. Falls im *evidence* Elemente auftauchen, die nicht in der Regel enthalten sind, schlägt eine Übereinstimmung fehl. Mit diesem *connective* wird sichergestellt, dass nur die in der Regel aufgeführten Elemente im *evidence* auftauchen.

and-exact

Übereinstimmung, falls ein oder mehrere *contained expressions* im *evidence* gefunden werden können. Falls im *evidence* Elemente enthalten sind, die nicht in der Regel auftauchen, so kommt es nicht zu einer Übereinstimmung. Mit diesem *connective* wird sichergestellt, dass die Elemente in der Regel identisch mit denen des *evidence* sind. Es fehlen keine und es sind auch keine weiteren aufgeführt.

4.2.4.1 Beispiel einer APPEL Präferenz

Um die Funktionsweise von APPEL zu illustrieren, wird im folgende ein Beispiel aufgeführt, das aus dem APPEL Working Draft [14] entnommen ist.

Szenario einer User Präferenz:

1. Anfragen bzgl. persönlichen Informationen, die dann an Dritte weitergegeben werden, sollen geblocked werden.
2. Der User hat nichts dagegen , click-stream und User Agent Informationen an Seiten weiterzugeben, soweit sie keine weiteren Informationen sammeln. Trotzdem sollte der Service Angaben jeglicher Art bzgl. der Datensicherheit machen.
3. Der User hat nichts dagegen, seinen Vor- und Nachnamen preiszugeben, solange sie nicht für Marketingzwecke benutzt werden. Der User möchte aber Sicherheitshinweise/-versicherungen sowohl von „PrivacyProtect“ als auch von „Trustus“ haben, bevor diesem Statement „geglaubt“ wird. Der User möchte auf jeden Fall in solchen Fällen informiert werden, bevor auf die Seite zugegriffen wird.
4. Wenn der User auf die Web Seite seiner Bank http://www.my-bank.com zugreift, akzeptiert er jegliche Datenanfragen, solange seine Daten nicht an andere Empfänger weitergeleitet werden.
5. Alle anderen Anfragen zum Datenaustausch sollten gemeldet werden und werden vom User selbst entschieden.

Im nachfolgenden tabellarischen Überblick wird dargestellt, welche Bereiche der User in seiner Privacy Präferenz anspricht und welche Matchingbedingungen und Handlungen dafür erfolgen sollen.

Die mit dem Wildcardsymbol „*“ gekennzeichneten Felder bedeuten dabei, dass hier irgendeine aber keine spezielle Angabe vom User erwartet wird. Der tatsächliche Wert ist unbedeutend, solange überhaupt ein Wert angenommen wird. Bei leeren Feldern wird auch keine Angabe für diesen Bereich gefordert.

Behavior/ Prompt	**Element/Set**	**URI**	**Disputes**	**Purpose**	**Recipient**
block / no	category="physical", or category="demographic", or category="uniqueid"				same, other, delivery, public or unrelated
request / no	dynamic.http.useragent, dynamic.clickstream.server		*		
request / yes	user.name.*		"PrivacyProtect" and "TrustUs"	current, admin, customization or develop	
request / no		www.my-bank.com			ours
limited / yes	[otherwise]				

Tabelle 4.8: Schema einer Userpräferenz

Die dazugehörige APPEL-Formulierung sieht folgendermassen aus:

```
<appel:RULESET xmlns:appel="http://www.w3.org/2001/02/APPELv1"
               xmlns:p3p="http://www.w3.org/2000/12/P3Pv1"
               crtdby="W3C" crtdon="1999-11-03T09:21:32-05:00">

  <appel:RULE behavior="block" description="Service collects
                 personal data for 3rd parties">
    <p3p:POLICY>
      <p3p:STATEMENT>
        <p3p:DATA-GROUP>
          <p3p:DATA>
            <p3p:CATEGORIES appel:connective="or">
              <p3p:physical/>
              <p3p:demographic/>
              <p3p:uniqueid/>
            </p3p:CATEGORIES>
          </p3p:DATA>
        </p3p:DATA-GROUP>
        <p3p:RECIPIENT appel:connective="or">
          <p3p:same/>
          <p3p:other-recipient/>
          <p3p:public/>
          <p3p:delivery/>
          <p3p:unrelated/>
        </p3p:RECIPIENT>
      </p3p:STATEMENT>
    </p3p:POLICY>
  </appel:RULE>

  <appel:RULE behavior="request"
              description="My Bank collects data only for itself
                           and its agents">
```

```
    <appel:REQUEST-GROUP>
      <appel:REQUEST uri="http://www.my-bank.com/*"/>
    </appel:REQUEST-GROUP>
    <p3p:POLICY>
      <p3p:STATEMENT>
        <p3p:RECIPIENT appel:connective="or-exact">
          <p3p:ours/>
        </p3p:RECIPIENT>
      </p3p:STATEMENT>
    </p3p:POLICY>
  </appel:RULE>
  <appel:RULE behavior="request"
              description="Service only collects clickstream data">
    <p3p:POLICY>
      <p3p:STATEMENT>
        <p3p:DATA-GROUP appel:connective="or-exact">
          <p3p:DATA ref="#Dynamic.HTTP.UserAgent"/>
          <p3p:DATA ref="#Dynamic.ClickStream.Server"/>
        </p3p:DATA-GROUP>
      </p3p:STATEMENT>
      <p3p:DISPUTES-GROUP>
        <p3p:DISPUTES service="*"/>
      </p3p:DISPUTES-GROUP>
    </p3p:POLICY>
  </appel:RULE>
  <appel:RULE behavior="request" prompt="yes"
              description="Service only collects your name
                           for non-marketing purposes (assurance
                           from PrivacyProtect and TrustUs)">
    <p3p:POLICY>
      <p3p:STATEMENT>
        <p3p:PURPOSE appel:connective="or-exact">
          <p3p:current/>
          <p3p:admin/>
          <p3p:customization/>
          <p3p:develop/>
        </p3p:PURPOSE>
        <p3p:DATA-GROUP appel:connective="or-exact">
          <p3p:DATA ref="#User.Name.*"/>
        </p3p:DATA-GROUP>
      </p3p:STATEMENT>
      <p3p:DISPUTES-GROUP>
        <p3p:DISPUTES service="http://www.privacyprotect.com"/>
        <p3p:DISPUTES service="http://www.trustus.org"/>
      </p3p:DISPUTES-GROUP>
    </p3p:POLICY>
  </appel:RULE>
<appel:RULE behavior="limited" prompt="yes"
              description="Suspicious Policy. Beware!">
    <appel:OTHERWISE/>
  </appel:RULE>
 </appel:RULESET>
```

Abbildung 4.4 : Beispiel einer Präferenz in APPEL

4.2.5 APPEL und Erweiterungsmöglichkeiten

Bei P3P besteht die Möglichkeit mittels des Extension Elementes eigene selbstdefinierte Informationen zu codieren. Diese werden mit einem Optional-Attribut versehen, um zu kennzeichnen, ob diese Policy auch ohne diese Erweiterung verstanden werden kann oder

nicht. Da das EXTENSION Element Bestandteil des P3P Vokabulars ist, kann es auch vom User benutzt werden. Es muss dann auch mit dem entsprechenden *connective* verbunden werden.

Bei der Behandlung von service-seitigen Extensions bei der Überprüfung auf Übereinstimmung ist folgendes vorgesehen:

Ist ein EXTENSION mit optional="yes" versehen und findet der *rule evaluator* kein entsprechendes Element im *rule* (vgl. S. 48), so wird das EXTENSION entfernt und das *rule* erneut auf Übereinstimmung geprüft. Sind in einer Policy mehrere Erweiterungen, so wird nach einer erfolglosen Überprüfung das nächste EXTENSION, das mit optional="yes" belegt ist, entfernt. Falls EXTENSIONs mit optional="no" belegt sind, müssen sie entweder eine Übereinstimmung in einem *rule* finden, welches dann ausgeführt wird, oder falls aufgrund von „mandatory" EXTENSIONs mit keinem *rule* eine Übereinstimmung gefunden werden kann, kommt das *degenerate expression* <OTHERWISE> zum Tragen. Der User bekommt dann eine Prompt-Message und kann selbst für jede Web-Seite der Resource Entscheidungen treffen.

4.3 Bewertung des EXTENSION Elementes

Mit dem EXTENSION Element, das sowohl Bestandteil des P3P als auch des APPEL Vokabulars ist, besteht die Möglichkeit eigene Elemente einerseits in die P3P Policy und andererseits in eine APPEL Präferenz mit einzubinden. Damit ist das Vokabular praktisch unendlich erweiterbar. Solche Formulierungen sind jedoch nur dann sinnvoll, wenn sie ein „Gegenstück" auf der zu vergleichenden Seite haben, das heisst, nur wenn für einen bestimmten Sachverhalt das gleiche Vokabular und der gleiche Wertebereich benutz wird, kann es auf Übereinstimmung geprüft werden. Werden für einen Sachverhalt verschiedene Vokabeln und Wertebereiche in der Policy und der APPEL Präferenz benutzt, so kann es zu keinem Match kommen. Diese Formulierungen würden bei einem Vergleich, falls sie mit optional="yes" versehen sind, aus der Policy entfernt werden.

Obwohl mit diesem EXTENSION Element dem Nutzer von P3P bzw. APPEL theoretisch scheinbar alle Möglichkeiten zu eigenen Formulierungen gegeben werden, ist die praktische Umsetzung schwierig. Auch innerhalb des EXTENSION Elementes muss es zu einer Abstimmung des Vokabulars und des Wertebereiches für P3P und APPEL kommen, da nur so sinnvolle Formulierungen, die letztendlich zu einem für beide Seiten akzeptablen Ergebnis führen, codiert werden können.

Dies scheint jedoch für das Internet nicht vollführbar zu sein, da die Bedürfnisse der verschiedensten Nutzer dieses Mediums viel zu komplex ist. Es wird schwierig sein, einen gemeinsamen Nenner für alle verschiedenen Bereiche, die für die verschiedensten Internet-Nutzer wichtig sind, zu finden. Das Standardvokabular des W3Cs greift alle wesentlichen Aspekte bzgl. des Datenschutzes auf und sollte für den normalen Internetnutzer ausreichen.

Für das Lufthansa Intranet sollte dieses Element allerdings differenzierter betrachtet werden. Die Lufthansa AG kann dieses Element sehr wohl für ihre Zwecke nutzen, da der Kreis der Intranetnutzer begrenzt und überschaubar ist. Grundsätzlich müsste die Lufthansa AG ein eigenes Vokabular mit Wertebereichen zusamm enstellen und sie den Mitarbeitern zugänglich

machen, so dass diese ihre Präferenzen auf Grundlage dieses zusätzlichen Vokabulars formulieren können. Da nun auf beiden Seiten das gleiche Vokabular und der gleiche Wertebereich gültig sind, können Formulierungen über das EXTENSION Element miteinander verglichen werden und zu einem vordefinierten Verhalten führen.

Kapitel 5

Anwendungstools für P3P & APPEL

P3P ermöglicht es Web-Seiten ihre Datenschutzmassnahmen in eine standardisierte, maschinen-lesbare Form zu bringen, die durch den Browser des Benutzers automatisch gefunden und leicht ausgewertet werden kann. Diese maschinen-lesbare Form kann entweder manuell oder über automatische Tools erreicht werden (Abb. 5.1) [10].

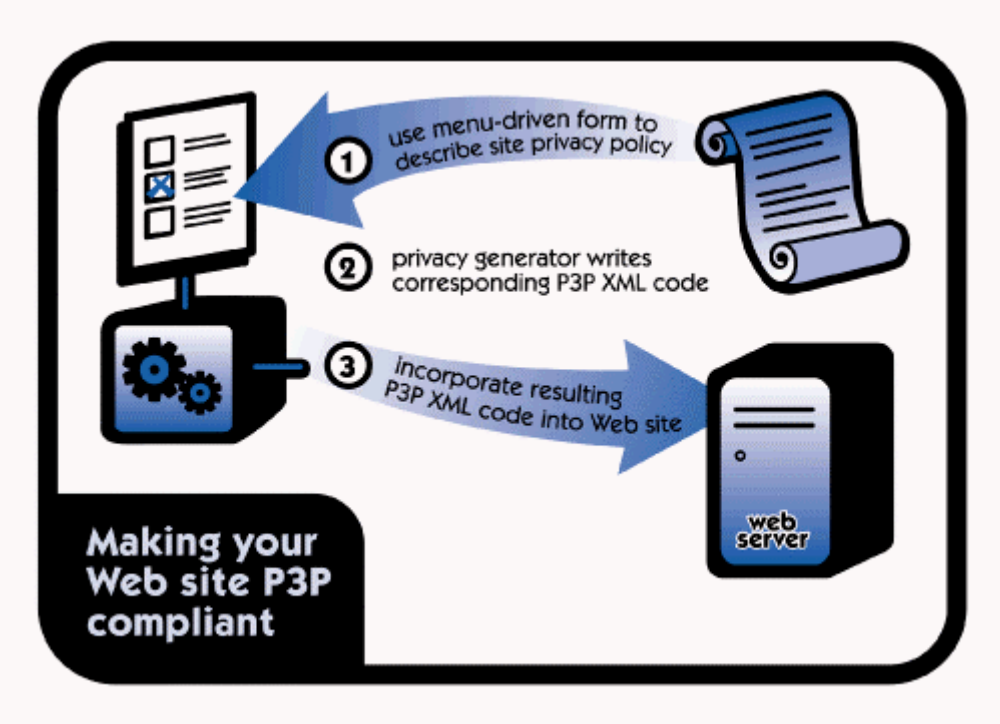

Abbildung 5.1: Schema einer Toolunterstützten Policygenerierung

In diesem Kapitel sollen drei Bereiche im Bezug auf P3P und APPEL untersucht werden. Zunächst werden Tools vorgestellt und bewertet, mit denen eine P3P Policy generiert werden kann. Im zweiten Abschnitt dieses Kapitels wird dann das zur Zeit einzige Hilfsmittel bzgl. APPEL, mit dem eine Präferenz erstellt werden kann, beschrieben. Als letztes werden verschiedene User Agents und ihre Handhabung vorgestellt. In allen drei Bereichen ist dabei die Bedeutung des EXTENSION Elementes und seine Handhabung durch diese Tools wichtig.

5.1 Tools bzgl. P3P

Auf der Homepage des W3Cs werden Links zu den zur Zeit auf dem Markt befindlichen Tools aufgeführt, die bei der Formulierung einer P3P Policy benutzt werden können [15]. In Tabelle 5.1 sind sie zusammengefasst.

Tool	**Link**	**Beschreibung**
PrivacyBot.com	www.privacyBot.com	PrivacyBot.com ist ein Privacy "Bestätigungsprogramm", dass Web Seiten helfen soll, "gute" Privacy Policies zu implementieren. Es generiert kundennahe XML-Policies, die auf den P3P Spezifikationen basieren. Durch eine Online-Registrierung ist man berechtigt, deren Trustmark als Referenz zu veröffentlichen.
P3Pedit	www.p3pedit.com	P3P Edit ist ein Web-basierter P3P Policy Generator. Die Benutzer können entweder zwei einfache Formulare ausfüllen oder einen sog. Policy Wizard benutzen. P3PEdit generiert dann W3C-konforme P3P Policies.
IBM P3P Policy Editor	www.alphaworks.ibm.com/tech/p3peditor	Der P3P Policy Editor von IBM bietet eine leichthandhabbare Benutzeroberfläche, um Privacy Policies in der P3P-Sprache des W3Cs für Web Seiten zu erstellen und zu aktualisieren.

Tabelle 5.1: Übersicht der Tools bzgl. P3P

Der Generator von PrivacyBot.com und der P3Pedit wurden nicht benutzt, da die Erhebung einer Gebühr, ohne dass man die Möglichkeit hatte, diese Generatoren zuvor anzuschauen bzw. zu testen, wenig vertrauenswürdig erschien. Der IBM P3P Policy Editor war im Gegensatz zu den anderen kostenfrei und wird im folgenden näher beschrieben.

5.1.1 IBM P3P Policy Editor

Der P3P Editor von IBM ist ein Generator der menü-gesteuert ist. Zunächst erscheint eine Anfangsmaske (Abb. 5.2). Nachdem man alle geforderten Eingaben getätigt hat, wird neben dem XML-Code der Policy auch eine HTML-Version erstellt. Dies ist die menschenlesbare Policy. Bei der Benutzung des Generators hat sich ausserdem noch herausgestellt, dass EXTENSIONs selbst formuliert und nachträglich in den XML-Code des IBM P3P Policy Editors miteingebunden werden müssen.

Zunächst wird im folgenden die Funktionsweise des Editors näher beschrieben. Die Auswertung des Editors und ein Vergleich der menschenlesbaren Policy vom IBM Editor mit dem Draft Statement des OECD´s findet in Abschnitt 5.1.4.2 statt.

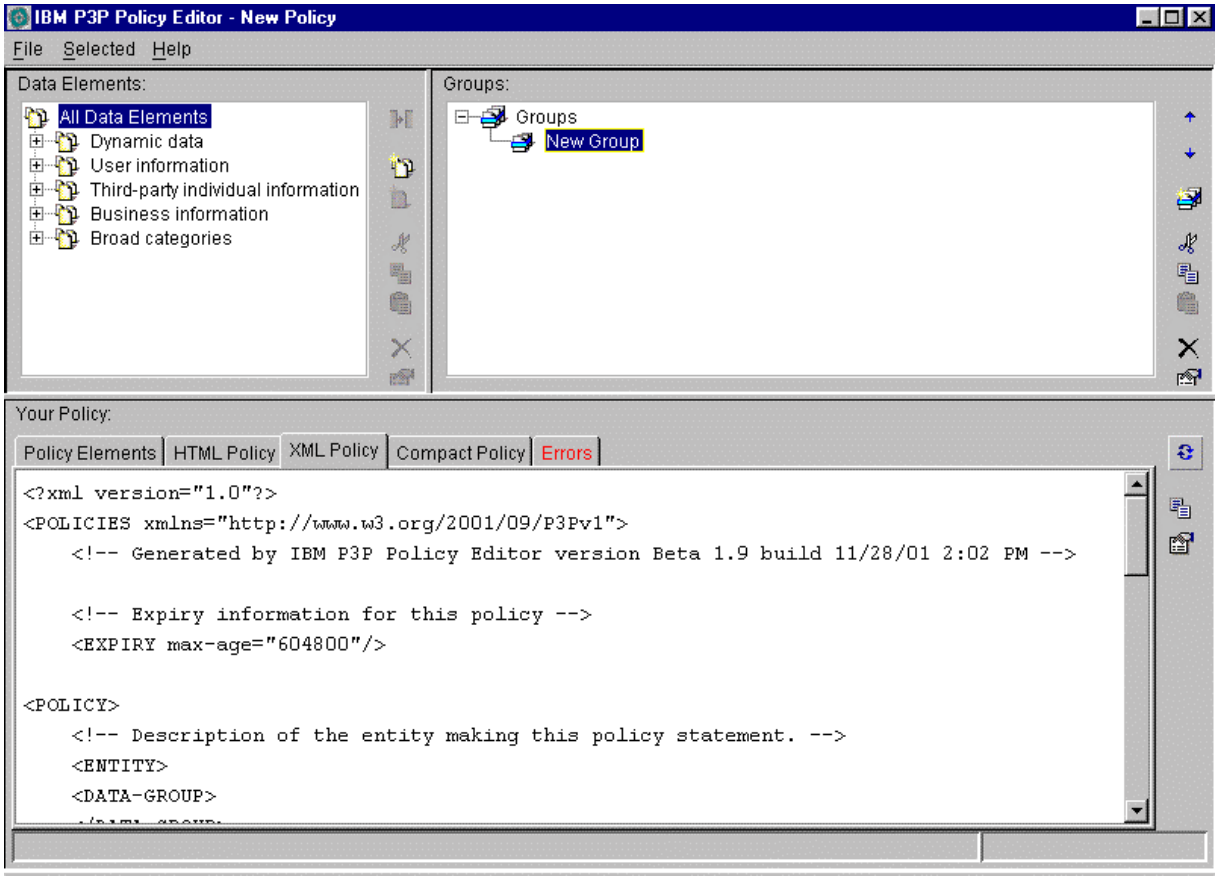

Abbildung 5.2: Benutzeroberfläche IBM Policy Generator

5.1.1.1 Funktionsweise

Der Generator teilt die Eingabe in zwei Bereiche auf:

1) Policy Properties und
2) Data Properties.

Bei dem ersten Bereich (Abb. 5.3) handelt es sich um allgemeine Angaben zum Service. Diese allgemeinen Angaben beziehen sich auf:

- Geschäftseinheit (Name , e-mail, Web homepage, Telefonnummer, Postanschrift)
- Web Seite (Policy Name, Opt-in/-out URL, URL der menschenlesbaren Privacy Policy)
- Access: Wird der Zugriff auf Daten gewährt? Wenn ja, welcher Art sind diese (identifizierbare usw.). Ausserdem wird hier auch ein Hinweis darauf gegeben, dass die menschenlesbare Form Anweisungen enthalten sollte, wie ein User Informationen über seine gespeicherten Daten erhalten kann und wie er sie aktualisieren kann.
- Assurances: Wer „überwacht“ die Policy? Über ADD können verschiedene Institutionen, Gesetze usw. eingeben werden. Dabei werden für jede Eingabe Detailinformationen verlangt:

- General: Name, URL Type (Kundendienst, unabhängige Organisation, Gesetz, Gericht), Beschreibung des Überwachungseinheit
- Remedies: Wie werden Privacyverstösse gehandhabt?:
  - einfach korrigiert
  - Korrektur auf Gesetzesgrundlage
  - Geldentschädigung

Dabei sollten mehr Details in der menschenlesbaren Policy aufgeführt sein

- Expiry:
  Wie lange ist diese Policy gültig? Dabei ist entweder eine Dauer oder ein konkreter Zeitpunkt möglich.

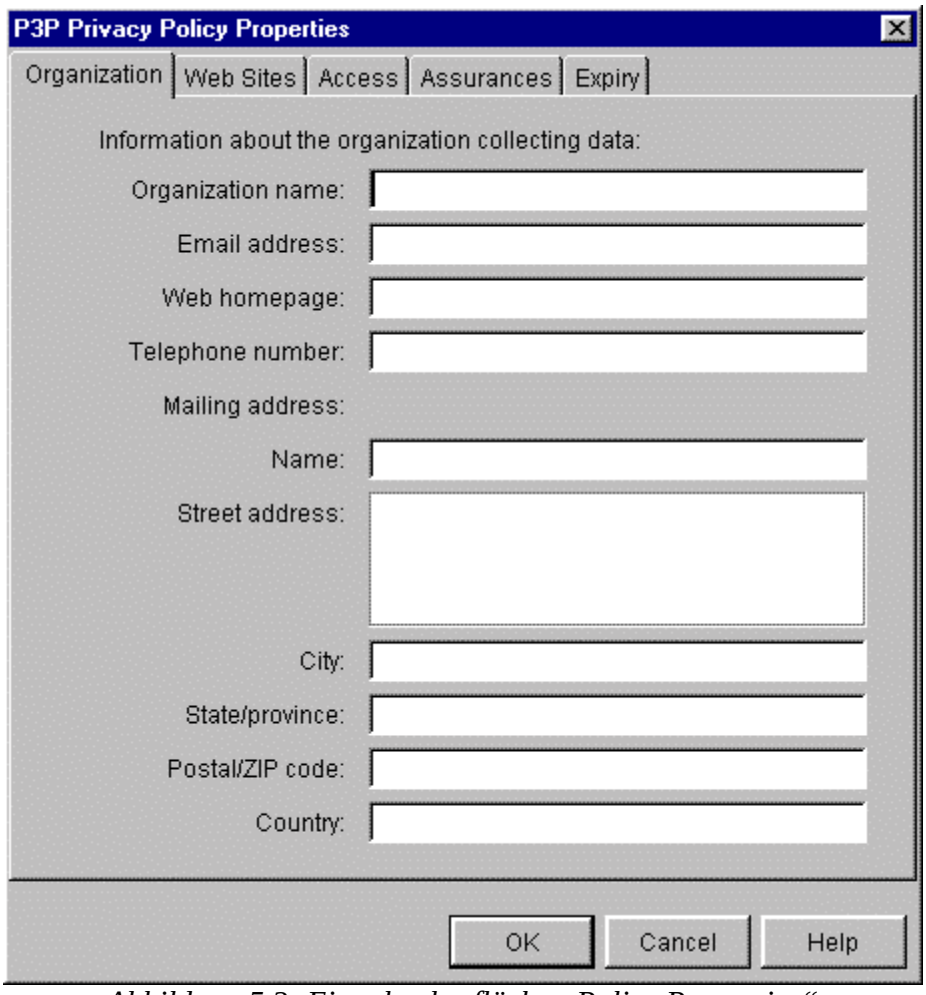

Abbildung 5.3: Eingabeoberfläche „Policy Properties“

Der zweite Bereich (Abb. 5.4) befasst sich mit den Daten selbst, die ggf. erhoben werden. Zunächst muss man Daten, die erhoben werden deklarieren. Hierzu sind die gesamten Daten in ein Schema aufgeteilt:

- All Data Elements
    - Dynamic Data
    - User Information
    - Third Party- individual Information
    - Business Information
    - Broad Categories

Diese einzelnen Bereiche werden noch weiter untergliedert. Durch einen *drag and paste* Mechanismus kann man nun die Daten, die erhoben werden, auswählen. Daten mit gleichen Praktiken können zusammengefasst werden. Für diese Datengruppen spezifiziert man dann die sogenannten Data Properties:

- General: Bezeichnung und eine Erklärung, weshalb diese Daten benötigt werden und was passiert, wenn man die geforderten Daten nicht preisgibt.
  Außerdem besteht die Möglichkeit, einen Hinweis darauf zu geben, ob mit diesen Daten die Identität des Besuchers feststellbar ist.

- Purpose: Hier können die vordefinierten Zwecke angeben werden. Dabei wird im ersten Schritt eine grobe Einteilung vorgenommen, die im zweiten Schritt näher spezifiziert werden muss:

1. Schritt	**2. Schritt**
Current request, site administration, R&D	- completion and support of the current activity - Web site and system administration - R&D
Site customisation	One-time tailoring
Anonymous user tracking	- Pseudonymous analysis of user behaviour - Pseudonymous decision-making
Individual user tracking	- individual user analysis - individualizes decision-making
Contacting the user	- contacting visitors for marketing - contacting visitors for marketing by telephone
Other purpose	- historical prevention - other purpose with description

Tabelle 5.2: Detaillierte Eingabe des Zweckes

  Bei der detaillierteren Angabe muss ausserdem noch angegeben werden, ob die Daten notwendig sind oder es die Möglichkeit von opt-in/-out gibt.

- Recipient:
  Empfängerspezifikation durch die vordefinierten Empfängergruppen. Auch hier soll eine Angabe gemacht werden, ob diese Empfänger notwendig sind (z. B. Lieferanten bei Warenbestellungen) oder ob der User die Möglichkeit von opt-in/-out hat.

- Retention:
  Aufgrund welcher Tatsachen werden Daten wie lange gespeichert:
  - nur während der Transaktion zum angegebenen Zweck
  - aufgrund von Gesetzesbestimmungen
  - aufgrund von angegebenen Geschäftspraktiken
  - unendlich

Dabei sollten mehr Details in der menschenlesbaren Policy angegeben werden.

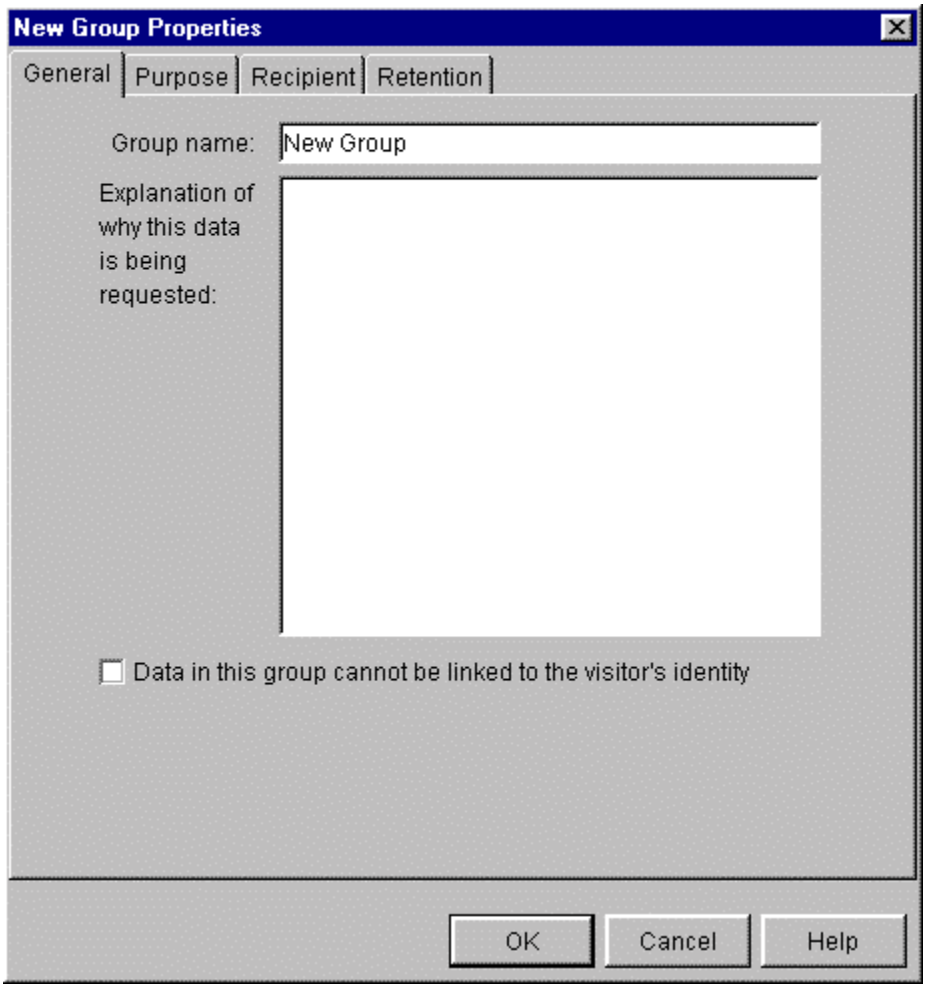

Abbildung 5.4: Eingabeoberfläche „Data Properties“

5.1.2 Benutzung des Editors mit “my Travel ex”

Mit den OECD Privacy Principles wurde schon ein gewisser Standard im Bezug auf Datenschutz aufgezeigt. Allerdings hatte sich bei der Benutzung des OECD-Generators gezeigt, dass es für einige Aspekte nicht notwendig ist, sie auf Projektebene zu formulieren, da sie einheitlich für Lufthansa konzernweit gelten und daher schon beim Eintritt ins Intranet formuliert sein sollten.

Um beurteilen zu können, ob ein P3P-Generator von IBM alle für Lufthansa erforderlichen Elemente bzgl. des Intranets berücksichtigt, soll im nächsten Abschnitt geprüft werden, ob die für das Lufthansa Intranet relevanten Bereiche, die sich aus der Auswertung des Drafts vom OECD-Generator ergeben haben, in der P3P Spezifikation wiederzufinden sind.

5.1.2.1 Gegenüberstellung LH Angaben und P3P Spezifikationsmöglichkeiten

Bei der Gegenüberstellung der LH Anforderungen und den P3P Spezifikationsmöglichkeiten in Tabelle 5.3 hat sich herausgestellt, dass für folgende Bereiche eine erweiterte Angabe notwendig ist, da sie nicht in der P3P Spezifikation enthalten ist:

1) Schnittstellen zu anderen Systemen und
2) wie Daten übertragen werden (besonders gesicherte Kanäle, Verschlüsselung der Daten usw.)

Diese zwei Bereiche können jedoch über das EXTENSION Element formuliert werden. Im Rahmen dieser Arbeit wurden diese Erweiterungen formuliert. Sie werden in Abschnitt 5.1.4.3 aufgeführt und näher erläutert.

Lufthansa	**P3P Spezifikationsmöglichkeiten beim IBM Generator**
Informationen über das Projekt/Abteilung und ihre Web-Seite(Abteilung, Co-mail, Name der zuständigen Person)	Über die Policy Properties „Organisation“ und „Web Sites“
Verbindung zu anderen Web-Seiten (Werden Daten von anderen mitgenutzt?)	Aussagen hierüber sind über das RECIPIENT Element möglich, die „Empfänger“ sind dann allerdings die verschiedenen möglichen Schnittstellen zu anderen Systemen
Automatische Sammlung von Daten	Durch die Einteilung der Daten in verschiedene Gruppen (z. B. clickstream usw.) ist eine Aussage darüber möglich.
Datenerhebung und ihre Begründung	Mit dem *Base Data Schema* können die Daten, die erhoben werden dargestellt werden Mit dem PURPOSE Element ist der Zweck darstellbar.
Veröffentlichung und Mitbestimmungsmöglichkeiten des Nutzers	Über das ACCESS Element ist darstellbar, ob und in wieweit Daten frei verfügbar gemacht werden. Durch die Benutzung des opturi Elementes kann dem Nutzer eine Art Mitbestimmungsmöglichkeit gegeben werden.
Selbstbeteiligung des Einzelnen/Zugriff	Mit CONSEQUENCE kann dem Nutzer mitgeteilt werden, wieso man die Daten braucht und was passiert, wenn der User nicht einwilligt (z. B. die Tranksaktion kann ansonsten nicht durchgeführt werden)

Tabelle 5.3: Gegenüberstellung von LH und P3P

Aufgrund der im Rahmen dieser Diplomarbeit getätigten Eingaben wurde folgender XLM-Code erstellt:

```
<?xml version="1.0"?>
<POLICIES xmlns="http://www.w3.org/2001/09/P3Pv1">
    <!-- Generated by IBM P3P Policy Editor version Beta 1.9 build 11/28/01
     2:02 PM -->

    <!-- Expiry information for this policy -->
    <EXPIRY max-age="604800"/>

<POLICY
    discuri="http://?????"
    opturi="?????"
    name="Travelex">
    <!-- Description of the entity making this policy statement. -->
    <ENTITY>
    <DATA-GROUP>
<DATA ref="#business.name">Deutsche Lufthansa AG</DATA>
<DATA ref="#business.contact-
info.online.uri">http://lww.travelex.dlh.de/</DATA>
<DATA ref="#business.contact-info.postal.organization">Deutsche Lufthansa
      AG</DATA>
<DATA ref="#business.contact-info.postal.street">Lufthansa Basis</DATA>
<DATA ref="#business.contact-info.postal.city">Frankfurt</DATA>
<DATA ref="#business.contact-info.postal.postalcode">60546</DATA>
<DATA ref="#business.contact-info.postal.country">Germany</DATA>
    </DATA-GROUP>
    </ENTITY>

    <!-- Disclosure -->
    <ACCESS><none/></ACCESS>


    <!-- Disputes -->
    <DISPUTES-GROUP>
        <DISPUTES resolution-type="service"
service="http://lww.finanzen.lh.cgn.dlh.de/servlet/PB/menu/1000222_pcontent
/content.html" short-description="Datenschutzbeauftragter Konzern">
            <LONG-DESCRIPTION>Datenschutzbeauftragter des Konzerns</LONG-
DESCRIPTION>
    <!-- No remedies specified -->
        </DISPUTES>
        <DISPUTES resolution-type="independent" service="http://www.lfd-
nrw.de" short-description="Landesbeauftragter für Datenschutz in NRW">
            <LONG-DESCRIPTION>Landesbeauftragter für Datenschutz</LONG-
DESCRIPTION>
    <!-- No remedies specified -->
        </DISPUTES>
    </DISPUTES-GROUP>

    <!-- Statement for group "Benachrichtigung" -->
    <STATEMENT>

        <EXTENSION optional="yes">
            <GROUP-INFO
xmlns="http://www.software.ibm.com/P3P/editor/extension-1.0.html"
name="Benachrichtigung"/>
        </EXTENSION>

    <!-- Consequence -->
    <CONSEQUENCE>
```

```
Die Telefonnummern werden für Rücksprachen benötigt.</CONSEQUENCE>

    <!-- Use (purpose) -->
    <PURPOSE><contact/><current/><telemarketing/></PURPOSE>

    <!-- Recipients -->
    <RECIPIENT><ours/></RECIPIENT>

    <!-- Retention -->
    <RETENTION><indefinitely/></RETENTION>

    <!-- Base dataschema elements. -->
    <DATA-GROUP>
    <DATA ref="#user.home-info"/>
    <DATA ref="#user.business-info"/>
    </DATA-GROUP>
</STATEMENT>

<!-- End of policy -->
</POLICY>
</POLICIES>
```

Die einzelnen Bereiche werden durch einleitende Informationen in „<...>“ kommentiert, so dass auch Laien sich einen Überblick über die diversen Informationen verschaffen können.

Die Daten (user.home-info, user.business-info), die erhoben werden, sind während der Eingabe zu der Gruppe „Benachrichtigung“ zusammengefasst worden. Dieser neue Namensraum wird mit Hilfe des EXTENSION Elementes spezifiziert. Da aber die Policy auch ohne dieses EXTENSIONs verstanden werden kann, ist das Attribut „optional“ mit „yes“ belegt. Die Angabe des Namensraumes und ihre Kreierung durch den IBM Editor ist für das Verständnis der Policy nicht von Bedeutung.

5.1.2.2 Auswertung des IBM P3P Policy Editors

Die Benutzung des IBM Editors für das Lufthansa Projekt „my Travel ex“ im Rahmen dieser Diplomarbeit hat gezeigt, dass die Handhabung des IBM Editors sehr gut ist. Der Nutzer braucht sich nicht mit dem Vokabular und der Syntax der P3P Spezifikation auseinander setzten. Er wird zu allen wichtigen Eingaben geführt.

Von Vorteil ist auch, dass mit der Erstellung des XML-Codes auch eine HTML-Version der Policy angefertigt wird. Diese HTML-Version der Policy, die für „my Travel ex“ im Rahmen dieser Diplomarbeit erstellt wurde, ist in Anhang E aufgeführt.

Im Vergleich zum OECD Draft Statement (vgl. Anhang B) ist diese Version wesentlich übersichtlicher und kürzer. Die tabellarische Auflistung aller möglichen Datenmengen im OECD Draft Statement ist eher verwirrend als informierend. Die Leser eines solchen Drafts würden eher abgeschreckt werden, als dass sie Vertrauen aufgrund der Policy aufbauen. Der Umfang der Policy des OECD im Vergleich zur Policy des IBM Editors ist zu gross. Bei dem IBM Generator sind die Formulierungen kürzer und daher leichter und schneller für den Leser verständlich.

Mit dem IBM P3P Policy Editor kann das Grundgerüst einer P3P Policy als XML-Code erstellt werden. EXTENSIONs müssten allerdings selbst formuliert und nachträglich in den vom IBM Editor erstellten XML-Code miteingebunden werden. Dies erfordert zumindest, dass sich der Nutzer dieses Tools in die Syntax und Semantik des EXTENSION Elementes einarbeitet.

Bei dem Gebrauch des IBM Editors für das Lufthansa Intranet um eine HTML-Version der Policy zu erhalten, müssten keine umfangreiche Anpassung der Software erfolgen wie beim OECD Generator. Es müssten lediglich die zusätzlich über das EXTENSION Element mit eingebrachten Informationen im XML-Code in die vom IBM Editor erstellte HTML-Policy eingefügt werden. Dies erscheint gegenüber der Neuprogrammierung eines Generators zur Erstellung einer menschenlesbaren Policy gemäss den Änderungsvorschlägen aus Abschnitt 3.5.2 sinnvoller. Im Ganzen erscheint die Benutzung des IBM P3P Policy Editors für das Lufthansa Intranet am sinnvollsten.

5.1.2.3 Serviceseitige EXTENSION Formulierung

Für die in Abschnitt 5.1.4.1 genannten Bereiche sind im Rahmen dieser Diplomarbeit EXTENTIONs formuliert worden. Sie werden im folgenden aufgeführt und erläutert.

Es sollen folgende Aussagen gemacht werden:

1. SSL wird benutzt und die Daten werden verschlüsselt übertragen.

```
<POLICY>
 discuri="http://...."
 opturi=" ...."
 name= .....
…
 <EXTENSION optional = "yes">
        <TRANSMISSION xmlns="http://lww.travelex.dlh.de/P3P/transmission">
         <ssl/>
         <encoded/>
        </TRANSMISSiON>
 </EXTENSION>
...
</POLICY>
```

Mit dem Attribut „optional" wird angegeben, ob die Policy auch ohne dieses EXTENSION verstanden werden kann oder nicht. Für User, denen die Art und Weise, wie Daten übertragen werden, egal ist und sie deshalb nichts zu diesem Aspekt in ihrer Präferenz formuliert haben, würde die Belegung dieses Attributs mit „no" zu keinem Match führen. Der User könnte diese Seite nur mit seiner manuellen Zustimmung bei der Fehlermeldung besuchen, obwohl für ihn diese Aussage in der Policy irrelevant ist. Er würde bei seinem Web Seiten Besuch unnötig gestört werden. Daher ist es sinnvoller dies Attribut mit „yes" zu belegen. Die Policy ist auch ohne diese zusätzliche Information verständlich. User, die jedoch Wert auf diese Information legen, finden sie vor und das von ihnen vorgegebene Verhalten wird ausgeführt.

Unter <TRANSMISSION xmlns=... wird der Namensraum für TRANSMISSION definiert. Danach kommen die Werte die TRANSMISSION hier einnimmt.

2. VIVA und AIDA sind Systeme innerhalb des Intranets, an die Daten übermittelt werden bzw. diese Systeme können Empfänger von Daten sein.

```
<POLICY>
…
 <RECIPIENT>
…
 <EXTENTION optional="yes">
  <INTERFACES xmlns=http://lww.travelex.dlh.de/P3P/interfaces">
   <aida/>
   <viva/>
  </INTERFACES>
 </EXTENSION>
</RECIPIENT>
….
</POLICY>
```

Auch bei diesem EXTENSION ist das optional Attribut mit „yes" belegt worden, damit User, die diesbezüglich keine Präferenzen geäussert haben, bei dem Besuch dieser Web Seite nicht unnötig gestört werden. Mit xmlns wird wieder der neue Namensraum INTERFACES eingeführt.

Diese zwei im Rahmen dieser Diplomarbeit formulierten EXTENSIONs können in den vom IBM Generator erstellten XML-Code eingefügt werden.

5.2 Tools bzgl. APPEL

In diesem Abschnitt wird das einzige zur Zeit auf dem Markt befindliche Hilfsmittel zur Erstellung einer APPEL Präferenz vorgestellt. Dass es zur Zeit nur dieses Tool gibt, liegt sicher daran, dass sich diese Spezifikation noch in einem Entwurfsstatus befindet. Es bleibt in Zukunft abzuwarten, wie der Markt auf eine Fertigstellung dieser Spezifikation reagiert.

5.2.1 JRC P3P APPEL Privacy Preference Editor

Mit dem JRC Editor können APPEL *Rulesets* erstellt werden. Zur Zeit scheint es der einzige Generator für den User zu sein. Dies mag daran liegen, dass sich die APPEL Spezifikation noch im Draft Status befindet und somit noch nicht entgültig ausgereift zu sein scheint.

5.2.1.1 Funktionsweise

Der JRC Editor arbeitet ähnlich wie der P3P Policy Editor von IBM. Abbildung 5.5 zeigt zunächst die Anfangsmaske des Editors.

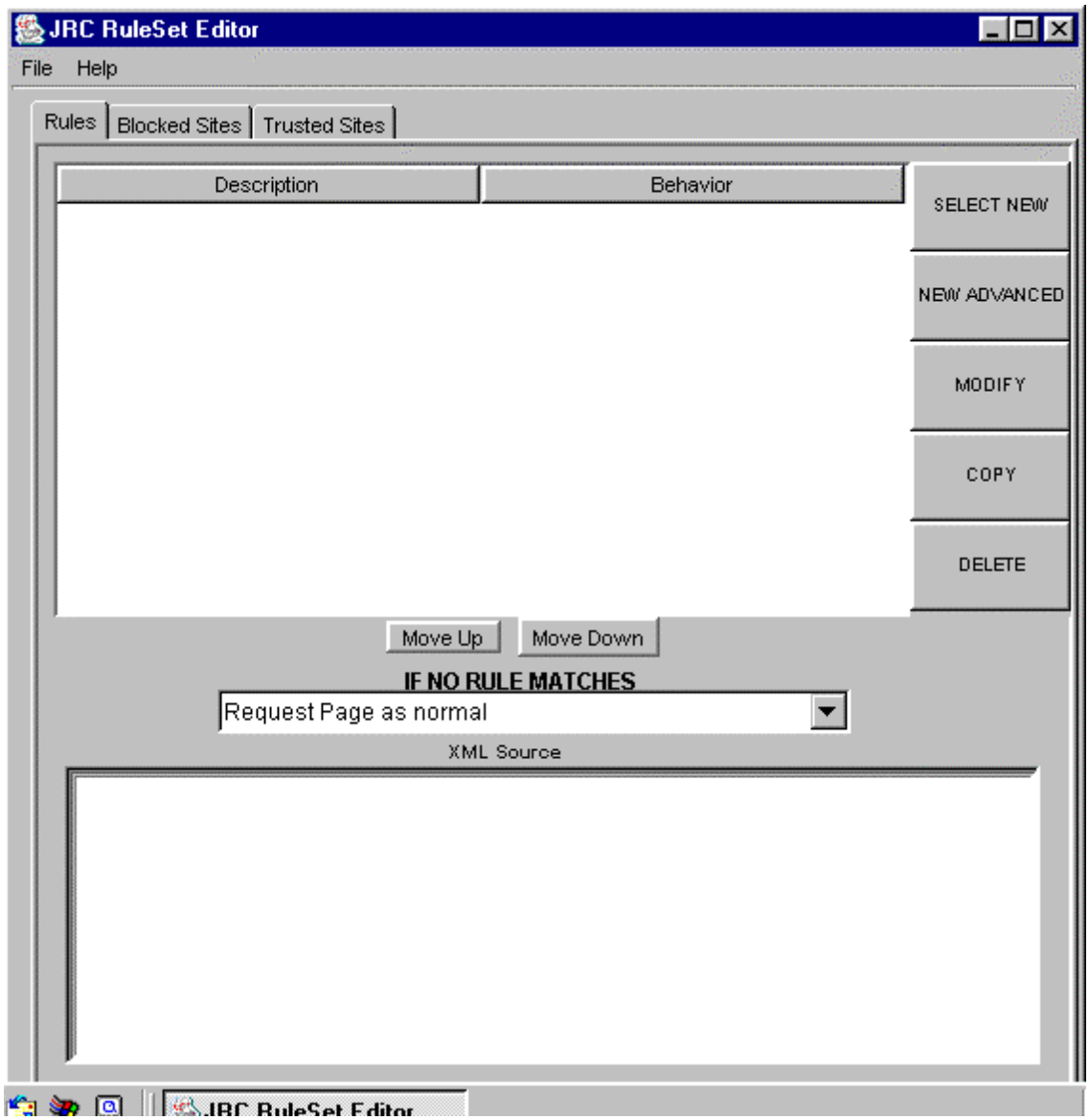

Abbildung 5.5: Benutzeroberfläche des JRC APPEL Privacy Preference Editors

Über diese erste Benutzeroberfläche können Angaben folgender Bereiche angezeigt bzw. eingegeben werden:

- Rules: bereits erstellte *rulesets*
- Blocked Sites: Web-Seiten, die gesperrt sind und
- Trusted Sies: Web-Seiten, die ohne Bedenken besucht werden können.

Ausserdem kann angegeben werden, was geschehen soll, falls kein Match stattfindet. Dies entspricht dem APPEL OTHERWISE Element. Dabei sind folgende Angaben möglich:

- Request page as normal,
- Block Page und
- Request but do not reveal information about my PC.

Um ein *rule* zu bearbeiten, kann man zwischen den Punkten

- Select New,
- New Advanced,
- Modify,
- Copy und
- Delete wählen.

Select New beinhaltet dabei vorgefertigte Rules, aus denen ausgewählt werden kann. Diese sind:

- Any marketing must be opt-in with prompt/Data Type/Any
- No compulsory marketing
- Blocked because site will use your information for marketing purpose
- Blocked because you cannot access all your data after submitting it
- Site will retain information collected by this resource beyond what is necessary
- Require identity and physical address of controller
- Passed all rules and find check on disclosure to countries outside EU
- Default rule fired

Über *New Advanced* hat man die Möglichkeit, wenn man sich mit APPEL auskennt, selbst *rules* zu erstellen. Dabei werden folgende Punkte aufgegriffen:

1) APPEL Rule: Was beinhaltet dieses *rule*?
2) What kind of data you want to apply this rule to: Um welche Daten geht es hier?
3) Other criteria: Andere Angabenmöglichkeiten. Dies sind:

    a. How long: Wie lange werden die Daten gehalten, auf welcher Grundlage?
    b. Who to: Werden die Daten an andere weitergeleitet?
    c. What for: Zweck der Datenerhebung
    d. Access to third data alter submittig: Hat man selbst Zugriff auf seine Daten nach der Übertragung ?

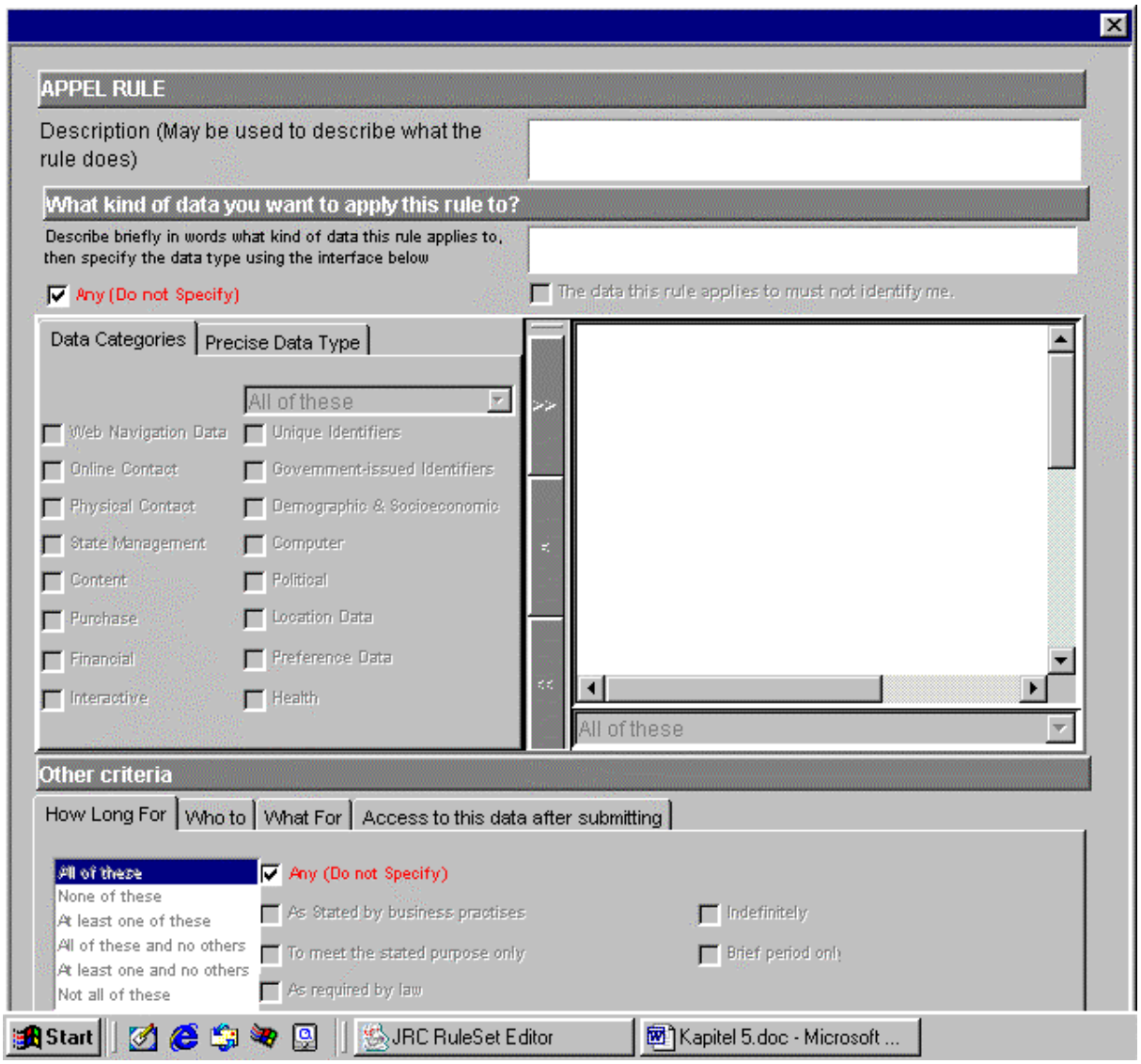

Abbildung 5.6 : Benutzeroberfläche bei New Advanced

Über die anfängliche Menüleiste ist es außerdem noch möglich Privacy Preference Settings, z.B. vorgefertigte Präferenzen unabhängiger Organisationen zu importieren.
Auch können so selbsterstellte EXTENSIONs mit eingebunden werden.

5.2.2 Userseitige Formulierung eines EXTENSIONS

Für die Bereiche „Sicherheit“ und „Schnittstellen zu anderen Systemen“ aus Kapitel 3, Abschnitt 3.5.2 ist in Rahmen dieser Diplomarbeit in Abschnitt 4.1.3.1 eine serviceseitige Formulierung mittels des EXTENSION Elementes vorgenommen worden. Diese kann allerdings nur durch eine entsprechende Formulierung in APPEL durch den User verstanden werden.

Im Rahmen dieser Diplomarbeit ist daher eine userseitige Präferenz formuliert worden. Der User fordert für diese Bereiche Informationen. Dabei kommt es allerdings nicht auf einen konkreten Wert an. Dies wird wie folgt formuliert:

```
…
<appell:RULE behavior=”…>
 <p3p:POLICY>
  …
   <p3p:EXTENSION appel:connective=”or”>
    <p3p:interface=”*”/>
    <p3p:transmission=”*”/>
   </p3p:EXTENSION>
  ….
 </p3p:POLICY>
</appel:RULE>
```

Der User fordert in seiner Präferenz eine Angabe zu den Bereichen interface und transmission. Mit dem Wildcardsymbol “*” wird allerdings kein spezieller Wert für diese zwei Bereiche gefordert. Dem User reicht es, wenn überhaupt eine Angabe dazu gemacht wird.

Diese Formulierung kann in den vom JRC P3P APPEL Privacy Preference Editor erstellten XML-Code eingefügt werden.

5.3 User Agents

In Abschnitt 4.1.1 wurde dargestellt wie eine Transaktion mit P3P funktioniert. Dafür sind sogenannte User Agent nötig. In diesem Kontext sind dies die Prozesse, die den Vergleich zwischen der Privacy Policy und User Präferenz für den Users selbst anstellen und dann gemäss des vorgegebenen Verhaltens agieren.

Das W3C gibt drei User Agents/Proxies an, die benutzt werden können [15]:

1) At&T Privacy Bird
2) Internet Explorer 6
3) JRC P3P Proxy.

5.3.1 AT&T Privacy Bird

Der AT&T Privacy Bird bietet neben der Importierung von APPEL Ruleset Settings im XML-Format auch die Möglichkeit an, Privacy Präferenzen durch vordefinierte „Sicherheitsniveaux“ auszudrücken. Dabei wird in folgende Bereiche unterteilt:

a) Health or Medical Information
b) Financial or Purchase Information
c) Personally Identifiable Information
d) Non-personally Identifiable Information(Demographic, interests, web sites etc.)

Man kann zwischen den Niveaux „Low“, „Medium“ und „High“ wählen, so dass eine automatische Auswahl der Präferenzen dem Niveau entsprechend stattfindet, oder man kann

über das Anklicken von „Customs“ die Präferenzen in den einzelnen Bereichen selbst auswählen.

Bei der Durchsicht der Help-Topics hat sich jedoch gezeigt, dass bei einer Einbindung anderer Settings das EXTENSION-Element nicht verwendet werden darf.

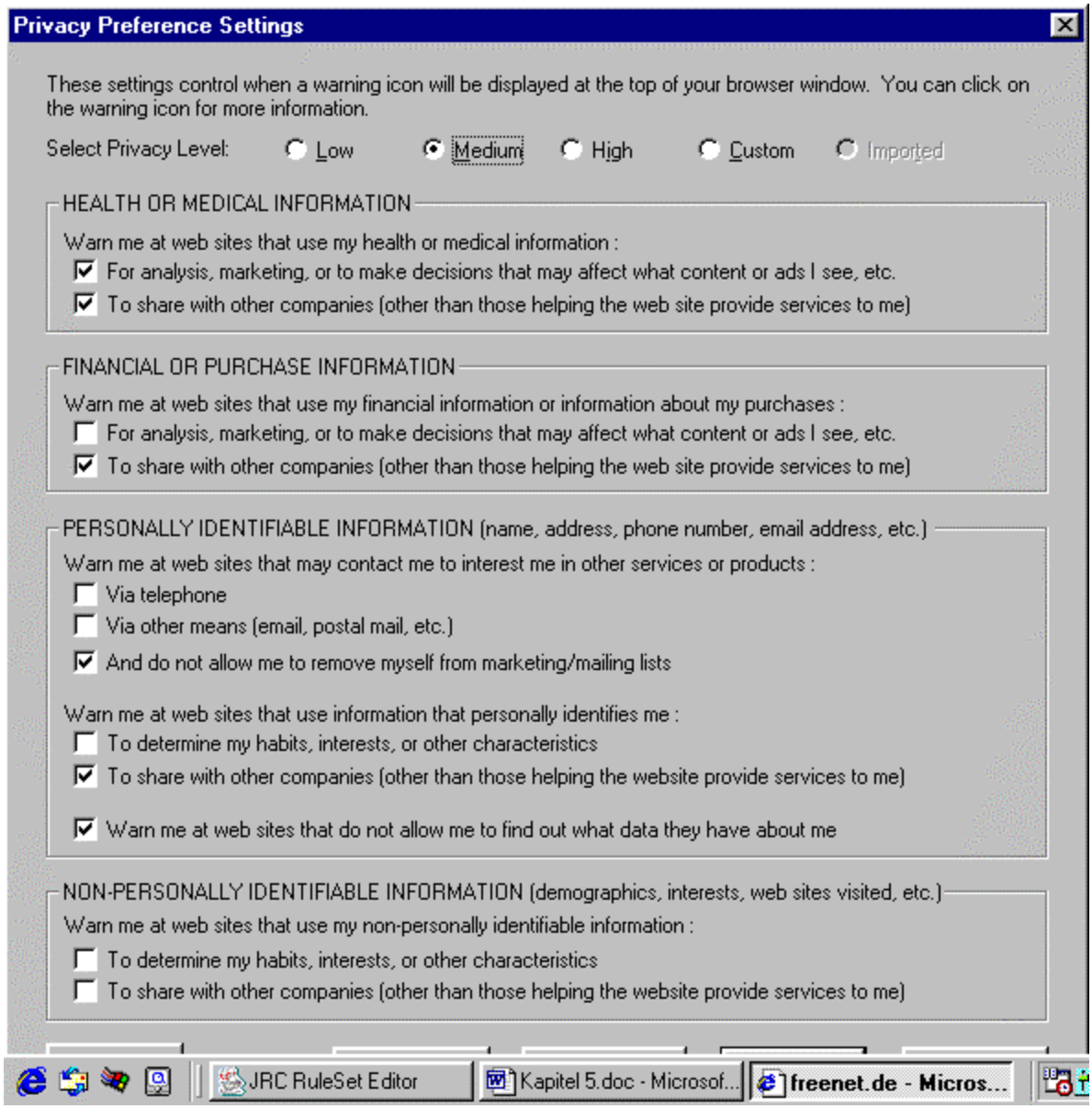

Abbildung 5.7: AT&T Privacy Bird

5.3.2 Internet Explorer 6

Der Internet Explorer 6 unterstützt Privacy Präferenzen, indem er dem User mehr Kontrolle über Cookies ermöglicht [16].

Die Privacyeinstellungen (Abb. 5.8) können über die Menüleiste mit *Extras* erreicht werden. Unter *Internetoptionen* findet man dann die Rubriken:

- General
- Security
- Privacy
- Content
- Connection
- Programms und
- Advanced.

Unter *Privacy* kann über voreingestellte Privacy-Levels ein Präferenzniveau ausgesucht werden. Dabei ist es auch möglich Rule Settings zu importieren. Ob das EXTENSION Element erlaubt ist, wurde allerdings nicht näher spezifiziert. Auf eine Anfrage diesbezüglich gab es bislang keine Antwort (vgl. Anhang F).

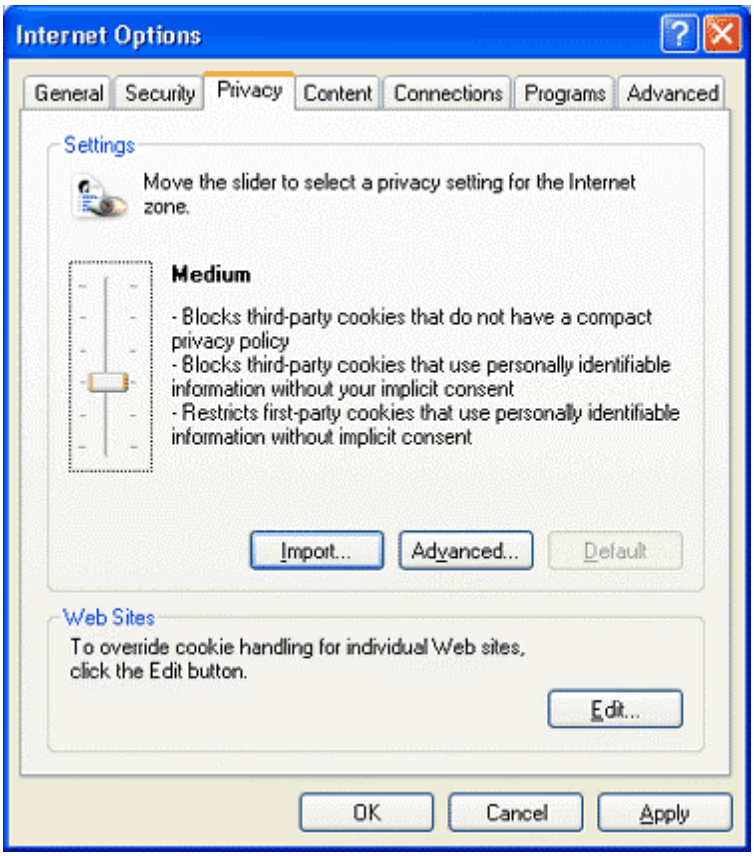

Abbildung 5.8: Internet Explorer 6

5.3.3 JRC P3P Proxy

JRC P3P Proxy arbeitet als vermittelnder Agent, der den Zugriff auf Web Seiten gemäss den angegebenen Privacy Präferenzen kontrolliert.

Dabei gibt es hier sechs vordefinierte Sicherheitsniveaux, unter denen ausgewählt werden kann. Die Importierung von Privacy Settings ist auch hier möglich. Diese werden bei JRC auf deren Server gespeichert. Mit Hilfe eines sogenannten Privacy Buttons, der auf dem eigenen PC installiert wird, kann man den Service aktivieren oder deaktivieren. Ist es aktiviert so wird bei einem Internetbesuch automatisch eine Verbindung zum Server hergestellt, auf dem die Privacy Präferenzen gespeichert sind.

Auf eine Anfrage wurde bestätigt, dass das EXTENSION Element in einem importierten Setting enthalten sein darf. Die Korrespondenz hierzu befindet sich in Anhang G.

Kapitel 6

Zusammenfassung & Ausblick

Es steht ausser Zweifel, das der Schutz der Privatsphäre von Internet-Nutzern gegenwärtig unzureichend ist. Die Chance sich im Netz relativ weiträumig und frei zu bewegen, steht die Möglichkeit gegenüber allerlei Informationen über Internet-Nutzer zu sammeln und auszuwerten. Dies ist natürlich auch im Intranet möglich.

Im Rahmen dieser Diplomarbeit wurden die verschiedenen Möglichkeiten überprüft, die zur Veröffentlichung von Datenschutzmassnahmen angeboten werden. Zunächst ist der OECD Privacy Statement Generator, dessen Principles Grundlage bei der Formulierung von Lufthansa Principles waren, auf Lufthansatauglichkeit untersucht worden. Dabei hat sich ergeben, dass trotz der theoretischen Übereinstimmung der Principles der Lufthansa AG mit denen der OECD, der Gebrauch des Generators bei Lufthansa in dieser Form nicht möglich ist. Da anfänglich eine Anpassung des Generators an Lufthansabedürfnisse geplant war, sind im Rahmen dieser Diplomarbeit Änderungsvorschläge gemacht worden. Die Anpassung des Codes erfolgte nicht, da dieser nur für öffentliche Stellen und nicht für Privatunternehmen zugänglich ist.

Mit P3P entwickelte das W3C eine Datenschutztechnik, die für Nutzer die Kontrolle über persönliche Daten automatisiert und damit den Schutz der Privatsphäre und die Akzeptanz der User verbessert. Nach der Einführung des P3P- und APPEL-Vokabulars, mit dem man einerseits Datenschutzmassnahmen und andererseits Datenschutzpräferenzen ausdrücken kann, sollte daher geprüft werden, ob dieses Vokabular ausreicht, um Lufthansa-spezifische Aussagen zu machen und in wieweit diese erweiterbar bzw. anpassbar sind. Die Untersuchung hat ergeben, dass das Vokabular bis zu einem gewissen Masse ausreicht und es ein Element gibt, das EXTENSION Element, mit dem eine Erweiterung des P3P Standardvokabulars möglich ist. Im Rahmen dieser Arbeit wurden solche auf Lufthansa abgestimmte Erweiterungen sowohl für eine P3P Policy als auch für eine entsprechende APPEL Präferenz formuliert. Die Lufthansa AG hat somit mit P3P die Möglichkeit, Ihre Datenschutzpraktiken für den Mitarbeiter transparenter zu gestalten, da sie auch über das Standardvokabular hinausgehende Aussagen formulieren kann.

In der Diplomarbeit sind ausserdem die sich zur Zeit auf dem Markt befindlichen Tools, die bei der Erstellung einer maschinenlesbaren Datenschutzmassnahme, der sog. Privacy Policy benutzt werden können, untersucht worden. Der IBM P3P Policy Editor scheint für den

Gebrauch bei Lufthansa denkbar, da die Handhabung des Generators einfach ist. Der Mitarbeiter, der die Policy für seine Abteilung erstellen soll, braucht sich nicht mit den Einzelheiten des P3P Vokabulars auseinander setzten. Mit diesem Editor kann zunächst ein Basisgerüst einer Policy erstellt werden. Die mit dem P3P Element EXTENSION formulierten Erweiterungen müssen jedoch selbsterstellt werden und können nachträglich in das Basisgerüst der Policy miteingebunden werden. Zusätzlich zu der maschinenlesbaren Form einer Policy erstellt der IBM Editor auch eine menschenlesbare HTML-Version der Policy. Dies ist sehr von Vorteil, da in einem Arbeitsgang zwei Policy-Versionen erstellt werden. Im Vergleich zu dem Formulierungsentwurf des OECD Generators ist die menschenlesbare Version des IBM Editors ausserdem wesentlich kürzer und dadurch auch übersichtlicher. Im Ganzen ist es daher sinnvoller, den IBM Editor zu benutzen, als den OECD Generator neu zu programmieren und dann mit Hilfe eines anderen Tools die P3P Policy zu erstellen.

Zur Erstellung einer APPEL Präferenz ist zur Zeit nur ein Hilfsmittel auf dem Markt erhältlich. Der Grund hierfür ist sicherlich, dass sich APPEL noch zu keinem Standard entwickelt hat, sondern sich noch in einem Entwurfsstadium befindet. Der APPEL Editor von JRC ist ähnlich wie der P3P Policy Editor von IBM aufgebaut. Auch hier müssen Erweiterungen selbst formuliert und in dem vom Editor erstellten Basisgerüst einer Präferenz eingebunden werden.

Nachdem die grundsätzliche Erweiterbarkeit von P3P in dieser Diplomarbeit festgestellt wurde, sind die sog. User Agents behandelt worden. Von Bedeutung war neben der Funktionsweise der einzelnen User Agents ihre Handhabung des EXTENSION Elementes. Da zu erwarten ist, dass nur wenige Nutzer die Voreinstellungen ihrer Software selbst verändern und sich mit der APPEL Spezifikation auseinander setzten, wird der Standardkonfiguration eines P3P User Agents eine große Bedeutung beigemessen. Bei allen vorgestellten User Agents gab es verschiedene Sicherheitsniveaux bzgl. Datenschutz aus denen der Nutzer auswählen konnte. Entsprechend des Niveaux wurde die Präferenz des Nutzers automatisch konfiguriert. Bei allen war es ausserdem möglich, selbsterstellte APPEL Formulierungen zu importieren. Bei dem Proxy von JRC ist es möglich, Settings mit einzubinden, die das EXTENSION Element beinhalten. AT&T erlaubt dies nicht und von Microsoft fehlt hierzu jegliche Angabe.

Bzgl. der Lufthansa AG erscheint es sinnvoll, den Mitarbeitern einen eigenen User Agent anzubieten, der alle zusätzlich formulierten Aspekte aufgreift und mit dem der Mitarbeiter seine Präferenzen bzgl. des Intranets leicht ausdrücken kann. Der Aufwand, den Mitarbeitern das erweiterte Vokabular für die Formulierung einer Präferenz zur Verfügung zu stellen, setzt voraus, dass jeder Mitarbeiter sich mit der Syntax und Semantik von P3P und APPEL auskennt. Dies ist im Vergleich zur Programmierung eines eigenen User Agents, der den Mitarbeitern zur Verfügung gestellt wird, aufwendiger und wahrscheinlich auch nicht realisierbar.

Grundsätzlich kann durch diese Massnahmen das Vertrauen der Mitarbeiter ins Intranet und damit die Nutzung dieses Mediums gesteigert werden. Die vermehrte Nutzung des Intranets auch für private Zwecke, wie zum Beispiel der Buchung von Reisen oder die Abfrage nach Flügen etc., würde für beide Seiten auch wirtschaftlichen Nutzen bringen. Für die Mitarbeiter selbst käme es z.B. zu einer Zeitersparnis, da sie jetzt zur Buchung ihrer Reisen nicht mehr in die Reisestelle müssen. Dies hätte natürlich auch wirtschaftliche Auswirkungen, da der Aufwand, um zur Reisestelle zu kommen, wegfällt. Aber auch die Lufthansa AG hätte durch die transparentere Gestaltung ihrer Datenschutzpraktiken wirtschaftlichen Nutzen. Die

Mitarbeiter z.B. in der Reisestelle würden durch das neue Vertrauen ihrer Kollegen ins Intranet und damit einhergehend die selbstständige Online-Buchungsmöglichkeit entlastet werden. Es könnten mehr Kapazitäten für andere Aufgaben frei werden. Das Ausmass der Vorteile für Lufthansa und Ihrer Mitarbeiter, die sich aus der Veröffentlichung von Datenschutzmaßnahmen ergeben und damit ist auch das vermehrte Vertrauen der Mitarbeiter ins Intranet gemeint, ist zur Zeit noch nicht in vollem Umfang erfassbar, da sich viele Intranetprojekte der Lufthansa AG noch im Entwicklungsstadium befinden.

Für die Zukunft ist jedoch auch festzustellen, dass datenschutzfreundliche Technologien allein nicht die Lösung zur Sicherstellung des Datenschutzes im Inter- als auch im Intranet sein können. Vielmehr müssen die aufkommenden technischen Maßnahmen durch nationale und internationale Regelungen unterstützt und ergänzt werden. Erst durch Festlegung internationaler Konventionen, die den Datenschutz in Zusammenhang mit grenzüberschreitenden Computernetzwerken und Diensten regeln, kann ein effektiver und unabhängiger Kontrollmechanismus sowie die Möglichkeit zu Sanktionen gewährleistet werden. Die Veröffentlichung von Datenschutzmassnahmen gewährleistet leider nicht ihre Einhaltung.

Kapitel 7

Anhang

A Fragebogen des OECD Privacy Statement Generators

In diesem Abschnitt ist der gesamte Fragenkatalog vom OECD Privacy Statement Generator, wie er für „my Travel ex“ ausgefüllt wurde, aufgeführt. Der Abschnitt 7.2 gehört allerdings nicht dazu, da die vorherige Frage so beantwortet wurde, dass diese Seite nicht vom Generator angezeigt wurde. Der Vollständigkeit wegen ist diese Seite jedoch mit aufgeführt worden.

Information about your Organisation and your Web Site (Section 1 of 11 , page 1)

This information will be disclosed in your privacy statement, so that visitors to your Web site(s) will know who you are.

1.1 Information about your organisation and the Web site(s) for which this statement is being generated

Organisation name:	Deutsche
Address	Lufthansa
City	Frankfurt
State/Province (where applicable)	
Zip/Postal Code	60546
Country	Germany
Name of the data controller	FRA XD/R
Principal activity(ies) of the Organisation (please indicate one activity in one field)	Buchung von
Web site(s) URL	lw w .travelex.

1.2 Do you want this statement to apply to any subsidiary of your Organisation, and its Web site(s) ?

( ) YES (•) NO

<< Back | Next >>

Providing Visitors with Anonymous Access (Section 2 of 11 , page 1)

2. Can visitors access your home page and browse your Web site(s) without disclosing personal data (except that data required for system administration, such as standard HTTP log information) ?

○ YES ◉ NO

<< Back | Next >>

Linkage Characteristics of your Web Site (Section 3 of 11 , page 1)

3.1 Can visitors communicate with other visitors or post data so that others may access it, via your Web site ?

○ YES ◉ NO

3.2 Does your Web site use a third party Web service provider (eg a company that collects personal data to distribute advertisements) that collects personal data about your visitors ?

◉ YES ○ NO

3.2.1 If yes, please specify the name of the third party:

1 eDirectory
2 AIDA
3 VIVA

<< Back | Next >>

Automatic Collection of Information (Section 4 of 11 , page 1)

4.1 Does your Web site use cookies for any reason ?

(•) YES ( ) NO

4.2 Does your organisation or Web site automatically log personal data by other means than cookies, such as programming, or link non-personal information logged automatically with personal data about a specific individual ?

(•) YES ( ) NO

4.2.1 If yes, for what purpose(s) ?

- [ ] Technical administration of the Web site
- [ ] Research and development
- [ ] Customer administration
- [ ] Marketing
- [ ] Trading in personal data
- [ ] Other . Please describe:

1 Abwicklung des Buchungsvorgangs
2
3

<< Back | Next >>

Automatic Collection of Information (Section 4 of 11 , page 2)

4.3 Does your organisation or Web site link non-personal information stored in cookies with personal data about a specific individual ?

○ YES ◉ NO

4.3.1 If yes, for what purpose(s) ?

- ☐ Technical administration of the Web site
- ☐ Research and development
- ☐ Customer administration
- ☐ Marketing
- ☐ Trading in personal data
- Other . Please describe:

1 _____

2 _____

3 _____

<< Back | Next >>

Data Collection and Purpose Specification (Section 5 of 11 , page 1)

5.1 Does your organisation or Web site collect personal data about your Web site visitors, which are volunteered by them when using yours services ?

◉ YES ○ NO

5.2 Does your organisation or Web site collect personal data about your visitors from other sources such as public records or bodies, or private organisations ?

○ YES ◉ NO

<< Back | Next >>

Data Collection and Purpose Specification (Section 5 of 11 , page 2)

You have indicated in question(s) 4.2, 4.3, 5.1 and/or 5.2 that you collect personal data. Please choose all that apply in the tables below.

5.3.1 Primary personal data/Business information

- [x] volunteered by each visitor
- [ ] collected from public records or bodies
- [ ] collected from private organisations

Primary personal data	Technical administration of the Web site	Research &development	Customer Administration	Marketing	Trading in personal data
Name	☐	☐	☐	☐	☐
Gender	☐	☐	☐	☐	☐
Address	☐	☐	☐	☐	☐
E-mail address	☐	☐	☑	☐	☐
Phone/Fax number	☐	☐	☑	☐	☐
other (describe) Reisepartner	☐	☐	☑	☐	☐

Business Information	Technical administration of the Web site	Research & development	Customer Administration	Marketing	Trading in personal data
Employer/organisation	☐	☐	☐	☐	☐
Job title	☐	☐	☐	☐	☐
Address	☐	☐	☐	☐	☐
E-mail address	☐	☐	☑	☐	☐
Phone/Fax number	☐	☐	☑	☐	☐
other (describe)	☐	☐	☐	☐	☐

5.3.2 Other personal details and profiling data

- [ ] volunteered by each visitor
- [ ] collected from public records or bodies
- [ ] collected from private organisations

	Technical administration of the Web site	Research & development	Customer Administration	Marketing	Trading in personal data
Personal details	☐	☐	☐	☐	☐
Physical description	☐	☐	☐	☐	☐
Family characteristics	☐	☐	☐	☐	☐

Education and skills	☐	☐	☐	☐	☐
Life style or personal tastes	☐	☐	☐	☐	☐
Financial resources	☐	☐	☐	☐	☐
other (describe) _____	☐	☐	☐	☐	☐

5.3.3 Identifiers

☐ volunteered by each visitor

☐ collected from public records or bodies

☐ collected from private organisations

	Technical administration of the Web site	Research & development	Customer Administration	Marketing	Trading in personal data
On-line identifiers	☐	☐	☐	☐	☐
Financial identifiers	☐	☐	☐	☐	☐
Identifiers assigned by Public bodies	☐	☐	☐	☐	☐
Biometrics identifiers	☐	☐	☐	☐	☐
other (describe) _____	☐	☐	☐	☐	☐

5.3.4 Specific Data

☐ volunteered by each visitor

☐ collected from public records or bodies

☐ collected from private organisations

	Technical administration of the Web site	Research & development	Customer Administration	Marketing	Trading in personal data
Racial or ethnic origin	☐	☐	☐	☐	☐
Political opinions	☐	☐	☐	☐	☐
Religious or philosophical beliefs	☐	☐	☐	☐	☐
Trade union membership	☐	☐	☐	☐	☐
Health/Medical data	☐	☐	☐	☐	☐
Sex life	☐	☐	☐	☐	☐
Police/Justice data such as civil/criminal actions brought by or against the visitor	☐	☐	☐	☐	☐
other (describe) _____	☐	☐	☐	☐	☐

<< Back | Next >>

Data Collection and Purpose Specification (Section 5 of 11 , page 3)

5.4 Is there any other purpose for which you collect and use personal data ?

○ YES ◉ NO

5.4.1 If yes, please describe the other purpose(s) for which you collect and use personal data (eg. We collect and use personal data for the additional purpose of...) ?

1 _____
2 _____
3 _____

5.5 Where you wish to use your visitor's personal data for purposes other than those indicated in previous sections of this questionnaire, do you give your visitors the opportunity to consent to those new purposes ?

◉ YES ○ NO

5.5.1 If yes, how can visitors express their choice ?

- ☐ By indicating in a box at the point on the site where personal data is collected
- ☐ By sending an email (Email address they should send mail to) _____
- ☐ By visiting this url (URL that they should visit) _____
- ☐ By sending postal mail to this address (Address to which they should write) _____
- ☐ By calling this telephone number (number to call) _____
- Other (explain) _____

<< Back | Next >>

Children's Privacy (Section 6 of 11 , page 1)

6.1 Do you knowingly collect personal data on children ?

(•) YES ( ) NO

6.2 Do you take specific steps to protect the privacy of children whose personal data you collect ?

(•) YES ( ) NO

6.2.1 If yes, please describe the specific steps you take to protect the privacy of children, and tick all relevant boxes below:

☑ We make reasonable efforts to verify that a parent has consented to the collection of the child's personal data.

☑ We give parents the option to consent to the collection and use of the child's personal data for internal use.

☑ We give parents the option to consent to the collection and use of the child's personal data for disclosure to third parties.

Other. Please describe (To ensure that children's privacy is respected on our Web site, we ...)

1 [ ]
2 [ ]
3 [ ]

6.2.2 Do you provide information detailing your personal data practices in relation to children on your home page and at every point at which you collect personal data from children ?

(•) YES ( ) NO

<< Back | Next >>

Disclosure and Visitor Choice (Section 7 of 11 , page 1)

7.1 Does your Web site or your organisation disclose personal data about its Web site visitors to its subsidiaries or to other organisations ?

○ YES ◉ NO

<< Back | Next >>

Disclosure and Visitor Choice (Section 7 of 11 , page 2)

7.2 Where disclosure occurs for the same purposes as you have indicated in previous sections of this questionnaire, do you offer your visitors the means to

☑ Opt-in

or / and

☐ Opt-out

7.2.1 Where you offer your visitors the means to opt-in or opt-out, how can visitors express their choice ?

☑	By indicating in a box at the point where your site collects personal data	
☐	By sending an email (Email address they should send mail to)	
☐	By visiting this url (URL that they should visit)	
☐	By sending postal mail to this address (Address to which they should write)	
☐	By calling this telephone number (number to call)	
	Other (explain)	

Confidentiality / Security (Section 8 of 11 , page 1)

8.1 Do you give visitors to your Web site the option of using a secure transmission method to send personal data to you ?

○ YES ◉ NO

8.2 Please indicate the types of personal data you allow visitors to send via a secure transmission method, by ticking the appropriate boxes:

☐ Primary personal data (such as name and contact details)

☐ Other personal and profiling data (such as physical description, leisure activities)

☐ Identifiers (such as credit card details, Web site password)

☐ Specific personal data (such as racial or ethnic origin, religious beliefs, medical data)

Other. Please describe :

1 _____

2 _____

3 _____

8.3 Does your Web site have security policies, rules or technical measures in place to protect visitor's personal data which are under your control from:

8.3.1 Unauthorised access ◉ YES ○ NO

8.3.2 Improper use or disclosure ◉ YES ○ NO

8.3.3 Unauthorised modification or alteration ◉ YES ○ NO

8.3.4 Unlawful destruction or accidental loss ◉ YES ○ NO

8.4 Are your employees and data processors obliged to respect the confidentiality of visitors' personal data ?

◉ YES ○ NO

8.5 Does your organisation and Web site ensure that visitors' personal data will not be disclosed to State institutions and authorities except if required by law or other regulation ?

◉ YES ○ NO

<< Back | Next >>

9.1 Can a visitor find out from your organisation or Web site whether you are keeping personal data relating to him or her ?

(•) YES ( ) NO

9.1.1 If yes, how can a visitor find out whether your organisation or Web site is keeping personal data about him or her ?

☑	By sending an email (Email address they should send mail to)	cgndsb@dlh.de
☑	By visiting this url (URL that they should visit)	http://lw w .travelex.dlh.de/
☐	By sending postal mail to this address (Address to which they should write)	
☐	By calling this telephone number (number to call)	
	Other (explain)	

9.2 Can a visitor obtain from your organisation or Web site an intelligible copy of the personal data that you keep about him or her ?

(•) YES ( ) NO

9.2.1 If yes, how can a visitor obtain an intelligible copy of the personal data that you keep about him or her?

☑	By sending an email (Email address they should send mail to)	cgndsb@dlh.de
☑	By visiting this url (URL that they should visit)	http://lw w .travelex.dlh.de/
☐	By sending postal mail to this address (Address to which they should write)	
☐	By calling this telephone number (number to call)	
	Other (explain)	

9.2.2 How long does it usually take for the visitor to obtain the information ?

☑	Almost instantaneously on-line	
☐	Within a week	
☐	Within a month	
☐	Longer (specify):	

9.2.3 Do you make a specific charge ?

○ YES ◉ NO

9.2.4 Please specify the amount of the charge:

9.3 Do you allow a visitor to challenge the data that you hold ?

◉ YES ○ NO

9.3.1 If a challenge is successful, can the visitor have their personal data (as may be appropriate to the particular case):

☑ Erased

☑ Rectified or amended

☑ Completed

9.4 Do you reserve the right to refuse to provide the data ?

○ YES ◉ NO

9.4.1 If yes, do you give reasons for refusing to provide information to a visitor ?

◉ YES ○ NO

9.4.2 Can a visitor challenge your refusal to provide personal data that you hold ?

◉ YES ○ NO

9.5 Do you require proof of identity before providing the personal data ?

◉ YES ○ NO

<< Back | Next >>

Privacy Compliance (Section 10 of 11 , page 1)

10.1 Are there any national privacy laws or self-regulatory schemes applicable to your web site or organisation?

(•) YES ( ) NO

10.1.1 If yes, is your privacy policy compliant with the applicable national privacy law or self-regulatory schemes ?

(•) YES ( ) NO

10.1.2 Please mention the main privacy instrument(s) your policy is compliant with (title and country in each field)

1	Bundesdatenschutzgesetz BDSG
2	Betriebsverfassungsgesetz BetrVerfG
3	

10.2 Are there any global or regional privacy regulatory or self-regulatory schemes applicable to your Web site or organisation ?

(•) YES ( ) NO

10.2.1 If yes, is your privacy policy consistent with a global or regional regulatory privacy instrument or self-regulatory privacy scheme?

(•) YES ( ) NO

10.2.2 Please mention the main global or regional regulatory privacy instrument(s) or self-regulatory scheme(s) your policy is consistent with (title and origin in each field)

1	Lufthansa Konzern Datenschutz Prinzipie
2	
3	

10.3 In order to demonstrate that your privacy policy accords with the applicable regulation indicated above, are you:

☑ Voluntarily committed to a Self Assessment procedure

☐ Voluntarily committed to a Third Party Organisation certification

☑ Subject to a Government Agency supervision

☑ Subject to an Independent Data Protection Authority supervision

10.3.1 Please indicate the following details for all that apply above:

Self Assessment procedure

Name or designation of the privacy policy person or service	Konzern Datenschutz
URL	
Address	CGN DSB
Country	

Third Party Organisation certification

Designation of the organisation	
URL	
Address	
Country	

Government Agency supervision

Designation of the agency	Landesbeauftragte für
URL	www.lfd-nrw.de
Address	Düsseldorf
Country	Germany

Independent Data Protection Authority supervision

Designation of the authority	Landesbeauftragte für
URL	www.lfd-nrw.de
Address	Düsseldorf
Country	Germany

<< Back | Next >>

Privacy Support (Section 11 of 11 , page 1)	
11.1 Do you provide visitors to your Web site with details of who to contact if they have a privacy enquiry or concern ? ◉ YES ○ NO	

B Draft Privacy Statement für das Projekt „my Travel ex“ erstellt vom OECD Generator

***<Draft>* Privacy Statement of Deutsche Lufthansa AG**
Statement N° 7252

Information about our Organisation and Web site

Modern information and communication technologies play a fundamental role in the activities of an organisation like Deutsche Lufthansa AG . We are based in Germany .
Our principal activity is: Buchung von ID-Reisen
Our privacy policy covers Deutsche Lufthansa AG and its Web site:

Organisation Name:	Deutsche Lufthansa AG
Address:	Lufthansa Basis
City, Zip:	Frankfurt , 60546
Country:	Germany
Controller:	FRA XD/R
Web Sites(s):	lww.travelex.dlh.de/

The services and links of our Web site

Our Web site does not enable our visitors to communicate with other visitors or to post information to be accessed by others.

Our Web site includes a link to:

- eDirectory
- AIDA
- VIVA

Such third party Web service providers may collect personal data about our visitors.

Automatic Collection of Information

We automatically log personal data by means such as programming or we link information automatically logged by such means with personal data about specific individuals. We do so for the following purposes:

- Abwicklung des Buchungsvorgangs

We do not use cookies to store personal data nor do we link non-personal information stored in cookies with personal data about specific individuals.

Data Collection and Purpose Specification

We collect the personal data that you may volunteer while using our services.

We do not collect information about our visitors from other sources, such as public records or bodies, or private organisations.

To access the table of personal data collected and purposes for which they are used, please click here

We do not collect or use personal data for any purpose other than that indicated in the table below.

If we wish to use your personal data for a new purpose, we offer you the means to consent to this new purpose:

Children's Privacy

We knowingly collect personal data from children.

We take specific steps to protect the privacy of children by:

- making reasonable efforts to ensure that a parent has authorised the collection of the child's personal data and use of the child's personal data for the disclosure to third parties.
- giving parents the option to consent to the collection and use of the child's personal data for our internal use and use of the child's personal data for the disclosure to third parties.

We do provide information about our personal data practices in relation to children on our home page and wherever we knowingly collect personal data from children on our Web site.

Disclosure and Visitor Choice

We do not disclose your personal data to our subsidiaries or other organisations.

Where we disclose your personal data for the same purposes as those indicated in the table below, we provide you with the means to opt-in to disclosure:

- by indicating in a box at the point on the site where personal data is collected
-
-
-

Where we disclose your personal data for purposes which are different from those indicated in the table mentioned above, we offer you the opportunity to consent to disclosure:

- by indicating in a box at the point on the site where personal data is collected
-
-
-

Confidentiality / Security

We do not give visitors to our Web site the option of using a secure transmission method to send us their personal data.

We have implemented security policies, rules and technical measures to protect the personal data that we have under our control from:

- unauthorised access
- improper use or disclosure
- unauthorised modification
- unlawful destruction or accidental loss

All our employees and data processors, who have access to, and are associated with the processing of personal data, are obliged to respect the confidentiality of our visitors' personal data.

We ensure that your personal data will not be disclosed to State institutions and authorities except if required by law or other regulation.

Access to the personal data we may hold about you

You can ask us, by:

- sending an email (cgndsb@dlh.de)

- visiting this url (http://lww.travelex.dlh.de/)

whether we are keeping personal data about you.

Upon request, which you can indicate by:

- sending an email (cgndsb@dlh.de)
- visiting this url (http://lww.travelex.dlh.de/)

We will provide you with a readable copy of the personal data which we keep about you, almost instantaneously on-line. - although we may before require proof of your identity -. We will provide the information without any charge.

We allow you to challenge the data that we hold about you and, where appropriate, you may have the data:

- erased
- rectified or amended
- completed

We do not reserve the right to refuse to provide you with a copy of your personal data.

We do, however, allow you to challenge our decision to refuse to provide you with a copy of your personal data.

Privacy Compliance

Our privacy policy is compliant with the following instruments:

- Bundesdatenschutzgesetz BDSG
- Betriebsverfassungsgesetz BetrVerfG

It is also compliant with the following global or regional regulatory, or self-regulatory instrument: Lufthansa Konzern Datenschutz Prinzipien

In order to demonstrate that our privacy policy accords with the above privacy instruments, we are:

- voluntarily committed to a Self Assessment procedure
- subject to a Government Agency supervision
- subject to an Independent Data Protection Authority supervision

Self Assessment procedure

Name or designation of the privacy policy person or service	Konzern Datenschutz Beauftragter
URL	
Address	CGN DSB

Country	

Government Agency supervision

Designation of the agency	Landesbeauftragter für Datenschutz in NRW
URL	www.lfd-nrw.de
Address	Düsseldorf
Country	Germany

Independent Data Protection Authority supervision

Designation of the authority	Landesbeauftragter für Datenschutz in NRW
URL	www.lfd-nrw.de
Address	Düsseldorf
Country	Germany

Privacy Support

If you have an enquiry or concern about our privacy policy, please contact:

	Contact 1
Name/designation :	Jürgen Weber
Department :	FRA DSB
Address :	Lufthansa Basis
Phone Number :	069 696 3206
Fax Number :	069 696 93899
Email address :	juergen.weber@dlh.de
URL :	lww..finanzen.lh.cgn.dlh.de/servlet/PB/menu/1000222_pcontent/content.html

If you are not satisfied with our response to your concern:

- you may wish to contact LfD NRW (www.lfd-nrw.de)
- you may wish to contact LfD NRW (www.lfd-nrw.de)

TABLE of personal data collected and purposes for which they are used

Primary personal data/Business information

x volunteered by each visitor

- collected from public records or bodies
- collected from private organisations

Primary personal data	Technical administration of the Web site	Research &development	Customer Administration	Marketing	Trading in personal data
Name	-	-	-	-	-
Gender	-	-	-	-	-
Address	-	-	-	-	-
E-mail address	-	-	**x**	-	-
Phone/Fax number	-	-	**x**	-	-
other (describe) *Reisepartner*	-	-	**x**	-	-

Business Information	Technical administration of the Web site	Research & development	Customer Administration	Marketing	Trading in personal data
Employer/organisation	-	-	-	-	-
Job title	-	-	-	-	-
Address	-	-	-	-	-
E-mail address	-	-	**x**	-	-
Phone/Fax number	-	-	**x**	-	-
other (describe)	-	-	-	-	-

Other personal details and profiling data

- volunteered by each visitor
- collected from public records or bodies
- collected from private organisations

	Technical administration of the Web site	Research & development	Customer Administration	Marketing	Trading in personal data
Personal details	-	-	-	-	-
Physical description	-	-	-	-	-
Family characteristics	-	-	-	-	-
Education and skills	-	-	-	-	-
Life style or personal tastes	-	-	-	-	-
Financial resources	-	-	-	-	-
other (describe)	-	-	-	-	-

Identifiers

- volunteered by each visitor
- collected from public records or bodies
- collected from private organisations

	Technical administration of the Web site	Research & development	Customer Administration	Marketing	Trading in personal data
On-line identifiers	-	-	-	-	-
Financial identifiers	-	-	-	-	-
identifiers assigned by Public bodies	-	-	-	-	-

Biometrics identifiers	-	-	-	-	-
other (describe)	-	-	-	-	-

Specific Data

- volunteered by each visitor
- collected from public records or bodies
- collected from private organisations

	Technical administration of the Web site	Research & development	Customer Administration	Marketing	Trading in personal data
Racial or ethnic origin	-	-	-	-	-
Political opinions	-	-	-	-	-
Religious or philosophical beliefs	-	-	-	-	-
Trade union membership	-	-	-	-	-
Health/Medical data	-	-	-	-	-
Sex life	-	-	-	-	-
Police/Justice data such as civil/criminal actions brought by or against the visitor	-	-	-	-	-
Other (describe)	-	-	-	-	-

C Korrespondenz mit OECD

1. Ausgangsbrief

Dear Sirs,

I am a student of computer science at the Johann-Wolfgang-Goethe-University in Frankfurt/Germany.

As part of my masters thesis I used your generator to examine the possibility weather this generator is applicable for the Lufthansa Intranet. There are two questions I would be pleased if they could be answered.

1)While using it a problem occurred in section 5 with question 5.5:

“Where you which to use your visitors personal data for purposes other than those indicted in previous sections of this questionnaire, do you give your visitors the opportunity to consent to those new purposes?”

On the one hand you offer the possibility to agree or to deny to this question, but on the other hand the generator only accepts an agreement to this question.

I know that the USE LIMITATION PRINCIPLE requires that the individual has a possibility to consent to it, but to carry on with the questionnaire, the user would have to “lie” here if that is not his policy.

The draft of the privacy statement you offer would not represent the real privacy policy of the user.

Is there any other possibility to solve this matter than to give a false answer?

2) For my masters thesis I am also examining the usage of P3P for Lufthansa.

Is there any further planning in giving the user of your generator a XML-version of the draft statement along with the human readable form?

This would be an easing for the user as he has already answered your questions and would not have to use another generator to convert your draft statement into an XML-version.

It would be nice to have the questions answered for the proceeding of my masters thesis.
I thank you for answering these questions beforehand.

Yours sincerely

Bhakti Meyer

2. Antwortschreiben und weitere Korrespondenz

Anmerkung: Diese Korrespondenz ist aus meinem e-mail Fach kopiert und deshalb in umgekehrter Reihenfolge aufgeführt.

Dear Bhakti,

When do you need to submit your thesis? Or are you defending it? I am treating your letter urgently with the technicians - and hope to have an answer soon. As Ms. Carblanc said, a yes/no answer to Question 5.5 was not deliberate (and I had noted a "logic" problem with it as well) - so we will be looking to fix this. I am checking the future possibility of XML versions of the statements - and will get back to you as soon as possible.

Thanking you for your patience - and my apologies for our late response!

Sincerely,

Julie Harris
OECD Information, Computer and
Communications Policy Division
Tel: (33 1) 45 24 18 74
Fax: (33 1) 44 30 62 59
E-mail: julie.harris@oecd.org <mailto:julie.harris@oecd.org>

-----Original Message-----
From: CARBLANC Anne, STI/ICP
Sent: Thursday, March 07, 2002 3:19 PM
To: 'bhakti@freenet.de'
Cc: HARRIS Julie, STI/ICP
Subject: RE: Questions regarding your generator

Dear Mr. Meyer,

Thank you for your interest in the OECD Privacy Generator. We are happy to receive feed-back on its use because it helps us correct errors and improve the tool.

Julie Harris, who is on cc, will get back to you on the two issues that you mention, after a discussion with our technical experts.

However, as concerns your first question, I can already tell you that there was never a deliberate choice not to take account of a negative answer in

5.5.

Do not hesitate to contact us again.

Best regards.
Anne Carblanc

-----Original Message-----
From: bhakti@freenet.de [mailto:bhakti@freenet.de]
Sent: Thursday, March 07, 2002 9:33 AM
To: Anne.CARBLANC@oecd.org
Subject: Questions regarding your generator

Dear Mrs.Carblanc,

I'm a computer science student at the university in Frankfurt/Germany. For my masters thesis at Lufthansa AG I used your privacy generator. While using it some questions occurred. Regarding this I've already contacted your organization twice, but until now there has been no reply.
Mr. Weber, who contacted you last November regarding the source code of the generator, gave me your e-mail address. May-be you could help me. I've attached my former letter to the OECD. Please read it for details and reply even if you cannot answer my questions. May-be there is someone else I could contact.

Regards
Bhakti Meyer

3. Endschreiben

Dear Bhakti,

Here are the answers to your questions:

1. We are currently looking at rephrasing question 5.5 or separating it into two questions. In the first case, the question might read something like: If you were to wish to use your visitor's personal data for purposes other than those indicated in the previous sections of this questionnaire in the future, would you, or do you, give your visitors the opportunity to consent to those new purposes? This reformulation highlights the possible FUTURE use of personal data which was not clear in the question. Alternatively, we could split the question into two questions: "Do you use visitor's data for other purpose than already indicated ?", followed conditionally by "If Yes, do you give the visitors the opportunity to ...". We hope to resolve this issue in the very near future - as it has posed problems for other users as well.

2. P3P compliance was discussed a bit during the development of the Privacy Generator. At this time, there was little support, no finished standardization and no industry products implementing it, so, with regards to the cost of implementation of this feature, the decision was made at that time to not generate a P3P XML policy. As there are no current plans to issue a new version (V4) of the Privacy Generator, implementing P3P policy generation will not be possible at this time.

Hoping this proves useful, and that if we can be of further assistance, you will not hesitate to contact us again.

Sincerely,

Julie Harris
OECD Information, Computer and
Communications Policy Division
Tel: (33 1) 45 24 18 74
Fax: (33 1) 44 30 62 59
E-mail: julie.harris@oecd.org <mailto:julie.harris@oecd.org>

D XML-Code für das Projekt „my Travel ex“ erstellt vom IBM P3P Privacy Editor

```
<?xml version="1.0"?>
<POLICIES xmlns="http://www.w3.org/2001/09/P3Pv1">
    <!-- Generated by IBM P3P Policy Editor version Beta 1.9 build 11/28/01
2:02 PM -->

    <!-- Expiry information for this policy -->
    <EXPIRY max-age="604800"/>

<POLICY
    discuri="http://?????"
    opturi="?????"
    name="Travelex">
    <!-- Description of the entity making this policy statement. -->
    <ENTITY>
    <DATA-GROUP>
<DATA ref="#business.name">Deutsche Lufthansa AG</DATA>
<DATA ref="#business.contact-
info.online.uri">http://lww.travelex.dlh.de/</DATA>
<DATA ref="#business.contact-info.postal.organization">Deutsche Lufthansa
           AG</DATA>
<DATA ref="#business.contact-info.postal.street">Lufthansa Basis</DATA>
<DATA ref="#business.contact-info.postal.city">Frankfurt</DATA>
<DATA ref="#business.contact-info.postal.postalcode">60546</DATA>
<DATA ref="#business.contact-info.postal.country">Germany</DATA>
    </DATA-GROUP>
    </ENTITY>

    <!-- Disclosure -->
    <ACCESS><none/></ACCESS>


    <!-- Disputes -->
    <DISPUTES-GROUP>
        <DISPUTES resolution-type="service"
service="http://lww.finanzen.lh.cgn.dlh.de/servlet/PB/menu/1000222_pcontent
/content.html" short-description="Datenschutzbeauftragter Konzern">
            <LONG-DESCRIPTION>Datenschutzbeauftragter des Konzerns</LONG-
DESCRIPTION>
    <!-- No remedies specified -->
        </DISPUTES>
        <DISPUTES resolution-type="independent" service="http://www.lfd-
nrw.de" short-description="Landesbeauftragter für Datenschutz in NRW">
            <LONG-DESCRIPTION>Landesbeauftragter für Datenschutz</LONG-
DESCRIPTION>
    <!-- No remedies specified -->
        </DISPUTES>
    </DISPUTES-GROUP>

    <!-- Statement for group "Benachrichtigung" -->
    <STATEMENT>
```

```
        <EXTENSION optional="yes">
            <GROUP-INFO
xmlns="http://www.software.ibm.com/P3P/editor/extension-1.0.html"
name="Benachrichtigung"/>
        </EXTENSION>

    <!-- Consequence -->
    <CONSEQUENCE>
Die Telefonnummern werden für Rücksprachen benötigt.</CONSEQUENCE>

    <!-- Use (purpose) -->
    <PURPOSE><contact/><current/><telemarketing/></PURPOSE>

    <!-- Recipients -->
    <RECIPIENT><ours/></RECIPIENT>

    <!-- Retention -->
    <RETENTION><indefinitely/></RETENTION>

    <!-- Base dataschema elements. -->
    <DATA-GROUP>
    <DATA ref="#user.home-info"/>
    <DATA ref="#user.business-info"/>
    </DATA-GROUP>
</STATEMENT>

<!-- End of policy -->
</POLICY>
</POLICIES>
```

E HTML-Version für das Projekt „my Travel ex“ erstellt vom IBM P3P Privacy Editor

Privacy Policy

About Us

This is a privacy policy for Deutsche Lufthansa AG. Our homepage on the Web is located at http://lww.travelex.dlh.de/. The full text of our privacy policy is available on the Web at http://????? Users may go to ????? for information on how to opt-in or opt-out of use of their information.

We invite you to contact us if you have questions about this policy. You may contact us by mail at the following address:

```
Deutsche Lufthansa AG
Lufthansa Basis
Frankfurt, 60546
Germany
```

Dispute Resolution and Privacy Seals

We have the following privacy seals:

- **Datenschutzbeauftragter Konzern**: Datenschutzbeauftragter des Konzerns
- **Landesbeauftragter für Datenschutz in NRW**: Landesbeauftragter für Datenschutz

Additional Information

This policy is valid for 1 week from the time that it is loaded by a client.

Data Collection

P3P policies declare the data they collect in groups (also referred to as "statements"). This policy contains 1 data group. The data practices of each group will be explained seperately.

Group "Benachrichtigung"

We collect the following information:

- User's Home Contact Information

- User's Business Contact Information

This data will be used for the following purposes:

- Completion and support of the current activity.
- Contacting visitors for marketing of services or products.
- Telemarketing.

This data will be used by ourselves and our agents.

The following explanation is provided for why this data is collected:

> Die Telefonnummern werden für Rücksprachen benötigt.

Cookies

Cookies are a technology which can be used to provide you with tailored information from a Web site. A cookie is an element of data that a Web site can send to your browser, which may then store it on your system. You can set your browser to notify you when you receive a cookie, giving you the chance to decide whether to accept it.

We do not make use of HTTP cookies.

Policy Evaluation

Microsoft Internet Explorer 6 will evaluate this policy's compact policy whenever it is used with a cookie. The actions IE will take depend on what privacy level the user has selected in their browser (Low, Medium, Medium High, or High; the default is Medium. In addition, IE will examine whether the cookie's policy is considered satisfactory or unsatisfactory, whether the cookie is a session cookie or a persistent cookie, and whether the cookie is used in a first-party or third-party context. This section will attempt to evaluate this policy's compact policy against Microsoft's stated behavior for IE6.

Note: this evaluation is currently experimental and should not be considered a substitute for testing with a real Web browser.

Satisfactory policy: this compact policy is considered *satisfactory* according to the rules defined by Internet Explorer 6. IE6 will accept cookies accompanied by this policy under the High, Medium High, Medium, Low, and Accept All Cookies settings.

F Brief an Microsoft

Dear Sirs,
I’m a student of computer science at the university of Frankfurt. For my masters thesis I’m focusing on the EXTENSION Element of the P3P Specification of the W3C.
With your Internet Explorer 6 it is possible for a user to import privacy preference settings from other resources or self-defined ones.
My question is:
Is the EXTENSION Element allowed in such an imported setting?

I already found out that the AT&T Privacy Bird does not allow the EXTENSION element. And the JRC P3P Proxy allows it.

For finishing my thesis it would be nice if you could answer my question as soon as possible.

Thank you for your effort.

Yours sincerely
Bhakti Meyer

G Korrespondenz mit JRC

Anmerkung: Die Korrespondenz ist aus meinem e-mail Fach kopiert und deshalb in umgekehrter Reihenfolge aufgeführt.

Betreff: Re: Re: Extension-Mechanism

Yes - this is what I understood you to mean.
Yes it does.

----- Original Message -----
From: <bhakti@freenet.de>
To: "Giles Hogben" <giles.hogben@jrc.it>
Sent: Monday, May 13, 2002 9:43 AM
Subject: Re: Re: Extension-Mechanism

> Dear Mr. Hogben,
>
> I think my last mail was a bit misunderstanding. I did not mean the extension element in the P3P statement of a service.
> My question was pointing at the extension element in a preference setting of an user . Does your server allow to import settings that include the extension element in selfdefined privacy preferences of an user?
>
> Bhakti Meyer
> ----- original Nachricht --------
>
>
>
> Yes as far as I know, it should accept the extension element.
> The matching algorithm used is just a general subtree match with logical
> connectives.
> It does not really "care" about the names of the tags.
> If you read the algorithm for matching on
>
> <u>http://www.w3.org/TR/P3P-preferences</u>;
>
> Section 5.5, you can see how it works.
>
> However, I would add, that our version is using a slightly older version

of
> the specification as regards optional elements. This should not make much
> difference to the Extension element behavior. I will alter it shortly.
>
> The java code is available on the site.
>
> Let me know if you need to know anything else (I will be away from today
> afternoon till next wed)
>
> Giles
>
> _____
> Giles Hogben
> TP361
> CyberSecurity Unit
> Institute for the Protection and Security of the Citizen (IPSC)
> European Commission - Euratom Centro Comune di Ricerca
> Via Enrico Fermi 1
> 21020 Ispra, Italy
> e-mail: giles.hogben@jrc.it
>
>
> ----- Original Message -----
> From: <bhakti@freenet.de>
> To: <giles.hogben@jrc.it>
> Sent: Wednesday, May 08, 2002 10:01 AM
> Subject: Extension-Mechanism
>
>
> > Dear Mr. Hogben,
> >
> > I’m a student of computer science at the university of Frankfurt/Main in
> Germany. For my masters thesis I am examining the P3P Specification
> regarding the extension element.
> >
> > With your proxy server, where one has to register, it is possible to
> import selfdefined stettings. My question now is:
> > Is the extension element accepted by your server?
> > Unfortunately I could not find an information to this question.
> >
> > I have also examined the AT&T Privacy Bird and it does not accept the
> extention element.
> >
> > It would be nice to get an answer from you as soon as possible.
> > I thank you for your effort and remain
> > Yours sincerely
> > Bhakti Meyer

Literaturverzeichnis

1. *Bundesdatenschutzgesetz – Text und Erläuterungen* - ,cw Obotritendruck GmbH, 4. Auflage November 1996

2. *Arbeitsrichtlinie Datenschutz der Lufthansa AG*, Januar 1995

3. OECD: *What is the OECD Privacy Statement Generator?*, http://cs3-hq.oecd.org/sripts/pwv3/pwhome.htm

4. OECD: *Developing a Privacy Policy and Statement*, http://cs3-hq.oecd.org/sripts/pwv3/pwpart1.htm

5. OECD: *Help for using the OECD Privacy Generator*, http://cs3-hq.oecd.org/sripts/pwv3/Help.html

6. OECD: *Guidelines on the Protection of Privacy and Transborder Flows of Personal Data*, 05 January 1999, http:// www1.oecd.org/dsti/sti/it/secur/prod/PRIV-EN.HTM

7. *LH Privacy Principles*, Datenschutzgrundsätze des Lufthansa Konzerns

8. W3C: *Platform for Privacy Preferences (P3P) Project*, 31.07.2001, http://www.w3c.org/P3P

9. Presler-Marshall: *The Platform for Privacy Preferences 1.0 Deployment Guide*, W3C Note 30 November 2001, http://www.w3c.org/TR/p3pdeployment

10. W3C: *P3P 1.0: A New Standard in Online Privacy*, 22.10.2001, http://www.w3c.org/P3P/brochure.html

11. Rigo: *P3P and Privacy on the Web FAQ*, 22.06.2001, http://www.w3c.org/P3P/p3pfaq.htlm

12. Koike: *Make Your Web Site P3P Compliant*, 31.01.2002, http://www.w3c.ogr/P3P/details.html

13. Cranor, Langheinrich, Marchiori, Presler-Marshall, Reagle: *The Platform for Privacy Preferences 1.0 (P3P1.0) Specification*, W3C Recommendation, 14.04.2002,

14. Cranor, Langheinrich, Marchiori: *A P3P Preference Exchange Language 1.0 (APPEL 1.0)*, W3C working Draft 26.02.2001, http://www.w3c.org/TR/P3P-preferences

15. W3C: *References for P3P Implementations*, http://www.w3c.org/P3P/implementations

16. Microsoft: W*eb Privacy*, 27.08.2001, http://www.microsoft.com/windows/ie/evaluation/overview/privacy.asp

17. W3C: *XML: Extensible Markup Language (XML)* http://www.w3c.org/XML