WIRTSCHAFTSUNIVERSITÄT WIEN

DIPLOMARBEIT

Titel der Diplomarbeit:
Analyse der Akzeptanz von datenschutzfreundlichen Technologien von Kunden und Unternehmen

Verfasserin/Verfasser: Sandra Wickenhauser

Matrikel-Nr.: 0150761

Studienrichtung: J151 Betriebswirtschaft

Beurteilerin/Beurteiler: Univ. Prof. Dipl.-Ing. Mag. Dr. Wolfgang Panny

Ich versichere:

dass ich die Diplomarbeit selbstständig verfasst, andere als die angegebenen Quellen und Hilfsmittel nicht benutzt und mich auch sonst keiner unerlaubten Hilfe bedient habe.

dass ich dieses Diplomarbeitsthema bisher weder im In- noch im Ausland (einer Beurteilerin/ einem Beurteiler zur Begutachtung) in irgendeiner Form als Prüfungsarbeit vorgelegt habe.

dass diese Arbeit mit der vom Begutachter beurteilten Arbeit übereinstimmt.

Datum

Unterschrift

Deckblatt

Analyse der Akzeptanz von datenschutzfreundlichen Technologien von Kunden und Unternehmen

Kurzfassung

Datenschutzfreundliche Technologien sollen den Nutzern helfen, ihre persönlichen Daten aktiv im Internet zu schützen. Je nachdem welches Tool eingesetzt wird, kann die Übertragung von personenbezogenen Informationen auf ein Minimum reduziert werden. Diese Arbeit beschäftigt sich mit den Themen Datenschutz, Privatsphäre, rechtlichen Grundlagen zum Thema Datenschutz und datenschutzfreundlichen Technologien („privacy enhancing technologies“ - PET). Des Weiteren wird im Detail auf die PETs P3P, APPEL und EPAL eingegangen. Im empirischen Teil der Arbeit wird zunächst der Einsatz von P3P bei ausgewählten Unternehmen der Forbes 400 untersucht. In einem weiteren Schritt werden StudentInnen der Wirtschaftsuniversität Wien mittels eines Fragebogens zu Einflussfaktoren auf das Kaufverhalten im Internet und eventuellen Ängsten befragt. Weiters sollen der Einfluss und die Wahrnehmung von Datenschutzerklärungen und -zertifikaten auf die Kundenseite untersucht werden.

INHALTSVERZEICHNIS

Abbildungsverzeichnis

Tabellenverzeichnis

Einleitung – Motivation und Zielsetzung der Arbeit

In diesem Kapitel werden die Forschungsfragen und Ziele der Arbeit festgelegt. Weiters wird die Arbeit kapitelweise zusammengefasst, um den/der LeserIn einen Überblick zu verschaffen

1.1. Problemstellung

Gemäß Kobsa (2007) zeigen Konsumentenstudien, dass Internet-Nutzer gerne auf personalisierte Seiten zugreifen. Gleichzeitig sind Kunden aber über ihre Privatsphäre bei der Nutzung dieses Services besorgt, vor allem wenn sie personenbezogene Daten übermitteln müssen. Der/die KonsumentIn kann sich nicht sicher sein, welche seiner/ihrer Daten gespeichert und analysiert werden. Datenschutzfreundliche Technologien sollen dabei dem Benutzer eine Hilfestellung bieten. Neben der rechtlichen Verpflichtung von Unternehmen die Daten ihrer Kunden nicht zu missbrauchen, oder mehr zu sammeln als ihnen erlaubt wurde, gibt es auch seitens der Kundenbindung beziehungsweise des Konsumentenvertrauens Aspekte die für eine aktive Datenschutzpolitik sprechen.

Zurzeit besteht für Kunden das Problem, dass es sehr zeitaufwändig ist, erstens die Datenschutzerklärung auf einer Homepage zu finden und zweitens diese dann auch zu verstehen, da sie oft sehr komplex und lang geschrieben sind. „P3P-Agenten“ sind Tools, die helfen diesen umständlichen Prozess nutzerfreundlicher zu gestalten. Die Nutzer können im Vorfeld definieren welche persönlichen Daten freigegeben werden. Der P3P-Agent fragt, bevor eine Homepage geladen wird, automatisiert ab, welche Daten auf der jeweiligen Homepage erfasst und zu welchem Zweck sie verwendet werden. Sollten die Einstellungen des Kunden und der Webseite nicht übereinstimmen, wird die Seite nicht angezeigt oder es erscheint eine Warnung. Problematisch hierbei ist aber, dass dieses Tool keine Garantie für die Einhaltung der versprochenen Datenverarbeitung liefert; es überprüft lediglich die vom Anbieter definierte elektronische Version der Datenschutzerklärung mit den Einstellungen des Nutzers [P3PToolbox].

1.2. Inhalt und Vorgehensweise - Überblick über die Arbeit

Diese Arbeit unterteilt sich in zwei Abschnitte. Der erste Abschnitt (Kapitel 2-3) bildet die Literaturgrundlage, um den/die LeserIn in die Problematik einzuführen. Kapitel zwei beschäftigt sich mit dem Thema Datenschutz. Zuerst werden Definitionen für Datenschutz und Privatsphäre vorgestellt und in einem weiteren Schritt die Gründe, die für Datenschutz sprechen, erläutert. Danach folgt eine Aufbereitung der Literatur über Konsumentenvertrauen im Internet. Des Weiteren werden rechtliche Rahmenbedingungen auf nationaler und europäischer Ebene vorgestellt (DSG2000, EU Richtlinien, TKG2003). Anschließend werden die „datenschutzfreundlichen Technologien“ (privacy enhancing technologies – PET) erläutert. Das 3. Kapitel beschäftigt sich mit P3P, EPAL und APPEL und stellt deren Funktionsweisen, Ziele, Vor- und Nachteile vor. Kapitel vier beinhaltet den empirische Teil der Arbeit und bildet den zweiten Abschnitt. Folgende Fragen werden beantwortet:

- Wird P3P bei einer ausgewählten Stichprobe der Forbes 400 Unternehmen eingesetzt und wenn ja, stimmen die für den Menschen lesbaren Datenschutzerklärungen mit der P3P Policy überein?
- Welchen Einfluss haben Datenschutzklauseln auf die Bereitschaft von Kunden im Internet personenbezogene Daten preiszugeben? (Zusatzfrage: Gibt es weitere Faktoren, die Einfluss auf Konsumentenvertrauen im Internet haben?)

Zunächst wird in Kapitel 4.1. eine Stichprobe der Forbes 400 Unternehmen ausgewählt und überprüft, ob P3P eingesetzt wird. Des Weiteren werden die Datenschutzklauseln, welche auf den jeweiligen Webseiten der Unternehmen zu finden sind, mit der P3P Compact Policy verglichen. Dabei soll untersucht werden, ob die für den Menschen lesbare Datenschutzerklärung mit der für den Computer lesbaren Version übereinstimmen. Kapitel 4.2. beinhaltet eine Untersuchung mittels Fragebogen an StudentInnen der Wirtschaftsuniversität Wien. Dabei sollen Einflussfaktoren auf das Kaufverhalten im Internet ermittelt, sowie eventuell bestehende Ängste aufgezeigt werden. Weiterer Aspekt der Umfrage ist die Eruierung des Einflusses von Datenschutzerklärungen und –zertifikaten, sowie die Identifikation von möglichen Einflussfaktoren auf das Vertrauen von Konsumenten.

I. Theoretischer Teil

Dieser Teil der Arbeit bietet eine theoretische Einführung in die Themengebiete Konsumentenvertrauen sowie datenschutzfreundliche Technologien und fasst die relevante Literatur zum Thema Datenschutz zusammen. Ziel ist es den/die LeserIn auf den empirischen Teil vorzubereiten.

2. Datenschutz

In diesem Kapitel werden die verschiedenen Gründe, die für Datenschutz sprechen, erläutert. Zuerst soll eine kurze Einführung zu den Themen Privatsphäre und Datenschutz einen Einblick in die Thematik gewähren und deren Entwicklung erläutert werden. Danach wird die Frage untersucht, wozu es überhaupt Datenschutz gibt. Anschließend werden Einflussfaktoren auf das Vertrauen von Konsumenten im traditionellen Handel und Internet beleuchtet. Ein weiterer Punkt sind die rechtlichen Rahmenbedingungen und abschließend werden die datenschutzfreundlichen Technologien, die dem Benutzer teilweise automatisiert helfen sollen, ihre Daten bestmöglich zu schützen oder nur diejenigen freizugeben, die sie selbst bestimmt haben, vorgestellt.

2.1. Definition von Privatsphäre und Datenschutz

Gemäß Fischer-Hübner (2001) stammte die erste Definition zu Privatsphäre („privacy“) von Samuel D. Warren und Louis D. Brandeis in ihrem berühmten Artikel „The Right to Privacy“, welcher im Harvard Law Review erschien [Warren & Brandeis, 1890 In: Fischer-Hübner, 2001, S. 5]. Die beiden amerikanischen Anwälte definierten Privatsphäre als „the right to be alone“, also als das Recht in Ruhe gelassen zu werden. Die Veröffentlichung des Artikels kann auf die Entwicklung neuer Technologieformen, die mit weiteren Errungenschaften einhergingen, zurückgeführt werden. Vor allem wurde von den Autoren die Fotografie der Sensationspresse („yellow press“) als Angriff auf die Privatsphäre, im Sinne vom Recht in Ruhe gelassen zu werden, kritisiert [Fischer-Hübner, 2001, S. 5f].

Als allgemein gebräuchliche Definition für Privatsphäre ("privacy") gilt jene von Alan Westin: *„Privacy is the claim of individuals, groups and institutions to determine for themselves, when, who and to what extent information about them is communicated to others"* [Westin, 1967 In: Fischer-Hübner, 2001, S. 6].

Gemäß der Definition von Alan Westin haben sowohl natürliche als auch juristische Personen ein Recht auf Privatsphäre. In vielen Ländern, wie beispielsweise in Deutschland, USA und Großbritannien gibt es keine rechtliche Verankerung für die Privatsphäre von juristischen Personen, während es in Ländern wie Frankreich, Österreich oder Dänemark einen derartigen Schutz gibt [Fischer-Hübner, 2001, S. 6].

Persönliche Daten sind jegliche Informationen die mit einer Person, über persönliche oder materielle Gegebenheiten, in Verbindung gebracht werden können. Unter Datenschutz versteht man den Schutz von persönlichen Daten, um die Privatsphäre zu garantieren und dieser ist somit ein Teil des Konzepts (der Privatsphäre). Problematisch an diesem Konzept ist, dass die Privatsphäre nie 100%ig garantiert werden kann, da oft Konflikte mit anderen Rechten oder legitimen Werten entstehen können und des Weiteren auch deshalb, weil Individuen durch jede Teilnahme an der Gesellschaft oder generell im sozialen Umfeld persönliche Daten preisgeben. Die Gesetzgebung muss, um die Privatsphäre schützen zu können, jedes Mal eingreifen, sobald persönliche Daten gesammelt, abgespeichert oder verarbeitet werden [Fischer-Hübner, 2001, S. 6].

2.2. Wozu Datenschutz?

Berechtigterweise kann gefragt werden wozu Datenschutz überhaupt nötig ist. Durch die Verbreitung des Computers als Werkzeug, um Daten digital zu verwalten und mit der Verbreitung des Internets in den neunziger Jahren des 20. Jahrhunderts, ist es immer leichter für Unternehmen und andere Subjekte geworden, an Daten von Personen heranzukommen. Schon im Jahre 1597[1] soll Francis Bacon gesagt haben „Wissen ist Macht". Er meinte damit damals wohl eher, dass das Wissen dem Menschen Macht über die Natur verschafft, aber dieses Zitat behält seine Richtigkeit auch im Kontext von personenbezogenen Daten. Dieses Wissen findet sich als In-

[1] Die Jahreszahl stammt von der Wikipedia-Seite über Francis Bacon. Datum und Uhrzeit der Abfrage: 04. Dez. 2007 20:30. http://de.wikipedia.org/wiki/Francis_Bacon

formationen beziehungsweise als Daten über natürliche Personen in einer Vielzahl von Datenbanken und in manuell geführten Karteien wieder, diese werden gespeichert, miteinander verknüpft und mittels Analysetools Abfragen durchgeführt, die als „Machtmittel über Menschen“ ausgewertet werden können. In Österreich gilt derzeit das Datenschutzgesetz 2000 (siehe Kapitel 2.4.1 auf Seite 26) und als Umsetzung mehrerer EU-Richtlinien das Telekommunikationsgesetz 2003 (siehe Kapitel 2.4.4 auf S.32) um das Grundrecht auf Datenschutz zu wahren [Dohr, S. 2]. Dohr (o.J.) sieht dabei aber den Datenschutz nicht nur an juristische Vorgaben gebunden, sondern betrachtet den Datenschutz auch aus der ökonomischen Sicht. Er zählt Information als neuen Produktionsfaktor zu Kapital, Arbeit und Boden. Diese, als „klassisch“ bezeichneten, Produktionsfaktoren unterliegen unterschiedlichen Regelungen und Gesetzen, um die Nutzung zu gestalten und in einer sozial akzeptablen Weise zu erhalten. Weshalb es dann als natürlich anzusehen ist, dass Informationen, als neue Produktionsfaktoren, auch mit Hilfe von Gesetzen zu regeln sind [Dohr, S. 2].

Des Weiteren liegt der Fokus von Unternehmen darauf, durch eine gesetzeskonforme Behandlung von Daten jeglicher Art (siehe dazu für nähere Informationen Kapitel 2.4.1 auf Seite 26), Verwaltungsstrafen und Schadenersatzforderungen zu vermeiden. Zusätzlich können Verfahren aufgrund von Datenschutzverletzungen oder Äußerungen von Geschädigten sehr schnell an die Medien gelangen und die empfindliche Reputation von Unternehmen angreifen, wie man Ende März 2008 am Beispiel von Lidl in Deutschland verfolgen konnte[2]. Durch transparente Datenschutzrichtlinien kann für MitarbeiterInnen und Kunden/Innen eine Transparenz im Bezug auf die Datenverarbeitung geschaffen werden, wodurch eine Atmosphäre von Sicherheit und Zufriedenheit geschaffen werden kann [Pommerening, 2004].

[2] Der Firma Lidl (Deutschland) wurde von einer Ex-Mitarbeiterin einer Überwachungsfirma vorgeworfen, dass ohne Information und Einverständnis seitens der MitarbeiterInnen Kameras im gesamten Geschäft und vor allem im Kassenbereich zur Überwachung installiert wurden. Des Weiteren konnte auf den Videoaufnahmen auch der PIN-Code von Kunden/Innen eingesehen werden, wenn sie mit einer EC-Karte gezahlt haben. Zusätzlich wurden Protokolle über private Gespräche, Verhaltens- und Arbeitsweisen der Lidl-Angestellten verfasst
(vgl. http://www.spiegel.de/wirtschaft/0,1518,543431,00.html Datum und Uhrzeit der Abfrage: 22.04.2008 14:33).

Resümee

Zusammenfassend kann gesagt werden, dass ein erhöhter Anspruch an den Datenschutz daraus resultiert, dass die Digitalisierung Personen für Unternehmen oder andere Subjekte transparenter werden lassen. Da mit Hilfe von Analysetools und Verknüpfungen mehrerer Datenbanken, in denen unterschiedlichste persönliche Daten gespeichert wurden, machtvolle Abfragen gestartet werden können deren Umfang in Detailliertheit weit über jener der Einzelquellen liegt. Informationen können als moderner Produktionsfaktor angesehen werden, welcher, so wie die traditionellen, auch bestimmten Restriktionen unterworfen werden müssen, um die Privatsphäre der Betroffenen zu gewährleisten. Weitere Ansprüche an Datenschutz stammen aus gesellschaftspolitischer und ökonomischer Sicht, da diese weitestgehend Einfluss auf Reputation und wirtschaftliche Wettbewerbsfähigkeit der Unternehmen hat. Als weitere Gründe, die für Datenschutz sprechen, kann man das Vertrauen der Kunden und rechtliche Rahmenbedingungen nennen. Auf diese Punkte wird in den Kapiteln 2.3 und 2.4 näher eingegangen.

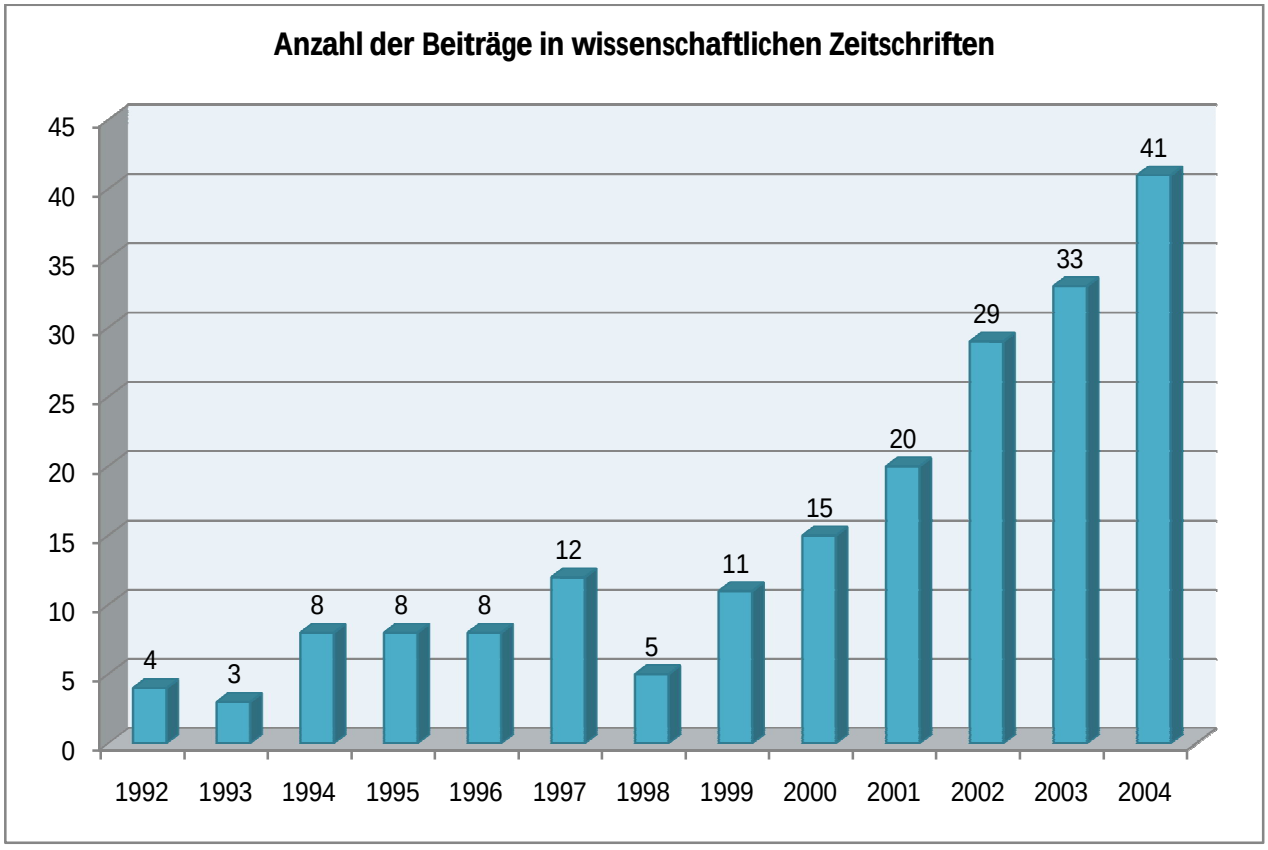
2.3. Konsumentenvertrauen im Internet

Wie unter 2.2 bereits erwähnt kann das Vertrauen der Kunden auch als Grund für einen aktiven Datenschutz sprechen. Nachfolgend wird deshalb auf den Begriff Vertrauen näher eingegangen und eine Definition für diese Arbeit festgelegt. Kapitel 2.3.2 beschäftigt sich dann mit der Besonderheit des Vertrauensbegriffs im E-Commerce.

2.3.1. Allgemeiner Vertrauensbegriff

Seit einigen Jahren hat sich Vertrauen als ein Trendthema der Sozialwissenschaften etabliert. Der Begriff selbst besitzt jedoch eine lange Tradition und wurde erstmals von Simmel (1908) aufgegriffen. Vor allem im Marketingbereich wurde in den letzten fünf bis zehn Jahren sehr viel zu diesem Thema geforscht und publiziert. Das erhöhte Interesse an Vertrauen ist vor allem auf die Erkenntnis, dass Vertrauen Beziehungen aufrechterhalten kann, zurückzuführen. Diese internationale Entwicklung wird in Abbildung 1 grafisch dargestellt [Kenning & Blut, 2006, S. 4f].

Abbildung 1: Entwicklung der wissenschaftlichen Publikationen zum Thema "Vertrauen" im Bereich Marketing



Quelle: Eigene Darstellung in Anlehnung an [Kenning & Blut, 2006, S.5]

Vertrauen wird in den Wirtschaftswissenschaften aus gesamt- und einzelwirtschaftlicher Perspektive analysiert. Mit den Auswirkungen von Vertrauen auf ökonomische Größen (zum Beispiel Wirtschaftswachstum, Einkommen, etc.) beschäftigt sich die gesamtwirtschaftlich orientierte Forschung. Bei der einzelwirtschaftlichen Perspektive können vier große Forschungsbereiche bestimmt werden [Kenning & Blut, 2006, S. 5].

- *Interpersonell*: Hierbei wird vor allem das Vertrauen zwischen Individuen erforscht. Vertrauen wird als Erwartung darauf definiert, dass der Vertrauensnehmer seine Stellung nicht zum Nachteil des Vertrauensgebers ausnutzt [Kenning & Blut, 2006, S. 5].
- *Interorganisational*: In diesem Bereich wird Vertrauen als Ehrlichkeit in Kooperationen zwischen zwei Organisationen verstanden [Kenning & Blut, 2006, S. 5].
- *Intraorganisational*: Intraorganisationale Forschung beschäftigt sich mit Vertrauen innerhalb einer Organisation zum Beispiel zwischen Mitarbeiter und Vorgesetzten [Kenning & Blut, 2006, S. 5f].
- *Technologiebezogen*: Dies ist der jüngste Bereich der Vertrauensforschung, welcher sich mit dem Einfluss von Technologien (vor allem des Internets) auf das Vertrauen zwischen Subjekten und Objekten in unterschiedlichen Kontexten beschäftigt [Kenning & Blut, 2006, S. 6].

In der Literatur herrscht eine Vielzahl an Definitionen zu dem Begriff Vertrauen, welche aber kaum Übereinstimmungen aufweisen. Diese Uneinigkeit bei der Begriffsdefinition wird des Weiteren durch Artikel aus der Soziologie, Psychologie, Ökonomie, Anthropologie und Philosophie vermehrt [Osterloh & Weibel, 2006, S. 35]. Weitere Einflüsse stammen auch aus dem Relationship-Management-Ansatz. Dieser Ansatz richtet seinen Fokus auf die Beziehung zwischen der Organisation und deren Kunden, um durch Vertrauen eine nachhaltig stabile und auf Dauer ausgerichtete Beziehung aufzubauen [Kenning & Blut, 2006, S. 6]. An dieser Stelle sollen einige Definitionen zu Vertrauen, ohne einen Anspruch auf Vollzähligkeit zu erheben, angeführt werden:

Zand (1997) liefert diese Definition: „Vertrauen besteht aus der Bereitschaft deine Verwundbarkeit gegenüber einer anderen Person zu erhöhen, deren Verhalten du nicht kontrollieren kannst, in einer Situation, in der dein potenzieller Vorteil viel geringer ist als dein potenzieller Verlust, falls die andere Person deine Verwundbarkeit ausnutzt“ [Neuberger, 2006, S. 14].

„Vertrauen ist die Erwartung, dass ein Interaktionspartner wohlwollendes Verhalten zeigen wird, obwohl dieser die Möglichkeit hat andere, nicht wohlwollende Verhaltensweisen zu wählen“ [Koller, 1990, S. 1 in Neuberger, 2006, S. 14].

Zündorf (1982) definiert Vertrauen als „… die freiwillige Übertragung der Kontrolle über Ressourcen, Handlungen oder Ereignisse in Erwartung einer nicht genau im voraus festgelegten Gegenleistung in einer nicht genau terminierten Zukunft“ [Neuberger, 2006, S. 14].

Noteboom (2002) sieht Vertrauen in einer engen Definition wie folgt: „‘Real‘ trust, or trust in the strong sense, is an expectation that things or people will not fail us, or the neglect or lack of awareness of the possibility of failure, even if there are perceived opportunities and incentives for it“ [Neuberger, 2006, S. 14].

Coleman (1990) stellt folgende Bedingung auf, damit von Vertrauen gesprochen werden kann: $p*G > (1-p)*V$ wobei G der mögliche Gewinn ist, V der mögliche Verlust, p ist die Gewinnchance, wenn der Interaktionspartner vertrauenswürdig ist, (1-p) ist die Verlustchance bei Vertrauensbruch. Er leitet daraus ab: „The elements confronting the potential trustor are nothing more or less than the considerations a rational actor applies in deciding whether to place a bet“ [Neuberger, 2006, S. 15].

Osterloh und Weibel (2006) definieren als Kern der unzähligen Definitionen: „Vertrauen ist der Wille, sich verletzlich zu zeigen“ [Osterloh & Weibel, 2006, S. 35]. Aus diesem Zitat schließen die Autorinnen auf die Vertrauensdimensionen Verletzlichkeit, Vertrauenssprung und positive Erwartung. Die Dimension Verletzlichkeit ergibt sich daraus, dass die Person die vertraut ein gewisses Risiko eingeht einen Schaden zu erleiden. Luhmann (1989) sieht Vertrauen als eine riskante Vorleistung an und bringt genau wie Osterloh & Weibel (2006) die Dimension Verletzlichkeit zum Vorschein.

Dies entsteht dadurch, dass der/die Vertrauende aus der Handlung entweder einen Gewinn oder Verlust erleiden kann, welcher aber vollständig vom Verhalten des Vertrauensnehmers abhängt. Interessant bei dieser Interaktion ist vor allem, dass der Verlust für den/die Vertrauenden immer größer ist als der Gewinn. Der Vertrauenssprung entsteht aus der Tatsache, dass der/die Vertrauende in Handlungen die eigene Verletzlichkeit gefährdet. Das bedeutet, Vertrauen erfordert immer ein gewisses Maß an Wagnis. Dabei ist aber zu beachten, dass der Vertrauensgeber den Vertrauenssprung machen muss, um zu zeigen, dass er verletzlich ist und somit ein „Vertrauensgeschenk“ an den Anderen weitergibt. Die positive Erwartung ist der Grund dafür, dass der Vertrauende sich sozusagen „ausliefert“ und vom Vertrauensnehmer nur Gutes erwartet. Der Vertrauensgeber ist nur dann dazu bereit seinen Vertrauenssprung zu wagen, wenn er den/die Andere so einschätzt, dass er/Sie ihm/ihr nicht schaden will [Osterloh & Weibel, 2006, S. 35ff]. Der Ansatz von Luhmann (1989) ist zwar bereits fast 20 Jahre alt, aber besitzt bis heute passende inhaltliche Aspekte, weshalb dieser Ansatz auch für die Definition des Vertrauensbegriffs für diese Arbeit übernommen wird.

Weiters soll erwähnt werden, dass die Konstrukte Kundenzufriedenheit, Commitment und Vertrauen Einfluss auf die Kundenbindung beziehungsweise Beziehungsqualität nehmen. Auf die beiden ersteren soll in dieser Arbeit aber nicht näher eingegangen werden. Erwähnenswert ist, dass diese Konstrukte gewissermaßen voneinander abhängig sind, obwohl sie unterschiedliche zeitliche Elemente besitzen. Beispielsweise übt die Kundenzufriedenheit, als vergangenheitsorientierte Komponente, Einfluss auf die zukünftige Kundenbindung aus, da als Ergebnis hoher Zufriedenheit der Kunde beziehungsweise die Kundin wieder einkaufen wird. Die Zufriedenheit wirkt sich des Weiteren auch auf Vertrauen und Commitment aus. Wenn ein Kunde zufrieden mit seinen Einkäufen bei einem bestimmten Verkäufer war, erhöht sich somit das Vertrauen darauf, dass zukünftig die Leistungen genauso sein werden. Zufriedenheit bewirkt gleichzeitig auch eine Bindung des Kunden zum Anbieter, woraus Commitment entsteht [Bornemann, Hennig-Thurau, & Hansen, 2006, S. 329].

2.3.2. Besonderheit des Vertrauensbegriffs im E-Commerce

Zuerst stellt sich die Frage warum es einer anderen Definition des Begriffs Vertrauen im Bezug auf den Internethandel (E-Commerce) im Vergleich zum traditionellen Handel bedarf. Dies hängt von mehreren Faktoren ab, die sich schon allein durch die geänderten Bedingungen beim Kauf via Internet ergeben. Zuerst können die technischen Möglichkeiten des internetbasierten Kaufs genannt werden, wodurch eine andere Beziehung zwischen den Teilnehmern am Markt entsteht. Anstatt der üblichen one-to-one oder one-to-many Kommunikation, gibt es bei diesem Medium keine traditionellen Regeln. Aufgrund der Interaktivität ist zugleich eine Massenkommunikation möglich, die im traditionellen Bereich auf persönliche Kommunikation beschränkt ist. Des Weiteren weißt die Kommunikation die Faktoren Echtzeit und Multimedialität auf. Eine Schwachstelle des Internets ist das große Maß an Anonymität, welche bei der traditionellen Beziehung durch den persönlichen Kontakt zwischen Kunden und Verkäufer gar nicht möglich ist. Die Marktsituation im Internet besitzt kaum bis gar keine Wechselbarrieren für den Kunden, da ohne größere Bemühungen ein neuer Anbieter ausgewählt werden kann [Bornemann, Hennig-Thurau, & Hansen, 2006, S. 327].

Wodurch entsteht beim Online-Kauf nun das Risiko des Käufers? Das wahrgenommene Risiko besteht aus zwei multiplikativ verknüpften Komponenten, aus den „negativen Kauffolgen“ und der „wahrgenommenen Unsicherheit“. Unter negativen Kauffolgen kann das finanzielle Risiko (zum Beispiel Missbrauch der Kontoinformationen), funktionales oder leistungsbezogenes Risiko, Sicherheitsrisiko (zum Beispiel Datensicherheit), psychologisches Risiko (zum Beispiel Datenschutzprobleme aufgrund der Datenübermittlung) oder Risiko des Zeit- oder Bequemlichkeitsverlusts (zum Beispiel Reklamation, fehlende Usability) zusammengefasst werden. Die Risikowahrnehmung beim Online-Kauf ist des Weiteren auch durch Eigenschaften des Internets wie beispielsweise Technikdominanz, Neuartigkeit, Komplexität oder Sicherheitsproblemen bei der Übertragung von Daten verstärkt, darüber hinaus ist auch, wie bereits weiter oben erwähnt, der fehlende direkte beziehungsweise persönliche Kontakt zwischen Käufer und Verkäufer nicht zu unterschätzen. Die soeben genannten Eigenschaften wirken sich positiv auf die Kaufunsicherheit aus. Als zentrales Kaufhemmnis kann die erhöhte Unsicherheit zu einer gesteigerten Risikowahrnehmung führen [Weiber & Egner-Duppich, 2006, S. 343].

Die soeben festgelegten Kaufunsicherheiten konnten durch eine Studie aus dem Jahre 2005, die von der Postbank in Zusammenarbeit mit dem Europressedienst durchgeführt wurde, aufgezeigt werden. Dabei ergab sich, dass in Deutschland das Internet und der elektronische Handel immer mehr genutzt werden, aber gleichzeitig das Vertrauen in den elektronischen Handel ziemlich gering ausfällt. Die Studie ergab, dass 77,3% der Deutschen einen ihnen unbekannten Shop nur bedingt vertrauen, ist die Art der Bezahlung unbekannt haben 75,5% Bedenken und im Zuge dessen brechen 75,2% den gesamten Kaufvorgang ab. Die Studie ergab des Weiteren, dass die Unsicherheit sich zwar mit positiven Einkäufen verringert, aber andererseits konnte ermittelt werden, dass sogar für Personen die regelmäßig online einkaufen, dies immer mit einem erhöhten Maß an Angst beziehungsweise Skepsis verbunden ist. Überraschend ist, dass gesetzliche Regelungen, Aufrüstung der technologischen Sicherheit und die Schaffung von Vertrauensmaßnahmen wie beispielsweise Gütesiegel kaum bis keine Änderungen diesbezüglich schaffen können [Weiber & Egner-Duppich, 2006, S. 342].

Zukünftig werden Unternehmen, die sich ungenügend oder unprofessionell im Internet repräsentieren, nicht in die Perzeption der Kunden gelangen können. Der Online-Kauf wird maßgeblich das Einkaufsverhalten von Konsumenten beeinflussen. Der zentrale Erfolgsfaktor für Unternehmen im Internethandel wird das Vertrauen sein, da weiterhin eine hohe Unsicherheit beim Online-Kauf vorhanden ist. Vertrauen wird als Merkmal zur Differenzierung im Konkurrenzkampf mehr an Bedeutung gewinnen. Wichtig hierbei ist für Unternehmen die Einflussgrößen des Kundenvertrauens zu ermitteln und gezielt zu beeinflussen, um das Vertrauen der Kunden selbst zu forcieren [Weiber & Egner-Duppich, 2006, S. 342].

Beim Online-Kauf können fünf Vertrauensdeterminanten, welche jede eine unterschiedliche Wirkung auf die Kaufentscheidung hat, nachgewiesen werden [Weiber & Egner-Duppich, 2006, S. 346f]:

Als erste Determinante gilt die *Reputation* des Online-Anbieters. Diese findet vor allem dann ihre Funktion, wenn es nicht möglich ist, Informationen über die Leistungen des Anbieters nachprüfbar zu ermitteln oder wenn die Qualität eines Online-Handels nicht eruiert werden kann. Die Reputation eines Anbieters liefert Informationen über

Eigenschaften wie beispielsweise Kompetenz, Glaubwürdigkeit oder Ehrlichkeit. Anhand dieser Informationen kann der Konsument das voraussichtliche Verhalten im Vorhinein abschätzen. Je besser die Reputation, umso größer ist die Wahrscheinlichkeit, dass der Kunde dem jeweiligen Gegenüber sein Vertrauen schenkt. Bei Wiederholungskäufern spielt die Reputation eine untergeordnete Rolle, da diese, im Gegensatz zu Erstkäufern bei denen die Reputation eine wichtige Kaufentscheidung darstellt, auf eigene Erfahrungen mit dem Anbieter zurückgreifen können, [Weiber & Egner-Duppich, 2006, S. 347].

Die zweite Determinante ist der *Erste Eindruck*. Beim Online-Kauf kann der Kunde sich nicht durch visuelle Begutachtung des Geschäftslokals oder des Verkaufspersonals beziehungsweise der Person des Anbieters einen ersten Eindruck verschaffen. Da der Kaufprozess via Internet über ein unpersönliches Medium und durch eine asynchrone Kommunikation geprägt ist, kann sich der Kunde nur über die Webseite des Anbieters einen Eindruck über dessen Vertrauenswürdigkeit machen. Fogg et al. (2002) stellten fest, dass eine positiv gestaltete Webseite mit der Entstehung von Vertrauen verbunden ist und Egger (2003) benennt diesen Sachverhalt als „Appeal“ (Anziehungskraft) der Internetpräsenz, wodurch die Vertrauensbildung positiv beeinflusst wird. Der erste Eindruck stellt neben der Reputation einen wichtigen Anhaltspunkt in der Phase der Anbahnung und des ersten Kontaktes dar. Entsteht dabei ein positiver Eindruck, wird der Kunde in die nächsten Phasen des Transaktionsprozesses übergehen, somit spielt diese Determinante eine äußerst wichtige Rolle im Anbahnungsprozess [Weiber & Egner-Duppich, 2006, S. 347f].

Die nächste Determinante ist der *wahrgenommene Informationsgehalt* der Anbieter-Webseite. Der wahrgenommene Informationsgehalt der vom Anbieter bereitgestellten Informationen trägt maßgeblich zur Vertrauensbildung und Reduktion des wahrgenommenen Risikos bei. Dabei gibt der Anbieter Informationen über sich selbst, Produkte und Leistungen, den Transaktionsprozess, den Schutz der persönlichen Kundendaten und der Privatsphäre, sowie Datensicherheit etc. preis. Diese Informationen sollen den Kunden zum Kauf motivieren und Vertrauensmängel, die durch fehlende Informationen entstehen, reduzieren. Umso mehr vertrauensrelevante Informationen angeboten werden, umso einfacher ist die Vertrauensbildung [Weiber & Egner-Duppich, 2006, S. 348].

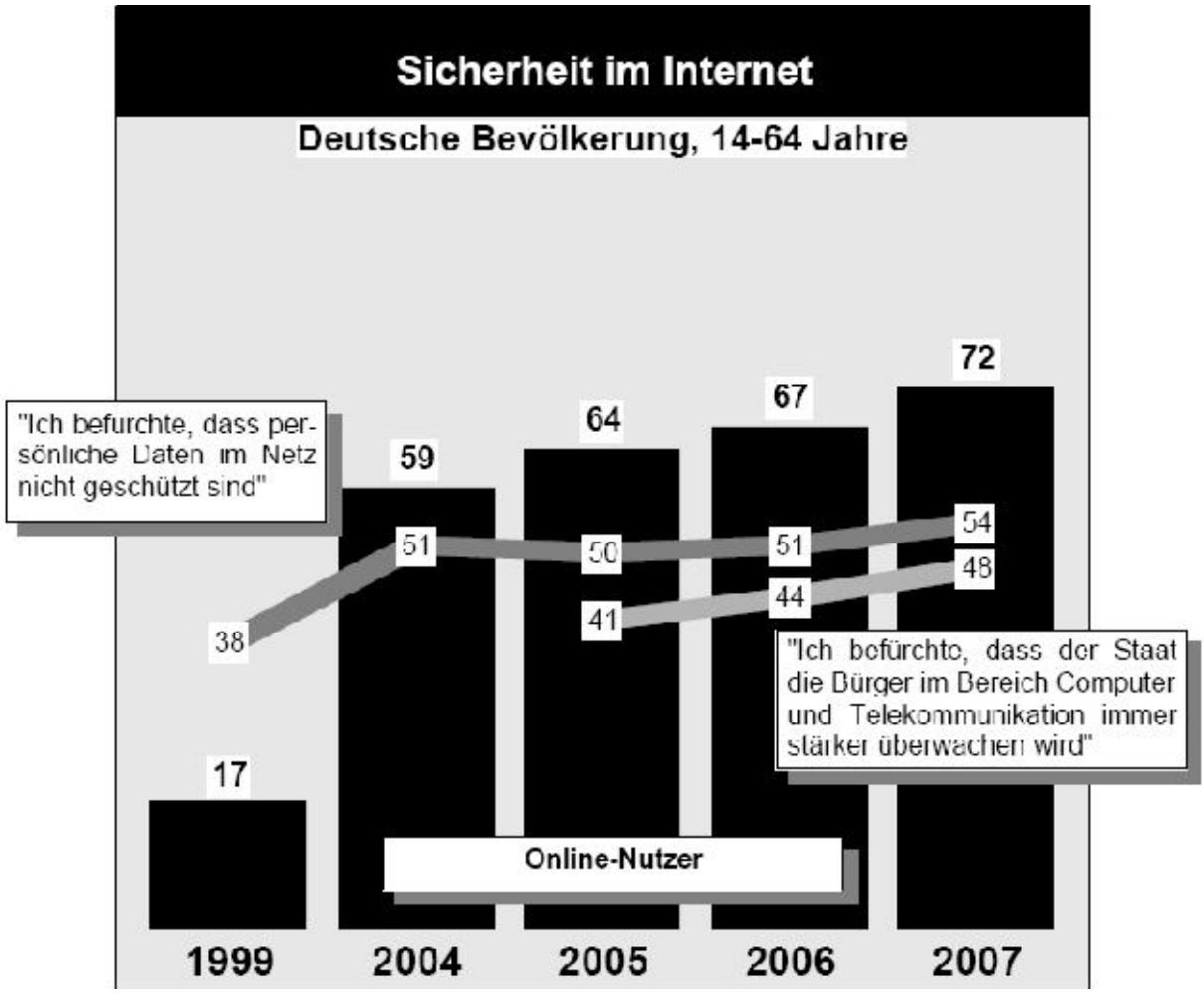
Als vierte Determinante ist die *Usability* (Benutzerfreundlichkeit) der Webseite und des Bestellsystems zu nennen. Die Usability spielt vor allem in der Phase des Kaufprozesses eine entscheidende Rolle, wobei Vertrauenserwartungen seitens des Kunden in den Anbieter entstehen. Dabei zählen zur Usability nicht nur das allgemeine Erscheinungsbild und das Design, sondern vor allem auch die Funktionalität und die technische Umsetzung des gesamten Prozesses beim Online-Kauf. Das Vertrauen in den Anbieter verschlechtert sich beispielsweise durch eine geringe Benutzerfreundlichkeit der Webseite beziehungsweise des Bestellsystems und durch unstrukturierte oder unübersichtliche Seiten [Weiber & Egner-Duppich, 2006, S. 348].

Die fünfte und letzte Determinante ist die *Interaktions- und Kommunikationsqualität*. Werden dem Kunden Kommunikationsmöglichkeiten, um mit dem Anbieter sowohl online als auch offline in Kontakt zu treten, angeboten, wird dies als Maß dafür wahrgenommen, dass der Kontakt beziehungsweise die Beziehung zum Kunden einen hohen Stellenwert geniest. Zu beachten dabei ist aber, dass nicht nur die Interaktionsmöglichkeiten zur Verfügung gestellt werden, sondern das auch die Interaktionen mit dem Kunden qualitativ hochwertig sind. Eine besonders hohe Wirkung auf die Bildung von Vertrauen hat die Kommunikationsmöglichkeit während und nach dem Kaufprozess, da der Kunde nach der Kaufabwicklung keinen Einfluss auf die Transaktion mehr nehmen kann. Insbesondere wenn beispielsweise Tools zur Auslieferungskontrolle beziehungsweise Erfüllung des Vertrags (zum Beispiel Tracking, Lieferqualität, Pünktlichkeit) angeboten werden, kann dies die Vertrauensgewinnung positiv forcieren [Weiber & Egner-Duppich, 2006, S. 349].

Nachfolgend wird eine Anfang November 2007 durchgeführte Studie des Instituts für Demoskopie Allensbach mit dem Titel „Sicherheit im Netz?“ präsentiert. Dabei wurden 10.369 Personen aus Deutschland im Alter zwischen 14 und 64 Jahren befragt. Bei der Befragung zeigte sich, dass schon vor einigen Jahren, als noch wenige Personen über einen Internetanschluss verfügten, InternetnutzerInnen befürchteten, dass ihre persönlichen Daten wenig bis gar nicht geschützt seien. Heutzutage denkt jeder Zweite (54%) genauso und 48% befürchten, dass der Staat die BürgerInnen im Computer- und Telekommunikationsbereich immer mehr überwachen könnte. Diese Ergebnisse wurden in Abbildung 2 übersichtlich zusammengefasst, die schwarzen

Balken geben in Prozent an, wie viele Personen über einen Internetanschluss verfügen [ACTA, 2007, S. 5].

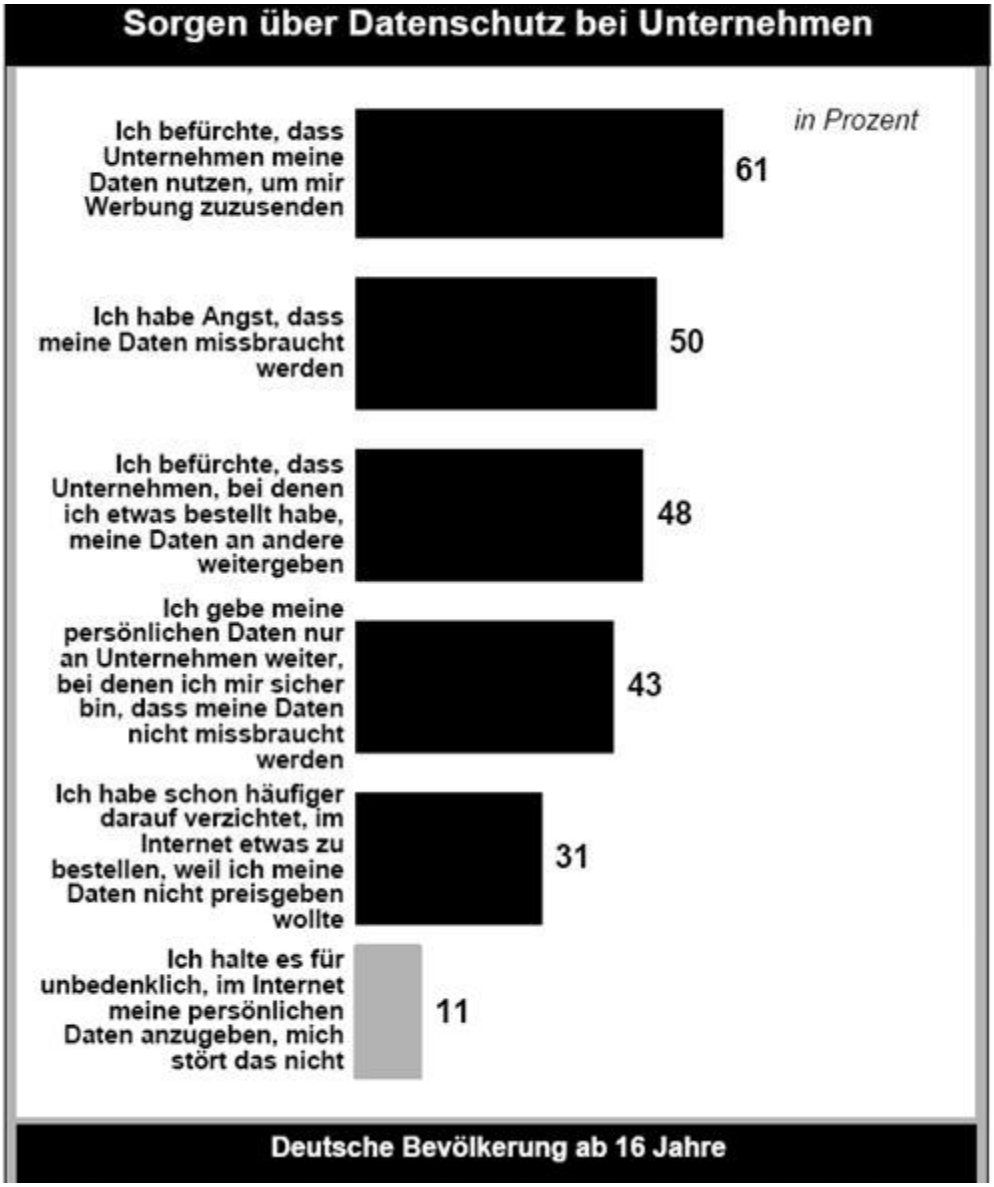
Abbildung 2: Sicherheitsbedenken von deutschen InternetnutzerInnen



Quelle: [ACTA, 2007, S. 2]

Gleichzeitig herrscht bei der deutschen Bevölkerung auch eine gewisse Besorgnis bezügliches des Datenschutzes in Unternehmen. Von den Befragten gaben 61% an, dass sie befürchten, wenn sie mit einem Unternehmen in Kontakt treten, danach unaufgeforderte Werbung erhalten und ganze 48% denken, dass ihre Daten an Andere weitergegeben werden. Jeder Zweite der Befragten gab an, Angst zu haben, dass die persönlichen Daten missbraucht werden könnten. Aufgrund dieser Bedenken hat schon in etwa jeder Dritte der Befragten (31%) nicht im Internet eingekauft. Lediglich jeder Zehnte (11%) hält es für unbedenklich im Internet seine Daten an Unternehmen zu übermitteln. Abbildung 3 fasst die Ergebnisse nochmals grafisch zusammen [ACTA, 2007, S. 2f].

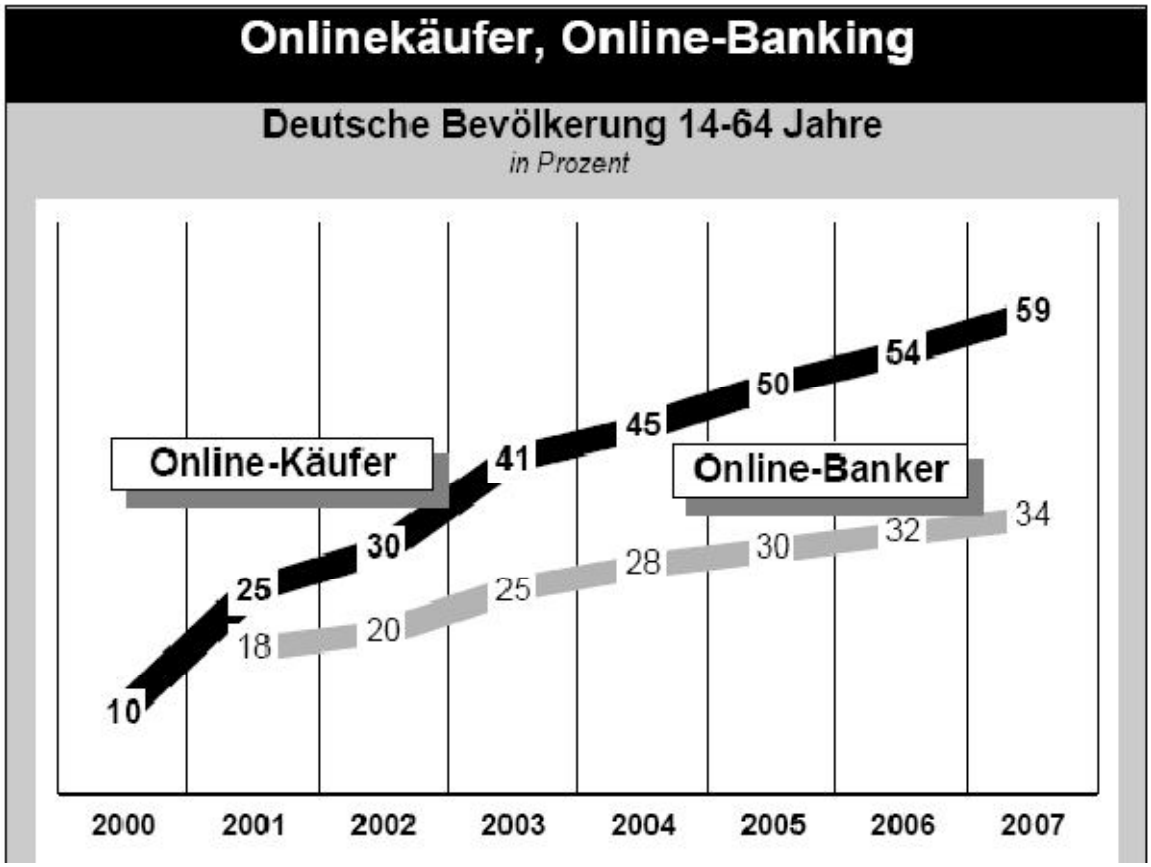
Abbildung 3: Sorgen über Datenschutz bei Unternehmen von deutschen InternetnutzerInnen



Quelle: [ACTA, 2007, S. 3]

Obwohl deutsche InternetnutzerInnen meist sehr große Bedenken beim Einkaufen im Internet bezüglich der Datensicherheit haben, hat sich die Anzahl der Personen die Online einkaufen von 10% im Jahr 2000 auf 59% im Jahr 2007 erhöht (siehe Abbildung 4). Die im Vergleich zum Online-Kauf langsamere Entwicklung des Online-Bankings ist daher nicht auf die Bedenken der InternetnutzerInnen bezüglich der fehlenden Datensicherheit zurückzuführen, sondern hängt wohl damit zusammen, dass es sich bisher nur bei einkommensstärkeren Personen durchsetzen konnte [ACTA, 2007, S. 4].

Abbildung 4: Anzahl der Online-Käufer und -Bänker in Deutschland in Prozent



Quelle: [ACTA, 2007, S. 4]

2.3.3. Resümee

Wie die beiden Studien der Postbank und des Institut Allensbach, die bereits im vorigen Kapitel präsentiert wurden, aufzeigten, sind die InternetnutzerInnen, trotz erhöhter Anzahl an Online-Käufen, nach wie vor skeptisch wenn sie über das Internet ihre Käufe tätigen. Von den Befragten hat sich die prozentuelle Anzahl der Personen, die von 2000 bis 2007 Online-Käufe tätigten, fast versechsfacht (von 10% auf 59%). Dabei zeigt sich erneut das große Potenzial für Unternehmen ihre Umsätze über Online-Verkäufe zu erhöhen. Das Vertrauen beziehungsweise die Vertrauensbildung des Kunden in den Anbieter spielt eine extrem große Rolle im Vergleich zum traditionellen Handel. Dabei sollten Unternehmen ihren Fokus auf die Determinanten Reputation, erster Eindruck, Informationsgehalt, Usability und Kommunikationsqualität legen, um das Vertrauen ihre Kunden nachhaltig positiv beeinflussen zu können und sich im Konkurrenzkampf durchzusetzen.

2.4. Rechtliche Grundlagen

In der europäischen Union wird der Datenschutz in Artikel 6 des EU-Vertrags, Artikel 286 des EG-Vertrags, Artikel 8 der Grundrechtcharta der EU, Richtlinie 95/46/EG und Richtlinie 2002/58/EG geregelt. Somit ist der Schutz personenbezogener Daten in der ganzen EU ein Grundrecht auf das sich jeder EU-Bürger berufen kann. Des Weiteren müssen die Organe und Einrichtungen der EU dem Grundsatz des Datenschutzes gemäß der Verordnung (EG) Nr. 45/2001 gewährleisten [EDPS].

In den drei nachfolgenden Kapiteln (2.4.1; 2.4.2 und 2.4.4) wird auf die momentane Rechtslage in Österreich und auf Sonderfälle des Datenschutzes im Internet eingegangen. In Kapitel 2.4.6 folgt ein umfassendes Resümee zum Datenschutzrecht.

2.4.1. Das Datenschutzgesetz 2000

In Österreich gilt derzeit, als Umsetzung der EG-Datenschutzrichtlinie, das „Datenschutzgesetz 2000 (DSG 2000), BGBl. I Nr. 165/1999“ welches am 01.01.2000 in Kraft getreten ist [Datenschutzkommission]. Des Weiteren gibt es noch das Telekommunikationsgesetz 2003, welches als „sektorspezifische datenschutzrechtliche Regelung“ für Provider gilt [Janisch & Mader, 2006, S. 32].

Nachfolgend werden Begriffe im Sinne des DSG 2000 definiert:

- *Auftraggeber*: Als Auftraggeber gemäß § 4 Ziffer 4 DSG gelten jede natürliche oder juristische Person, beziehungsweise Personengemeinschaft sowie Organe einer Körperschaft und die Geschäftsapparate dieser Organe die Daten für einen bestimmten Zweck verarbeiten, unabhängig davon ob sie dies selbst durchführen oder Dritte dazu heranziehen [Datenschutzkommission].
- *Betroffene/r*: Im Sinne des § 4 Z 3 DSG gilt als Betroffene/r „jede vom Auftraggeber verschiedene natürliche oder juristische Person oder Personengemeinschaft, deren Daten verwendet werden“ [Datenschutzkommission]. Der Begriff wurde durch die Vorgaben der Richtlinie 95/46/EG erweitert, da das DSG 1978 nur den Schutz von personenbezogenen Daten *natürlicher* Personen vorsah [Graf, 2004, S. 40].
- *Personenbezogene Daten*: Gemäß § 4 Z 1 DSG sind dies Angaben über Personen deren Identität bestimmt oder bestimmbar ist [Datenschutzkommission]. Jahnel et. al. (2007) verstehen unter personenbezogenen Daten nicht nur An-

gaben wie Name, Geschlecht, Adresse etc. einer Person, sondern auch personenbezogene Informationen wie zum Beispiel Werturteile.

- *Sensible Daten*: § 4 Z 2 DSG definiert sensible Daten als Angaben über Personen bezüglich ihrer ethnischen Herkunft, politischen Meinung, Gewerkschaftszugehörigkeit, Gesundheit, Sexualleben usw. [Datenschutzkommission; Janisch & Mader, 2006, S. 32].
- *Datei*: § 4 Z 6 DSG definiert eine Datei als eine „strukturierte Sammlung von Daten, die nach mindestens einem Suchkriterium zugänglich sind“ [Datenschutzkommission].
- *Datenanwendung*: Graf (2004) definiert Datenanwendung als „[…] die Summe der Verwendungsschritte, die zur Erreichung des Ergebnisses erfolgen.“
- *Verwenden von Daten*: Im Sinne des DSG 2000 versteht man unter „Verwenden von Daten“ (als einen Überbegriff für das Handhaben von Daten) das Verarbeiten und Übermitteln [Graf, 2004, S. 39].
- *Verarbeiten von Daten*: Mit „Verarbeiten“ ist jede mögliche Handhabung von Daten, mit Ausnahme der Übermittlung, gemeint. Graf (2004) zählt folgende Möglichkeiten auf: „ermitteln, erfassen, speichern, aufbewahren, ordnen, vergleichen, verändern, verknüpfen, vervielfältigen, abfragen, ausgeben, benützen, überlassen, sperren, löschen, vernichten“.
- *Zustimmung*: Unter einer Zustimmung im Sinne des DSG 2000 versteht man eine zwangsfreie Einwilligung des/r Betroffenen, in einem konkreten Fall bei der er/sie die Sachlage kennt und der Verarbeitung der Daten zustimmt [Graf, 2004, S. 40].

Das DSG 2000 gewährt in § 1 natürlichen sowie juristischen Personen und Personengemeinschaften das Grundrecht auf Geheimhaltung ihrer personenbezogenen Daten zur Achtung ihres Privat- und Familienlebens, insofern ein schutzwürdiges Interesse daran besteht [Datenschutzkommission; Janisch & Mader, 2006, S. 32]. Dabei ist unerheblich ob die Daten automationsunterstützt oder manuell verarbeitet werden (§ 1 Ziffer 3 DSG). Das heißt damit es zur Anwendbarkeit des DSG 2000 kommen kann, muss es sich um personenbezogene Daten handeln, deshalb fallen anonymisierte Daten nicht in den Geltungsbereich des DSG. Des Weiteren werden vom Gesetzgeber „sensible Daten“ (§ 4 Z 2 DSG) als besonders schutzwürdig erachtet (Definition siehe oben) [Datenschutzkommission; Janisch & Mader, 2006, S. 32].

Der räumliche Anwendungsbereich des DSG 2000 erstreckt sich auf jede Verwendung von Daten die in Österreich stattfindet. Verfügt der/die AuftraggeberIn über eine Niederlassung in einem EU-Mitgliedsstaat, wird das Recht des „Sitzstaates“ angewandt. Umgekehrt gilt das österreichische Datenschutzgesetz wenn es zu einer Datenverwendung in einem EU-Land kommt und dies für einen österreichischen Auftraggeber mit Haupt- oder Zweigniederlassung in Österreich geschieht. Kommt es zu einer Datenverarbeitung außerhalb der EU, gilt das Recht des Staates in dem die Verarbeitung stattfindet [Graf, 2004, S. 34].

Die §§ 26 ff DSG räumen den Betroffenen besondere Rechte ein, darunter fallen das Recht auf Auskunft (§ 26), Recht auf Richtigstellung und Löschung (§ 27), sowie § 28 Absatz 2 das Widerspruchsrecht des Betroffenen ohne Angabe von Gründen, wenn Daten aufgrund einer nicht gesetzlich bestimmten Erhebung in einer öffentlich zugänglichen Datei aufgenommen wurden [Datenschutzkommission; Jahnel, 2007, S. 24 und Janisch & Mader, 2006, S. 32]. Um den Rechtsschutz durchsetzen zu können, muss bei dem Auftraggeber unterschieden werden, ob er dem öffentlichen (zum Beispiel Gemeinden, Kammern) oder privaten Bereich zuzuordnen ist. Handelt es sich beim Auftraggeber, um eine öffentliche Behörde, dann ist die Datenschutzkommission (DSK) im Falle von Verletzungen der Rechte (siehe oben) des Betroffenen zuständig. Ist der Auftraggeber aus dem privaten Bereich, kann der/die Betroffene beim zuständigen Landgericht seine/ihre Rechte geltend machen. Handelt es sich jedoch um Verletzungen des Rechts auf Auskunft ist immer die Datenschutzkommission dafür zuständig [Janisch & Mader, 2006, S. 33].

Für jede Datenverarbeitung im Sinne des DSG 2000 gilt eine zweistufige Zulässigkeitsprüfung. Zuerst muss der Zweck, welcher der Verarbeitung der Daten zugrunde liegt, untersucht werden. Danach wird geprüft ob schutzwürdige Interessen zur Geheimhaltung eventuell verletzt werden können, wobei wiederum zwischen sensiblen und nicht-sensiblen Daten unterschieden wird. Zuletzt wird die Verhältnismäßigkeit geprüft, das heißt ob ein gewisses Maß beim Eingriff in die Privatsphäre nicht überschritten wird und des Weiteren ob „gelinde Mittel“ eingesetzt werden. Allgemein kann von einem Verbotsprinzip des DSG 2000 ausgegangen werden. Sollte die Zulässigkeitsprüfung negativ ausfallen, ist die Verwendung der

personenbezogenen Daten unzulässig [Graf, 2004, S. 41ff.]. Die nachfolgende Abbildung 5 zeigt das Schema für die Zulässigkeitsprüfung.

Abbildung 5: Schema für die Überprüfung der Zulässigkeit der Datenverwendung

Quelle: [Graf, 2004, S. 42]

Grundsätzlich gilt, dass jede Verwendung von Daten der Meldepflicht an das Datenverarbeitungsregister (DVR) unterliegt. Ausgenommen von dieser Regelung sind zum Beispiel Datenanwendungen die allgemein veröffentliche Daten oder indirekt personenbezogene Daten, die dazu dienen gesetzlich bestimmte Register oder Verzeichnisse zu führen, verwenden [Janisch & Mader, 2006, S. 33]. Für die Übermittlung von Daten mit Auslandsbezug wird eine Bewilligung der Datenschutzkommission benötigt. Ausgenommen davon sind lt. § 12 Absatz 1 DSG 2000 der Verkehr von

Daten innerhalb der EU. Dennoch muss die Übermittlung der Daten an das Ausland immer der Rechtmäßigkeitsüberprüfung des § 7 DSG 2000 standhalten. Besteht die Pflicht für den Auftraggeber eine Bewilligung einzuholen, so muss er/sie dies vor der Übermittlung oder Überlassung der Daten an das Ausland tun [Graf, 2004, S. 49].

Werden Daten ohne Meldung beim Datenverarbeitungsregister verarbeitet, können Verwaltungsstrafen in der Höhe von maximal 18.894,93 Euro ausgesprochen werden. Gab es bei einer Datenverwendung zusätzlich eine Gewinn- oder Schädigungsabsicht kann eine Freiheitsstrafe von bis zu einem Jahr verhängt werden [Dohr, S. 5].

2.4.2. Die Datenschutzrichtlinie 95/46/EG der EU

Das Europäische Parlament und der Rat verabschiedeten die Richtlinie 95/46/EG „zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten und zum freien Datenverkehr“ am 24. Oktober 1995 [Graf, 2004, S. 13]. Ziel dieser Richtlinie ist, vor allem den Verkehr von personenbezogenen Daten in der EU ohne Hinderungen und einen möglichst einheitlichen und hohen Schutz zu ermöglichen. Durch diese Mindeststandards an Schutz bei der Verarbeitung von personenbezogenen Daten sollen Verzerrungen des Wettbewerbs und Risiken einer Verlagerung des Standorts minimiert werden. Gleichzeitig müssen bei dem Austausch von Informationen innerhalb der EU die Grundrechte der BürgerInnen gewahrt werden. Dazu zählt zum Beispiel das Recht auf Privatsphäre welches in Art. 8 der Europäischen Konvention zum Schutze der Menschenrechte und Grundfreiheiten anerkannt wurde [Graf, 2004, S. 13f.].

Durch die Richtlinie erfasst ist jede automatisierte oder manuell durchgeführte Verarbeitung personenbezogener Daten von natürlichen Personen. Dadurch soll ein Binnenmarkt mit freiem Verkehr von Waren, Personen, Dienstleistungen und Kapital ermöglicht werden [Graf, 2004, S. 14]. Die Voraussetzungen, die eine rechtmäßige Verarbeitung von personenbezogenen Daten erlaubt, werden laut Art. 5 von den Mitgliedsstaaten selbst festgelegt. Für die Verarbeitung personenbezogener Daten sehen die Art. 6 bis 9 ein zweistufiges Zulässigkeitskonzept vor. Eine Verarbeitung muss erstens die in Art. 6 aufgelisteten Kriterien erfüllen, damit sie als zulässig qualifiziert werden kann. Auf die Kriterien wird hier nicht näher eingegangen, aber eine Verarbeitung von personenbezogenen Daten muss immer zweckgebunden sein. Aus diesem Grund kann eine Datensammlung auf Vorrat nie zulässig sein, da in diesem

Fall die Zweckgebundenheit nicht gegeben ist. Zweitens werden in Art. 7 konkrete Erlaubnistatbestände aufgeführt. Damit eine Verarbeitung legitim ist, müssen die Kriterien der Art. 6 und 7 erfüllt sein, das heißt die Verarbeitung muss zweckgebunden sein und unter einen der Erlaubnistatbestände fallen. In Art. 8 werden sensible Daten definiert (zum Beispiel ethnische Herkunft, religiöse Überzeugung, politische Meinung, etc.) die nicht verarbeitet werden dürfen, außer die Verarbeitung fällt die Ausnahmeregelungen des Artikels [Graf, 2004, S. 17f.].

Die Richtlinie räumt den Betroffenen ein Information- und Auskunftsrecht sowie einen Anspruch des Betroffenen auf Berechtigung, Löschung und Sperrung der Daten und ein Widerspruchsrecht ein [Graf, 2004, S. 20ff.]. Den Mitgliedsstaaten wird in einigen Punkten bei der Umsetzung der Richtlinie in innerstaatliches Recht, ein sehr großer Ermessensspielraum eingeräumt, weshalb es meiner Meinung nach nicht überraschend ist, dass die Einheitlichkeit bei der Umsetzung im EU-Raum nicht gewährleistet sein kann (siehe dazu weiter unten 2.4.6 Resümee).

2.4.3. Die Vorratsdatenspeicherungs-Richtlinie 2006/24/EG der EU

Die EU-Richtlinie 2006/24/EG des Europäischen Parlaments und des Rates vom 15. März 2006 beinhaltet die Vereinheitlichung der Vorratsspeicherung von Daten der Mitgliedsstaaten. Dabei ist die Richtlinie äußerst umstritten, da bei jeder elektronischen Kommunikation übermittelte Daten, ohne dass dabei ein Verdacht auf kriminelle oder terroristische Handlungen bestehen muss, bis zu zwei Jahre auf Vorrat gespeichert werden dürfen. Neben verfassungsrechtlichen Unsicherheiten bestehen auch Probleme mit der gemeinschaftsrechtlichen Kompetenz. Kritisiert wird hierbei vor allem, dass die EU in diesem Zusammenhang ihre Kompetenzen überschritten hat [Gitter & Schnabel, 2007, S. 411, 416].

Ziel der Richtlinie ist die Vereinheitlichung der Regelungen der Mitgliedsstaaten bezüglich der Vorratsspeicherung, um bei schweren Straftaten auf Verkehrsdaten zugreifen zu können. Der Begriff der „schweren Straftat“ muss von jedem Mitgliedstaat selbst definiert werden. Jeder Kommunikationsdienstleister ist gemäß der Richtlinie dazu verpflichtet, gewisse Daten auf Vorrat zu speichern und im Bedarfsfall an die zuständige Behörde weiterzuleiten. Dabei handelt es sich um alle Kommunikationsdaten (Verkehrs- und Standortdaten) sowie alle Daten die es ermöglichen den Nutzer der Dienstleistung zu identifizieren. Bei der Nutzung von Telefon und E-Mail

werden zusätzlich auch die Daten zur Identifizierung des Kommunikationspartners erhoben. Bei der Nutzung von mobilen Geräten muss der Standort ermittelt werden [Gitter & Schnabel, 2007, S. 411f].

Gemäß der weiter oben definierten Datenschutzrichtlinie 95/46/EG ist die, unabhängig von einem Verdacht, durchgeführte Speicherung von Kommunikationsdaten auf Vorrat verboten. Es besteht zwar eine Ausnahmeregelung in Artikel 13 Absatz 1 wenn beispielsweise die nationale oder öffentliche Sicherheit gefährdet ist, die Vorratsspeicherung muss aber „notwendig, angemessen und verhältnismäßig“ sein. Die Vorratsspeicherungs-Richtlinie geht einen Schritt weiter und verringert damit die Anonymität der übermittelten Daten, da die Mitgliedsstaaten die Vorratsspeicherung durchführen müssen, auch wenn die nationale Gesetzgebung dem entgegensteht [Gitter & Schnabel, 2007, S. 412].

2.4.4. Das Telekommunikationsgesetz 2003

Mit dem Telekommunikationsgesetz 2003 (TKG 2003) wurden einige EG-Richtlinien umgesetzt, vor allem die Datenschutzrichtlinie für elektronische Kommunikation. Das DSG 2000 wird durch datenschutzrechtliche Regelungen des TKG 2000 ergänzt, diese Regelungen gelten als Sonderdatenschutzrecht. Auf Anbieter, das sind gemäß § 92 Absatz 3 Ziffer 1 TKG Betreiber eines öffentlichen Kommunikationsdienstes beziehungsweise -netzes, finden die Sonderbestimmungen des TKG Anwendung. Darunter fallen Telefonie-Unternehmen, bestimmte Provider, Anbieter von Mehrwertnummern, Call-Shops, Kabelnetzbetreiber, Internet-Cafés und teilweise auch Rundfunkunternehmen. Unter anderem wird in § 93 Absatz 1 TKG ein Kommunikationsgeheimnis geregelt, diesem unterliegen Inhalts-[3], Verkehrs-[4] und Standortdaten[5] und des Weiteren auch Daten die bei erfolglosen Verbindungsversuchen gesammelt wurden. Diese soeben genannten Daten dürfen gemäß § 96 Absatz 1 TKG aufgrund des Zweckbindungsgrundsatzes nur im Zusammenhang der Bereitstellung eines Kommunikationsdienstes ermittelt beziehungsweise verarbeitet werden. Die Daten dürfen

[3] Inhaltsdaten: gemäß § 92 Absatz 3 Ziffer 5 TKG sind dies die Inhalte einer übertragenen Nachricht [Janisch & Mader, 2006, S. 34].
[4] Verkehrsdaten: darunter versteht man gemäß § 92 Absatz 3 Ziffer 4 TKG Daten, die für die Weiterleitung einer Nachricht an ein Kommunikationsnetz oder für die Fakturierung des Vorgangs verarbeitet beziehungsweise gesammelt werden [Janisch & Mader, 2006, S. 34].
[5] Standortdaten: § 92 Absatz 3 Ziffer 6 definiert Standortdaten als Daten, die erstens in einem Kommunikationsnetz verarbeitet werden und zweitens geben sie den geografischen Standort der Telekommunikationsendeinrichtung des Benutzers von einem öffentlichen Kommunikationsdienst an [Janisch & Mader, 2006, S. 34].

nur übermittelt werden, wenn das Vorhaben für die Leistungen des Kommunikationsdienstes, für welchen auch die Daten ermittelt beziehungsweise verarbeitet wurden, erforderlich ist [Janisch & Mader, 2006, S. 16; 33f.].

2.4.5. Sonderfälle des Datenschutzes im Internet

Cookies: Cookies sind Informationen im Textformat, die von einem Informationsanbieter im Internet erstellt und am Computer des Anwenders gespeichert werden. Die gespeicherten Daten dienen dazu, dass der Server des Informationsanbieters bei einem etwaigen nächsten Besuchs des Anwenders, diesen automatisiert wieder erkennen kann. Dadurch können zum Beispiel persönliche Voreinstellungen automatisch abgerufen und wieder hergestellt werden. Die Speicherung der Cookies erfolgt oftmals vom Anwender unbemerkt. Eine Gefahr geht von Cookies insofern aus, als dass das Surfverhalten des Anwenders auf einer Webseite aufgezeichnet oder auch Informationen über persönliche Interessen beziehungsweise Vorlieben gesammelt werden können, ohne dass dabei der Nutzer davon in Kenntnis gesetzt wird [Janisch & Mader, 2006, S. 34].

Cookies zeichnen primär „maschinenbezogene“ Daten auf, das heißt es kann nur ein Bezug zum PC des Anwenders hergestellt werden und nicht zu einer bestimmten Person. Beinhalten Cookies „zumindest indirekt personenbezogene Daten“ und besteht an diesen ein schutzwürdiges Geheimhaltungsinteresse welches vom Anwender ausgeht, dann fällt dieser Tatbestand unter den Geltungsbereich des DSG 2000. Daraus ergibt sich, dass im Einzelfall zu prüfen ist, ob ein Bezug zu einer konkreten Person durch die Cookies herzustellen ist. Der Bezug kann beispielsweise durch Verknüpfungen von User- und Passworteingaben oder mittels E-Mail-Adressen stattfinden. In den soeben genannten Fällen unterliegen die Cookies dem DSG 2000 und somit muss die mehrstufige Zulässigkeitsprüfung nach den §§ 6 bis 9 DSG (siehe Kapitel 2.4.1, S. 26) für eine zulässige Nutzung der Daten erfüllt sein [Janisch & Mader, 2006, S. 34f].

Bei der Umsetzung des TKG 2003 wurde keine direkte Regelung für Cookies erstellt. In § 96 Absatz 3 TKG wird nur eine Informationspflicht des Anbieters vorgeschrieben, bei der der/die BenutzerIn darüber informiert werden soll, welche personenbezogenen Daten ermittelt, verarbeitet und übermittelt werden, auf welcher rechtlichen Grundlage und zu welchem Zweck die Datensammlung erfolgt sowie die Dauer der

Speicherung. Zusätzlich muss der/die BenutzerIn, über das Recht der Verarbeitung widersprechen zu können, informiert werden. Zu beachten ist hierbei, dass die Regelungen nur für öffentliche Access- beziehungsweise Host-Provider gelten, da Content-Provider keine Anbieter im Sinne des TKG 2003 sind. In der Praxis werden Cookies aber gerade eben von Content-Providern eingesetzt, weshalb die Bestimmung in dieser Angelegenheit versagt und die Vorgaben der Datenschutzrichtlinie für elektronische Kommunikation nicht erfüllt [Janisch & Mader, 2006, S. 35].

Logfiles: Daten die während bestimmter Vorgänge am PC gesammelt werden, werden in sogenannten Logfiles abgespeichert. Zweck dieser Sammlung ist beispielsweise die Erstellung eines Protokolls über die Aufrufe der Dateien die sich am Server eines bestimmten Providers befinden. Daraus können Zugriffsprotokolle erstellt werden, bei denen dann auf einfache Weise ein Bezug zu einer Person mittels IP-Adresse erstellt werden kann. Aus diesen Protokollen kann dann ein persönliches Profil über den Anwender produziert werden. Wie beim vorherigen Sonderfall den Cookies, muss in jedem Einzelfall überprüft werden, ob ein Personenbezug über den Maschinenbezug heraus, erstellt werden kann. Für diese Prüfung gilt w.o. das mehrstufige Überprüfungsverfahren gemäß der §§ 6 bis 9 DSG [Janisch & Mader, 2006, S. 35].

Die gesamten Informationen aus Logfiles sind im Sinne des TKG 2003 unter dem Begriff der sogenannten „Verkehrsdaten“ (siehe Kapitel 2.4.4, S. 32) zu subsumieren. Wie weiter oben bereits erwähnt, dürfen diese Daten nicht gespeichert werden und müssen nachdem die Verbindung beendet wurde gemäß § 99 Absatz 1 TKG 2003 sofort gelöscht oder anonymisiert werden. Eine einzige Ausnahme von dieser Regelung findet man in § 99 Absatz 2 TKG 2003, wenn zwecks Verrechnung von Entgelten die Daten gesammelt wurden. In diesem Fall kann der Provider die Daten speichern, bis die rechtlichen Fristen zur Anfechtung der Verrechnung beziehungsweise aller Zahlungsansprüche abgelaufen sind. Sollte ein laufendes Verfahren bezüglich der Höhe des Entgeltes am Laufen sein, so müssen die Daten bis zur Entscheidung gespeichert bleiben. Gemäß § 96 Absatz 3 TKG trifft den Anbieter eine Informationspflicht, da Verkehrsdaten nur für Zwecke die für die Datenanwendung wesentlich sind, verwendet werden dürfen. Gibt es eine Zustimmung des Teilnehmers, so darf der Provider die Daten dafür verwenden, um seine eigenen Telekommunikations-

dienste zu bewerben oder um Services mit einem zusätzlichen Nutzen anzubieten [Janisch & Mader, 2006, S. 35f].

Web-Bugs: Unter Web-Bugs (clear GIFs) versteht man kleine Bilddateien, welche auf Webseiten, in HTML-Dokumenten oder in E-Mails zu finden sind und über die eine Logfile-Aufzeichnung sowie –Analyse möglich gemacht wird. Problematisch bei den Web-Bugs ist, dass sie meist unbemerkt bleiben, während zum Beispiel Cookies, sobald auf die entsprechende Webseite/E-Mail zugegriffen wird, durch entsprechende Browser-Einstellungen deaktiviert werden können. Durch die Web-Bugs kann ein Anbieter ein Profil über den Anwender produzieren. Dies geschieht beispielsweise durch das Öffnen einer E-Mail, wodurch der Web-Bug vom Server heruntergeladen wird und der Download gleichzeitig registriert wird. Der Provider kann dann analysieren wie oft, wann und von wem der Web-Bug heruntergeladen wurde, das heißt er kann ermitteln ob beziehungsweise wann eine E-Mail vom Anwender geöffnet oder eine bestimmte Webseite besucht wurde [Janisch & Mader, 2006, S. 36].

Damit der Geltungsbereich des DSG 2000 berührt wird, muss ein Personenbezug hergestellt werden, dies geschieht durch den gezielten Einsatz von Cookies oder durch die Registrierung des Anwenders auf der entsprechenden Webseite. Kann ein Personenbezug festgestellt werden, muss für eine rechtskonforme Datenanwendung das mehrstufige Zulässigkeitsverfahren nach den §§ 6 bis 9 des DSG (siehe Kapitel 2.4.1, S. 26) erfüllt sein [Janisch & Mader, 2006, S. 36].

Schutz von E-Mails: Es ist vorab zu klären, ob E-Mails unter den Geltungsbereich des Art. 10 StGG, dem Schutz des Briefgeheimnisses, fallen. Unter diesen Schutz fallen nur verschlossene Briefe, was im Regelfall bei E-Mails nicht gegeben ist, da diese nicht über ein „Kuvert“ im Sinne des Gesetzes verfügen. Man muss aber auf der anderen Seite beachten, dass diese Voraussetzung bei verschlüsselten E-Mails durchaus gegeben ist, da eine Verschlüsselung nach herrschender Ansicht als eine Art „elektronisches Kuvert“ angesehen wird [Janisch & Mader, 2006, S. 36].

Jedoch sind E-Mails gemäß Art. 10a StGG durch das Fernmeldegeheimnis geschützt. Diese Regelung schützt die Vertraulichkeit der Kommunikation über jede Art von Fernübermittlungsmöglichkeit (zum Beispiel Telefon, Funk, etc.), welche nicht für

Dritte bestimmt ist. Verstöße gegen das Grundrecht des Fernmeldegeheimnisses sind explizit im Gesetz geregelt und können auch nur mit gerichtlichem Bescheid durchgesetzt werden [Janisch & Mader, 2006, S. 36].

Auskunftspflicht des Access-Providers: Anfang 2005 beschäftigte viele Gerichte die Frage, ob und wenn ja unter welchen Voraussetzungen den Access-Provider eine Auskunftspflicht trifft, wenn aufgrund einer strafrechtlichen Verfolgung eine IP-Adresse zu einem Internetnutzer zugeordnet werden muss. Dabei ging es vor allem um die Forderungen der Musikindustrie die wahren Identitäten von Nutzern gewisser Tauschbörsen im Internet ausfindig zu machen. Nachdem es viele teils konträre Entscheidungen seitens der Gerichte gab, erkannte der OGH (Rechtssachen 11 Os 57/05z, 11 Os 58/05x und 11 Os 59/05v), dass die auskunftsbegehrenden Personen durch die Kenntnis der IP-Adresse nur Namen und Anschrift des Verdächtigen ausforschen wollen, dem diese IP-Adresse im Zeitpunkt des Rechtsverstoßes zugeordnet war. Bei diesen Daten handelt es sich um Stammdaten im Sinne des TKG 2003, welche nicht unter den Schutz des Grundrechts des Fernmeldegeheimnisses gemäß Art. 10a StGG fallen. §103 Absatz 4 TKG normiert, dass Name und Adresse von individuell zugeordneten Internetanschlüssen formlos bekannt gegeben oder durch Zeugenaussagen einer physischen Person in Vertretung des Access-Providers ermittelt werden können [Janisch & Mader, 2006, S. 36f].

2.4.6. Resümee

Zusammenfassend kann man sagen, dass der Rechtsschutz zwar für die Verarbeitung von personenbezogenen Daten von Betroffenen noch immer in den „Kinderschuhen“ steckt. Gleichzeitig kann von einer deutlichen Verbesserung der Situation im Vergleich zu den letzten Jahrzehnten ausgegangen werden.

Gemäß einer Mitteilung der Europäischen Kommission (2007) haben alle Mitgliedsstaaten inzwischen die Richtlinie 95/46/EG in innerstaatliches Recht umgesetzt. Die Kommission stellte aber teilweise eine lückenhafte Umsetzung der Richtlinie, sowie Abweichungen bei der Umsetzung die im Rahmen eines Ermessenspielraumes den Mitgliedsstaaten zusteht, fest. Diese Unterschiede werden aber von der Kommission „(…) als eine natürliche Folge eines solchen Spielraums“ bewertet. Als zukünftiges Ziel sieht die Kommission aber, trotz der davor als natürliche Folge definierten lückenhaften Umsetzung, eine Zusammenarbeit mit den Mitgliedsstaaten vor und wird

möglicherweise auch förmliche Vertragsverletzungsverfahren einleiten, mit dem Ziel gleiche Bedingungen in Bezug auf die Umsetzung der Richtlinie im gesamten EU-Raum zu schaffen. Des Weiteren wurde auch die Auswirkung der Datenschutzrichtlinie auf die Wirtschaft im Rahmen einer Studie (“Economic evaluation of the Data Protection Directive (95/46/EC)") von der Kommission untersucht. Die Studie zeigte auf, dass die Kosten für die Umsetzung der Richtlinie für Unternehmen eine geringe Auswirkung hatte und deshalb der freie Verkehr von personenbezogenen Daten, trotz Unterschiede im Binnenmarkt, mit einem hohen Niveau an Datenschutz ermöglicht wird [Kommission, 2007, S. 5f.; 7; 10].

2.5. Datenschutzfreundliche Technologien (privacy-enhancing technologies)

Das nachfolgende Kapitel bietet eine kurze Einleitung zu dem Thema datenschutzfreundliche Technologien. Zuerst wird der Begriff „PET“ definiert, danach werden Funktionen und Vor- beziehungsweise Nachteile erläutert, um dem/der Leser/In einen Überblick über datenschutzfreundliche Technologien zu bieten und gleichzeitig auf die Inhalte von Kapitel 3 (Standards um Datenschutzklauseln zu spezifizieren) vorzubereiten.

2.5.1. Was versteht man unter PET?

Unter PET (Privacy-enhancing technologies)[6] versteht man eine Vielzahl von Technologien, die zur Sicherung des persönlichen Datenschutzes, durch Minimierung oder vollständiger Verhinderung der Datensammlung, eingesetzt werden können [Fischer-Hübner, 2001, S. 107].

PETs können folgende Funktionen übernehmen [Cranor L. F., 2003, S. 80]:

- sie verhindern nicht autorisierte Zugriffe auf Nachrichten (communications) oder gespeicherte Daten,
- Automatisierung des Abrufs der Datenschutzpraktiken der Person die Daten abrufen/sammeln möchte und auf dieser Basis automatisierte Entscheidungsfindung für den/die BenutzerIn,
- automatisierte Überprüfung der Datenschutzpraktiken des Datensammlers,
- Filterung von unerwünschten Nachrichten,
- sie verhindern die automatische Datensammlung durch Cookies, Spyware, „web bugs“, etc.,
- erleichtern Transaktionen wobei persönliche Daten auf einem minimalen Niveau offenbart werden.

Fischer-Hübner (2001) identifiziert vier Sicherheitsaspekte, um die Vertraulichkeit, Integrität und Verfügbarkeit von persönlichen Daten zu erhöhen und somit die Privatsphäre besser zu wahren:

[6] Privacy Enhancing Technologies werden auf Deutsch auch als „datenschutzfreundliche Technologien“ bezeichnet. In dieser Arbeit wird im Folgenden ausschließlich die englische Bezeichnung beziehungsweise Abkürzung PET verwendet.

- *Anonymity (Anonymität):* Anonymität ist die Schlüsselkomponente um die Privatsphäre von Benutzern zu wahren. Dabei ist das Ziel die Identität einer Person, die eine Ressource oder ein Service (zum Beispiel Nachrichten versenden beziehungsweise erhalten) benutzt, geheim zu halten [Fischer-Hübner, 2001, S. 107].
- *Pseudonymity (Pseudo-Anonymität):* Pseudo-Anonymität soll die Benutzeridentität dann wahren, wenn Anonymität nicht gewährleistet werden kann. Dies kann beispielsweise dann der Fall sein, wenn der Benutzer für seine Handlungen oder Aktivitäten verantwortlich ist [Fischer-Hübner, 2001, S. 107].
- *Unobservability (Unbeobachtbarkeit):* Bei der Unbeobachtbarkeit sollen Andere, besonders Dritte, daran gehindert werden, einen Benutzer bei der Nutzung einer Ressource oder eines Services zu beobachten [Fischer-Hübner, 2001, S. 108].
- *Unlinkability*: Dabei soll der Benutzer auf Ressourcen und Services zugreifen können, ohne das Dritte diese Nutzungen miteinander verknüpfen können [Fischer-Hübner, 2001, S. 108].

Jensen et. al. (2007) haben in ihrer Untersuchung über die Datensammlung und Datenschutzpraktiken von Webseiten mithilfe des iWatch Web Crawlers Techniken beziehungsweise Terme aufgelistet, mit denen der Datenschutz einer Seite evaluiert werden kann. iWatch wurde speziell für die Untersuchung von Jensen et al. (2007) programmiert. Der Name iWatch soll eine Anspielung auf die berühmte Frage von Platon: „“Quis custodiet ipsos custodes?” sein, was soviel wie „Wer überwacht die Wächter?“ bedeutet. Der Web Crawler iWatch überwacht Webseiten die normalerweise die Nutzer überwachen. iWatch soll eine Quelle für Informationen über Datenschutz, Sicherheit und Datensammlung im Internet sein. Dabei gibt es verständlicherweise eine Limitierung auf nur jene Daten die für den Crawler sichtbar und automatisiert abrufbar sind. Die Vorgehensweise von iWatch ist wie bei jedem Web Crawler beziehungsweise Spider, er sucht nach und katalogisiert Datenverarbeitungspraktiken. Dabei werden HTTP Tokens oder HTML Konstrukte und Muster aufgezeichnet, welche bestimmte Datenverarbeitungs- beziehungsweise Datensammlungspraktiken aufzeigen [Jensen, Sarkar, Jensen, & Potts, 2007, S. 2-4] Die Katalogisierung erfolgte anhand folgender Merkmale, welche zur Evaluierung des Daten-

schutzstandards einer Webseite herangezogen werden können [Jensen, Sarkar, Jensen, & Potts, 2007, S. 4]:

- *Cookies*: Bezüglich Cookies wurde der Einsatz von verschiedenen Arten und deren Charakteristika untersucht. (siehe oben Kapitel 2.4.5 auf Seite 33 für eine Erläuterung zu dem Thema Cookies)
- *Unaufgeforderte Popups*[7] *(Unsolicited Popups):* Untersuchung des Einsatzes von unaufgeforderten Popups.
- *Web Bugs*: Analyse des Einsatzes von Hilfsmitteln, um Nutzer über mehrere Webseiten zu verfolgen. (siehe w.o. Kapitel 2.4.5 auf Seite 33 für eine Erläuterung zu dem Thema Web Bugs)
- *Banner*[8]*:* Auswertung des Einsatzes von unterschiedlichen Arten von Bannern, welche Nutzer über mehrere Webseiten verfolgen können.
- *P3P Policy:* Identifizierung des Einsatzes von P3P durch die Analyse des HTTP-Headers. (siehe Kapitel 3.1 auf Seite 45 für Informationen über P3P)
- *Datenschutz-Gütesiegel*: Untersuchung des Einsatzes von Datenschutz-Gütesiegeln (zum Beispiel TRUSTe, BBBOnline, WebTrust, etc.) auf den Webseiten einer Domain (Link und Grafik).
- *Netzwerke um gemeinsam Daten zu nutzen (Data-sharing networks)*: Analyse der Techniken mit deren Hilfe Nutzer über mehrere Seiten verfolgt werden können (Drittanbieter Cookies, Web Bugs, Banner) und der beteiligten Akteure.
- *Link-Struktur*: Erhebung der Basisinformationen über die Link-Struktur und Beziehungen zwischen den Seiten.
- *Geographische Informationen*: Kartographische Erfassung der Domain/Server IP von einem Land mithilfe der GeoLite Datenbank.

[7] Der Begriff Pop-up stammt aus dem Englischen „to pop up“ und bedeutet „plötzliches auftauchen“. Damit sind vor allem Pop-up-Fenster (Aufklappfenster) im Internet gemeint, die von Anbietern meist dazu genutzt werden um zu werben.
(vgl. http://de.wikipedia.org/wiki/Pop-up Datum und Uhrzeit der Abfrage: 28. Juli 2008 14:37)

[8] Als Banner bezeichnet man eine Form der Werbung im Internet. Diese sind entweder in die Webseite eingebettet oder legen sich für ein paar Sekunden über die gesamte Seite (sog. Powerlayer). Banner verfügen über einen Link, über den man auf die Webseite des Werbenden kommt.
(vgl. http://de.wikipedia.org/wiki/Werbebanner Datum und Uhrzeit der Abfrage: 29. Juli 2008 13:26)

2.5.2. Wozu dienen sie?

Wie bereits in Kapitel 2.5.1 erwähnt, übernehmen PETs bestimmte Funktionen. Nachfolgend sollen einige Beispiele für Technologien aufgeführt werden, welche diese genannten Funktionen übernehmen. Dabei wird aber kein Anspruch auf Vollständigkeit erhoben.

Encryption Tools: Encryption oder auch Verschlüsselung/Codierung genannt, wird dazu verwendet, um gespeicherte oder über das Internet übermittelte Informationen zu schützen. Eigentlich ist Verschlüsselung ein Sicherheitstool, um nicht autorisierte Zugriffe auf Computer, Kommunikation oder Dateien zu verhindern, wodurch gleichzeitig auch persönliche Daten geschützt werden können. Encryption sowie andere Sicherheitstools sind zwar für den Datenschutz sehr wichtig, aber nicht ausreichend. An dieser Stelle soll ein Beispiel diesen Zusammenhang aufzeigen. Ein Individuum benutzt einen verschlüsselten Kanal, um seine Daten an eine Webseite zu übermitteln. Diese Webseite benutzt wiederum eine Verschlüsselung, um Zugriffe auf die Datenbank zu vermeiden. Dabei ist aber nicht gewährleistet, dass die Betreiber/Inhaber der Webseite die gesammelten Daten der Kunden/Benutzer an Dritte für Marketingzwecke verkauft. Obwohl qualitativ hochwertige Encryption Software weit verbreitet ist und auch teilweise umsonst runtergeladen werden kann, wird dieses Sicherheitstool kaum verwendet. Die meisten Internetbrowser haben eingebaute Encryption Tools, die automatisch Daten verschlüsseln, sobald diese im Internet übermittelt werden, wobei die Benutzer meist gar nichts davon mitbekommen. Daraus resultiert die Gefahr, dass eine Vielzahl von E-Mails nicht verschlüsselt versendet werden und somit auf einfachste Weise abgefangen und gelesen werden, sei es am Computer zu Hause, beim Senden oder während sie beim Internet Service Provider gespeichert sind [Cranor L. F., 2003, S. 80].

P3P und Identity Manager: An dieser Stelle wird P3P als eine mögliche Technologie zum Schutz personenbezogener Daten erwähnt. Eine umfassende Erläuterung der Funktionsweise, sowie Vor- und Nachteile beziehungsweise Kritik findet sich in Kapitel 3.1 auf Seite 45. An dieser Stelle soll nur insoweit darauf eingegangen werden, als das bei P3P der Internetbrowser (oder eine andere P3P Software) automatisiert ermittelt welche Daten vom Webseitenbetreiber abgerufen werden, dies mit den Präferenzen des Benutzers vergleicht und im Falle eines Verstoßes gegen dessen Ein-

stellungen , diese Seiten nicht aufgerufen werden können oder Cookies geblockt werden [Cranor L. F., 2003, S. 80f].

Automated Privacy Audits (Automatisierte Datenschutzprüfungen): Ein oft genanntes Problem bei P3P ist, dass die Unternehmen zwar automatisiert über ihre Datenschutzerklärungen kommunizieren können, aber eine Garantie für deren Einhaltung fehlt. Für viele Organisationen ist es auch schwer herauszufinden ob sie überhaupt ihre eigene Erklärung bezüglich des Datenschutzes einhalten. Sogenannte Privacy Audits können diesbezüglich Abhilfe verschaffen. Automatisierte Tools helfen den Unternehmen bei der Überwachung der eigenen Datenkommunikationen und decken mögliche Datenschutzverletzungen auf. Dabei werden vor allem die Datenströme zur und von der Webseite der Organisation, ausgefüllte Formulare und die Verwendung von Cookies von einem Tool automatisch überwacht und ausgewertet. Wird ein Verstoß gegen die Datenschutzerklärung des Unternehmens durch die automatisierte Datenschutzprüfung aufgedeckt, wird dies an die zuständige Person weitergeleitet, welche dann den Sachverhalt überprüft und notfalls eingreift. Die Schwachstelle bei den Privacy Audits liegt darin, dass nicht sämtliche Datenbewegungen überprüft werden können, da es zu viele Möglichkeiten für Datenströme geben kann, die dann außerhalb der Reichweite des Audits liegen [Cranor L. F., 2003, S. 81].

Spam Filtering: Fast jeder Internet-Nutzer hat schon ungewollte Emails erhalten, welche als „Spam“ bezeichnet werden. Problematisch ist bei Spam-Mails, dass für gewöhnlich eine sehr hohe Anzahl unterschiedlicher Nachrichten an eine Adresse versendet werden und somit die Mailbox überlastet wird. Ein weiteres Problem sind auch die meist pornografischen Inhalte und irreführende Werbungen. Mittlerweile gibt es viele Tools um sich vor Spams zu schützen, aber keine 100%ige Lösung. Spammer lassen sich immer neue Möglichkeiten einfallen um Spamfilter zu umgehen, weshalb Spamfilter zwar das Problem eindämmen können, aber niemals eine komplette Lösung darstellen [Cranor L. F., 2003, S. 82].

Cookie Cutters, Bug Zappers und verwandte Tools: Cookie Cutters sind Programme die den Internetbrowser daran hindern Cookies mit Webseiten auszutauschen. Es gibt verschiedene Arten von Cookie Cutters, es gibt welche die alle Cookies blockieren, andere die über eine Konfiguration verfügen bei der eingestellt werden kann,

welche Cookies blockiert werden sollen und es gibt Cookie Cutters die regelmäßig Cookies vom PC des Benutzers löschen. Des Weiteren können auch Bannerwerbungen, Pop-up Fenster, animierte Grafiken und andere ungewollte Webelemente von Cookie Cutters blockiert werden. Einige dieser Tools suchen auch nach unsichtbaren Bildern die Cookies erstellen (sog. „Web Bugs“) oder nach Spyware. Bei Spyware handelt es sich um Programme, welche Informationen über den Nutzer sammeln und an die entsprechende Webseite senden, ohne dass die ausspionierte Person davon in Kenntnis gesetzt wird. Ein großer Vorteil von Cookie Cutters, Bug Zappers und verwandten Tools ist, dass sie weit verbreitet und darüber hinaus auch größtenteils umsonst oder zu einem sehr geringen Preis zu bekommen sind. Die Tools sind auch sehr einfach zu benutzen, obwohl die meisten Internet-NutzerInnen überhaupt nicht verstehen was ein Cookie ist, warum sie manche dieser Cookies blockieren sollten und wie man dies macht [Cranor L. F., 2003, S. 82].

Anonymizers („Proxy“): Anonymizers sind Tools und Services die es ermöglichen anonym im Internet zu surfen oder E-Mails zu schreiben. Diese Tools minimieren das Risiko des Nutzers durch Abfragen im Internet oder durch E-Mails mit einer IP-Adresse in Verbindung gebracht und somit identifiziert zu werden. Es gibt Anonymizers, die jegliche Informationen des Benutzers entfernen und danach die durch den Nutzer getätigten Abfragen weiterleiten. Eine Vielzahl von Proxy-Services ist kostenlos zu bekommen. Anonymizers sind eine sehr gute Wahl um Informationen des Nutzers bei Interaktionen, die online durchgeführt und bei denen keine persönlichen Informationen benötigt werden, zu transferieren. Eine Schwachstelle hierbei ist aber, dass sie kaum nützlich sind, wenn persönliche Daten explizit übertragen werden müssen [Cranor L. F., 2003, S. 82].

Andere PETs: Derzeit erscheinen immer mehr Endnutzerprodukte die für mehr Datensicherheit sorgen sollen. Viele dieser Produkte bestehen aus einer Software die Dateien löschen die durch Browser- oder E-Mailprogramme auf einem Computer hinterlassen werden. Des Weiteren gibt es auch speziell entwickelte Software, um den Zugang zu nicht jugendfreien Seiten für Kinder zu blockieren oder es unmöglich zu machen, persönliche Informationen über das Internet preiszugeben. Ein neuer Ansatz bei den PETs sind Tools die Informationen in Datenbanken nicht identifizierbar machen. Dabei werden Daten teilweise entfernt, um sicherzustellen das kein Zu-

sammenhang zu einem Individuum hergestellt werden kann [Cranor L. F., 2003, S. 83].

2.5.3. Vor- und Nachteile

Wie in Kapitel 2.5.2 gezeigt, können PETs eine Vielzahl von unterschiedlichen Funktionen übernehmen. Jedes Tool beziehungsweise Service verfügt dabei wiederum über individuelle Stärken und Schwächen, da es bis dato noch keine 100%ige Lösung für alle Bedürfnisse der Nutzer gibt. Um die Nachteile eines Tools umgehen zu können, kann ein Nutzer derzeit nur ein anderes Tool verwenden, welches diese Funktionen übernimmt. Die spezifischen Vor- und Nachteile der jeweiligen Tools und Services können weiter oben in Kapitel 2.5.2 nachgelesen werden.

2.5.4. Zusammenfassung und Ausblick

PETs können Nutzern sehr stark bei ihrem persönlichen Datenschutz helfen. Sie können aber nicht garantieren, dass wenn der Nutzer Daten preisgibt, mit den Informationen nicht in die Privatsphäre eingegriffen wird. Derzeit sind PETs „nur“ eine Ergänzung zu behördlichen oder selbstgeregelten Datenschutzinitiativen. Die Möglichkeiten sind auch teilweise aufgrund der oftmals störenden oder auch mühsamen Benutzung der Tools beschränkt. Die Effektivität von PETs könnte durch verbesserte Interfaces und durch nahtlose Integration in andere Tools (damit sie ohne zusätzliche Bedienung genutzt werden können) stark erhöht werden. Der Schutz der PETs wird aber weiterhin auf ein bestimmtes Maß begrenzt bleiben, da fast jede Online-Transaktion persönliche Daten abruft. Sobald die Architektur der Transaktionssysteme geändert und somit weniger Informationen übertragen werden würden, könnten PETs auch einen besseren Schutz für die Nutzer bieten. Während diese Änderungen technisch gesehen keine Probleme darstellen, scheint es an anderer Stelle maßgebliche Hindernisse zu geben die dies hemmen [Cranor L. F., 2003, S. 83].

3. Standards um Datenschutzklauseln zu spezifizieren

Kapitel drei stellt die datenschutzfreundlichen Technologien P3P, APPEL und EPAL im Detail vor. Dabei werden die Funktionsweise, Anwendungsbeispiele sowie Vor- und Nachteile jeweils analysiert. Eine Zusammenfassung der wichtigsten Punkte am Ende des Kapitels beendet die Darstellung dieser Technologien.

3.1. Platform for Privacy Preferences (P3P)

1994 wurde das WWW Konsortium (W3C) gegründet, mit dem Ziel die Entwicklung des World Wide Webs zu leiten und durch Wahrung der Interoperabilität dessen Weiterentwicklung zu fördern. Derzeit sind etwa 500 Unternehmen Mitglieder der W3C Arbeitsgruppe. Im „Advisory Committee“ sitzt jeweils ein Repräsentant von jedem Unternehmen das Mitglied ist. Die Vertreter arbeiten in „Working Groups“ (WGs), „Interest Groups“ und „Coordination Groups“. Die WGs schreiben technische Berichte, die auch zu einer Empfehlung erweitert werden können, das heißt das sich daraus ein W3C Standard entwickeln kann [Trček, 2006, S. 6].

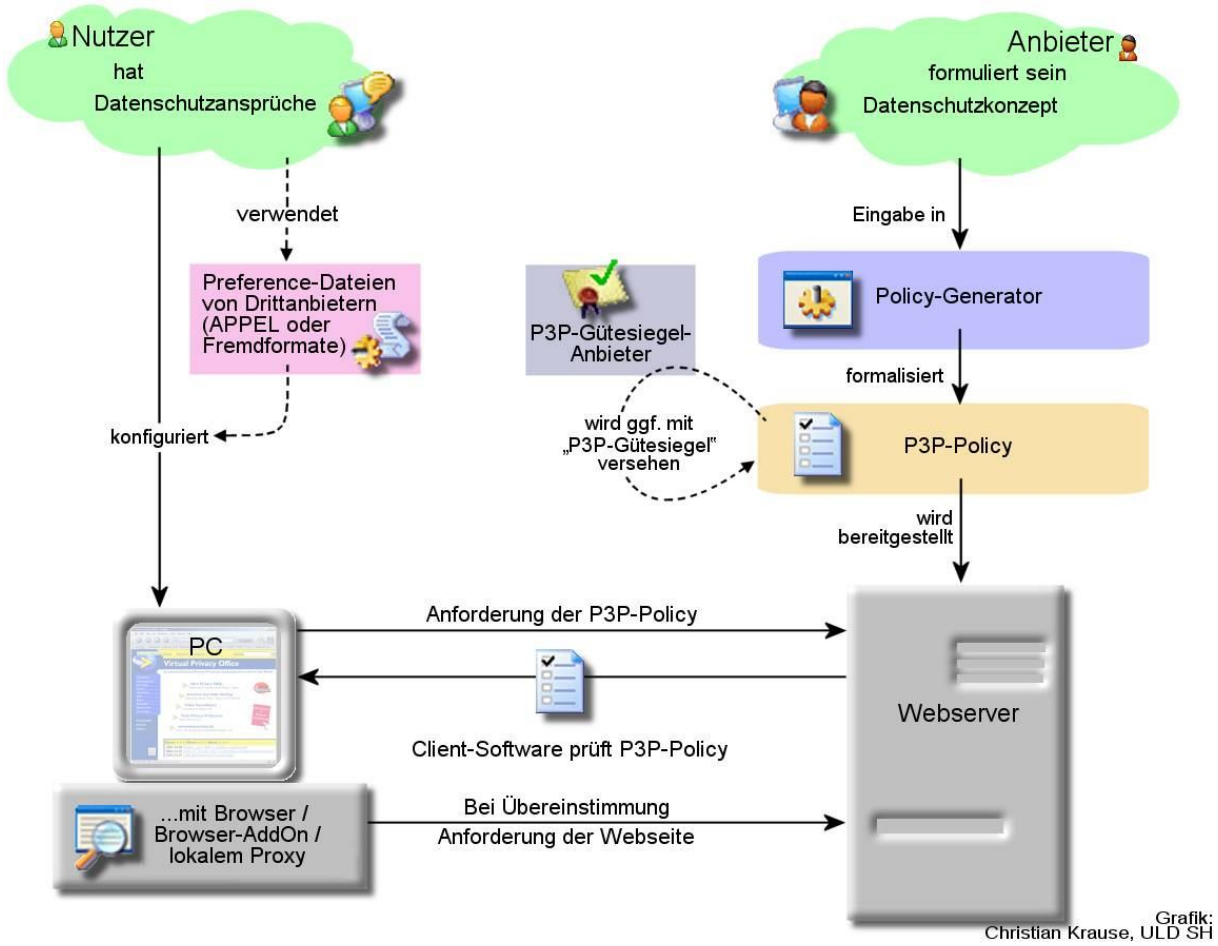
1993 wurde P3P (Abkürzung für „Platform for Privacy Preferences“) von W3C entwickelt. P3P ist eine international standardisierte, technische Plattform mit der Datenschutzinformationen über das Internet übermittelt werden können. Dadurch können Benutzer automatisiert feststellen, welche personenbezogenen Daten zu welchem Zweck von einer Webseite oder Dritten abgerufen beziehungsweise verarbeitet werden [Möller, Datenschutz mit P3P, 2003].

3.1.1. Funktionsweise

Zuerst legt der Anbieter einer Webseite seine Datenschutzerklärung mit seinen relevanten Praktiken der Datenverarbeitung als Textfile und im P3P-Format am Webserver ab. Die P3P-Policy, das heißt die Datenschutzerklärung des Anbieters im P3P-Format, entsteht durch übersetzen des Textfiles in den P3P-Standard. Die Erklärung besteht aus Antworten auf Multiple-Choice-Fragen und ist maschinenlesbar, da sie als XML-Datei mit P3P-Syntax gespeichert wird. Der Internet-Nutzer kann in einem P3P-Agenten (das ist z.B. ein P3P-fähiger Internetbrowser) einstellen, welche Art von Informationen er/sie an Webanbieter beziehungsweise Dritte weitergeben möchte. Kommt ein Nutzer auf eine Webseite, ruft dessen P3P-Agent automatisch die Datenschutzerklärung im maschinenlesbaren P3P-Format vom Server ab und vergleicht

die Angaben des Anbieters und Benutzers. Stimmen die Erklärungen nicht überein, wird der Internetsurfer durch eine Warnung darauf hingewiesen. Der Benutzer erhält dann in seiner Sprache alle Informationen der Datenschutzerklärung in einer zusammengefassten und für ihn/sie relevanten Version. In der Zusammenfassung wird darüber hinaus besonders auf die Unterschiede hingewiesen und ein Link zur Datenschutzerklärung im Textformat angezeigt, wodurch die Suche auf der Webseite entfällt [Möller, Datenschutz mit P3P, 2003; Ulber, 2004]. Abbildung 6 stellt den soeben beschriebenen Prozess graphisch dar.

Abbildung 6: Funktionsweise von P3P



Quelle: [Möller, 2003]

Das besondere an P3P ist, dass die Datenschutzerklärungen der Webseitenanbieter und die Datenschutzansprüche des Benutzers formalisiert werden. Das P3P-Format macht die Informationen für Maschinen lesbar und somit kann die Überprüfung der Erklärungen beider Seiten automatisiert durchgeführt werden. Nachfolgend soll ein

Anwendungsbeispiel von P3P den soeben beschriebenen Prozess erläutern [Möller, Datenschutz mit P3P, 2003].

3.1.1. Anwendungsbeispiel für die Nutzung von P3P

Die Nutzerin in diesem Beispiel heißt Claudia und sie besucht einen Onlineshop namens „CatalogExample“ auf der Seite www.catalogexample.com. Der Shop besitzt auf allen Seiten eine P3P-Policy und Claudias Browser verfügt über ein P3P-Addon. Wenn Claudia die Internetadresse von CatalogExample in ihren Browser eintippt, fordert dieser automatisch die P3P-Policy für diese Seite an. Die Policy gibt an, dass nur Daten, die in den Standard HTTP Access Logs zu finden sind, gespeichert werden. Nun überprüft der Internetbrowser, ob diese Policy mit den Angaben, die Claudia in ihrem Browser zuvor definiert hat, übereinstimmen. Wenn sie im Browser eingestellt hat, das diese Daten freigegeben sind, dann wird die Webseite ganz normal angezeigt. Manche Internetbrowser verfügen über kleine Symbole an den Rändern des Bildes, die anzeigen dass eine Policy abgerufen wurde und sie mit ihren Einstellungen übereinstimmt [W3C-WorkingGroup, 2006].

Beispielsweise zeigt der AT&T Privacy Bird in der oberen rechten Ecke der Titelleiste des Browsers verschiedenfarbige Vögel an. Je nachdem ob die P3P-Policy mit den Angaben des Nutzers übereinstimmen erscheint der Vogel in rot, gelb oder grün (siehe Abbildung 7). Des Weiteren kann der Nutzer auch mittels eines akustischen Lautes - einem Vogelzwitschern - auf Warnungen hingewiesen werden [P3PToolbox].

Abbildung 7: P3P Warnsymbole des AT&T Privacy Bird

Quelle: [P3PToolbox]

Zurück zum Anwendungsbeispiel, als nächstes besucht Claudia den Online-Katalog der Webseite, der mit einer komplexe Software realisiert wurde. Diese verwendet Cookies, um eine Warenkorb Funktion (shoping cart feature) zu implementieren. Da auf dieser Seite mehr Daten gesammelt werden, gibt es auch eine separate P3P-Policy. Sollte diese Policy auch mit Claudias Einstellungen übereinstimmen, wird ihr diese Seite ohne Warnungen (pop-ups) angezeigt. Claudia sucht sich einige Waren

aus und gelangt auf die Seite wo sie ihre Bezahlung tätigen kann. Auf der Seite von CatalogExample werden folgende zusätzliche Informationen gesammelt: Claudias Name, Adresse, Kreditkartennummer und ihre Telefonnummer. Eine neue P3P-Policy gibt an, dass diese Daten gesammelt und nur für die gegenwärtige Transaktion verwendet werden. Wieder überprüft ihr Browser die P3P-Policy. Angenommen Claudia möchte gewarnt werden, wenn eine Seite ihre Telefonnummer verlangt. Diesmal würde beim Browser eine Warnmeldung erscheinen, die erklärt, dass die Webseite ihre Telefonnummer fordert und gleichzeitig den Inhalt der P3P-Erklärung erläutern. Claudia kann dann entscheiden ob dies für sie akzeptabel ist und mit ihrer Bestellung fortfahren. Sollte sie die Bedingungen nicht akzeptieren, kann sie die Transaktion abbrechen [W3C-WorkingGroup, 2006].

3.1.2. Erstellen einer P3P-Datenschutzerklärung

Um eine P3P-Datenschutzerklärung erstellen zu können, muss in einem ersten Schritt eine Datenschutzerklärung für die eigene Firma geschrieben werden. Dabei sollte vor allem darauf geachtet werden - dies gilt auch für eine bereits vorhandene Erklärung - dass sämtliche Datensammlungen und –anwendungen aufgelistet werden, wer Zugang dazu hat und wie lange diese gespeichert werden. Diese Teile werden dann mithilfe eines (P3P-)Policy-Generators in eine maschinenlesbare Form umgewandelt. Sollte ein Unternehmen auf seinen Webseiten unterschiedliche Daten sammeln, kann für jede Seite eine eigene P3P-Policy erstellt werden. Dabei muss aber nicht auf eine gesamte Datenschutzerklärung für alle Webseiten zusammen, in einem für den Menschen lesbaren Format, verzichtet werden [W3C-Initiative, 2002].

Hat man diesen Punkt erledigt, kann man einen Policy-Generator auswählen. Derzeit gibt es fünf zur Auswahl. Nachdem man sich für einen Generator entschieden hat, kann die eigene Datenschutzerklärung als Orientierungshilfe für die Erstellung der P3P-Policy verwendet werden [W3C-Initiative, 2002]. Es müssen folgende Daten angeführt werden:

- *Entity*: Name, Adresse und Kontaktinformationen der Organisation.
- *Disclosure*: Gibt an, wo die schriftliche Datenschutzerklärung zu finden ist.
- *Assurances*: Eine Absicherung darüber, dass man die Datenschutzerklärung auch einhält. Darunter sind beispielsweise Zertifikate von unabhängigen Prüfungsinstitutionen zu verstehen.

- *Data Collection and Purpose*: Welche Daten gesammelt und was damit gemacht wird.

[W3C-Initiative, 2002; P3PToolbox]

Die Policy-Generatoren helfen bei der Erstellung und Veröffentlichung der P3P-Datenschutzerklärung. Bei der Erstellung sind die Felder vollständig und korrekt auszufüllen, da die Browser leere oder falsch formatierte XML.Dateien nicht akzeptieren [W3C-Initiative, 2002].

Nachdem alle benötigten Informationen in den Generator eingegeben wurden, überprüft dieser die Daten auf ausgelassene oder falsche Informationen. Wenn die Datei fehlerfrei ist kann diese als „policy1.xml“ abgespeichert werden. Sollte das Unternehmen mehrere Datenschutzerklärungen haben, können diese mit fortlaufender Nummer abgespeichert werden (zum Beispiel policy2.xml; policy3.xml; etc.) Der Generator erstellt automatisch eine Referenzdatei, die den Browser mitteilt wo die P3P-Policy zu finden ist. Diese Datei sollte unter „p3p.xml“ abgespeichert werden. Danach werden beide Dateien in das Hauptverzeichnis (Root Directory) des Servers hochgeladen [W3C-Initiative, 2002].

Das nachfolgende Beispiel stellt eine P3P-Referenzdatei in XML Code dar welche von der P3P 1.0 Spezifikation stammt:

```
<META xmlns=http://www.w3.org/2001/09/P3Pv1>
        <POLICY-REFERENCES>
                <POLICY-REF about =“/P3P/Policy3.xml“>
                        <INCLUDE>/cgi-bin/</INCLUDE>
                        <INCLUDE>/servlet/</INCLUDE>
                        <EXCLUDE>/sevlet/unknown</EXCLUDE>
                </POLICY-REF>

                <POLICY-REF about=”/P3P/Policy2.xml”>
                        <INCLUDE>/catalog/</INCLUDE>
                </POLICY-REF>
```

```
            <POLICY-REF about="/P3P/Policy1.xml">
                <INCLUDE>/*</INCLUDE>
                <EXCLUDE>/sevlet/unknown</EXCLUDE>
            </POLICY-REF>
        </POLICY-REFERENCES>
</META>
```

In diesem Beispiel verweist Policy1.xml auf alle Dateien mit Ausnahme vom „catalog“, „cgi-bin“ und „servlet“ Datenverzeichnis. Policy2.xml verweist auf alle Daten des „catalog“ Verzeichnisses und die übrigen Verzeichnisse („cgi-bin“ und „servlet“) werden von Policy3.xml mit der Ausnahme vom „servlet“ Unterverzeichnis „unknown“ abgedeckt. Da keine der P3P-Erklärungen auf „servlet/unknown“ verweist, sollte diese Gegebenheit in der für Menschen lesbaren Datenschutzerklärung erwähnt werden [W3C-Initiative, 2002].

3.1.3. Die Compact Policy

Eine P3P Compact Policy ist eine gewöhnliche P3P Datenschutzerklärung, welche mithilfe einer, für Entwickler lesbaren, Sprache zusammengefasst wurde. Diese Kürzung erfolgt, um die Byteanzahl (des HTTP Response Header[9]) der transferierten Datenmengen zu minimieren. In der Compact Policy werden dafür Kürzel (Token) verwendet, um folgende Elemente des P3P Vokabulars zu repräsentieren: Zugriff (Access), Schlichtstellen (Disputes), Rechtsmittel (Remedies), Nicht-Identifizierbar (Non-Identifiable), Zweck (Purpose), Empfänger (Recipient), Einbehaltung (Retention) und Kategorien (Categories). Bei der Analyse des Einsatzes von P3P im empirischen Teil dieser Arbeit (siehe Kapitel 4) wurden die Compact Policies der ausgewählten Unternehmen abgefragt. Nachfolgend werden daher die einzelnen Elemente in Tabelle 1 kurz näher erläutert [CompactPrivacyPolicy, 2007].

[9] Zusätzlich zum Server, welcher HTML an den Browser sendet, können auch andere Programminformationen übermittelt werden, welche für den/die NutzerIn nicht sichtbar sind. Dazu zählt auch der sog. HTTP Header, welcher Informationen über den Inhalt, der übermittelt wird, enthält. (vgl. http://www.compactprivacypolicy.org/p3p_definitions.htm Datum und Uhrzeit der Abfrage: 11. August 2008 16:17)

Tabelle 1: Elemente des P3P Vokabulars

Name des Elements	*Definition*
Zugriff (Access)	Das Access-Element gibt an, ob die Seite Zugriff auf verschiedene Arten von Informationen gewährt.
Schlichtstellen (Disputes)	Jede Policy sollte über ein Schlichtstellen-Element verfügen. Dieses Element beschreibt Lösungen in Streitfällen, wenn Datenschutzpraktiken nicht eingehalten werden.
Rechtsmittel (Remedies)	Jedes Schlichtstellen-Element kann über ein Rechtsmittel-Element verfügen, welches die Rechtsbehelfe aufführt, die im Falle eines Bruches der Datenschutzerklärung eingeschaltet werden können.
Nicht-Identifizierbar (Non-Identifiable)	Sollte die Datenschutzerklärung über ein Nicht-Identifizierbar-Element verfügen, dann beinhaltet die Compact Policy das Kürzel NID.
Zweck (Purpose)	Sollte kein NID-Element in einer Datenschutzerklärung vorhanden sein, so muss ein Zweck-Element mit einem oder mehreren Absichten der Datensammlung oder Datennutzung vorhanden sein.
Empfänger (Recipient)	Jede Datenschutzerklärung muss über ein Empfänger-Element, mit einem oder mehreren Empfängern der gesammelten Daten, verfügen.
Einbehaltung (Retention)	Ein Einbehaltungs-Element, welches angibt wie lange die gesammelten Daten aufgezeichnet bleiben, muss in jeder Datenschutzerklärung zu finden sein.
Kategorien (Categories)	Das Kategorien-Element zeigt dem/der NutzerIn und dem User-Agent wie die vorgesehene Nutzung der Daten erfolgt.

Quelle: [CompactPrivacyPolicy, 2007]

Wie weiter oben bereits angeführt, werden die einzelnen Elemente mithilfe von Kürzeln, welche aus einem dreistelligen Buchstabencode bestehen, dargestellt. Ein Beispiel für die Kürzel wäre „NOI“ im Zugriff-Element, welches bedeutet, dass keine identifizierbaren Daten, gemäß Compact Policy, gesammelt werden. Zusätzlich können die Kürzel auch mit einem optionalen Attribut, welches ein kleiner Buchstabe ist, versehen werden. Diese optionalen Attribute kodieren den Wert eines erforderlichen Attributs einer „vollen“ P3P Policy: der Wert kann „a“, „i“ und „o“ sein, welches bedeu-

tet, dass das geforderte Attribut in der dazugehörenden P3P Policy auf „immer“ (always), „anmelden beziehungsweise eintragen“ (opt-in) und „abmelden beziehungsweise austragen“ (opt-out) entsprechend gestellt werden muss. Der „a“-Wert bedeutet, dass es keine Möglichkeit für den/die NutzerIn gibt sich von der Nutzung der gesammelten Daten an- oder abzumelden. Der Wert „i“ gibt an, dass der/die NutzerIn sich für die Nutzung anmelden kann und „o“ bedeutet, dass man sich von der Verarbeitung beziehungsweise Sammlung der Daten abmelden kann [CompactPrivacyPolicy, 2007].

Nachfolgend werden die Abkürzungen der einzelnen Compact Policy Elemente, welche in Kapitel 4.1 bei der Analyse abgefragt wurden, erläutert [CompactPrivacyPolicy, 2007]:

Zugriff: Dieses Element gibt an, ob und wenn ja, welche Daten vom Unternehmen oder Dritten gesammelt werden.
NOI = Die Webseite sammelt keine identifizierbaren Daten
ALL = Zugriff auf alle übermittelten und identifizierbaren Daten.
CAO = Identifizierbare Kontaktinformationen und andere identifizierbare Daten: Zugriff auf online und physische Kontaktinformationen, sowie andere identifizierbare Daten.

Schlichtstellen: Sollte es zu einem Bruch bezüglich der Angaben in der Datenschutzerklärung oder Compact Policy kommen, dann nennt das Schlichtstellen-Element Organisationen, die in solchen Belangen verständigt werden können. Diese Stellen handeln oft als unabhängige Vermittler in Konfliktsituationen und sind eine Anlaufstelle für die Nutzer.
DSP = Die Datenschutzerklärung beinhaltet Organisationen im Falle eines Konflikts.

Rechtsmittel: Dieses Element einer Compact Policy nennt Rechtsmittel die im Falle eines Bruchs der Datenschutzerklärung, eingesetzt werden können.
COR = Fehler oder unrechtmäßige Handlungen in Verbindung mit der Datenschutzerklärung werden vom Service behoben.
LAW = Rechtsmittel für Brüche der Datenschutzklausel werden aufgrund des Rechts, welches in der menschenlesbaren Beschreibung erwähnt wird, ermittelt.

Zweck: Das Zweck-Element gibt an, aus welchem Grund Daten gesammelt werden.
CUR = Informationen werden für die Vervollständigung einer Aktivität, für die sie bereitgestellt wurden, benutzt.
ADM = Daten werden für den technischen Support der Webseite und des Computersystems benutzt.
DEV = Informationen werden zur Verbesserung, Auswertung oder zur Nachbearbeitung der Seite, des Services oder der Produkte benutzt.
TAI = Die gesammelten Daten werden für die Maßschneiderung oder Modifizierung der Inhalte oder des Designs der Webseite benutzt.
PSA = Informationen werden zur Schaffung oder Erstellung einer Aufzeichnung eines bestimmten Individuums oder Computers, welches mit einer Pseudonym-Kennung (Bezeichnung) verbunden ist, ohne dabei identifizierbare Daten (wie Name, Adresse, Telefonnummer oder Email-Adresse) damit zu verbinden, genutzt. Dieses Profil wird dazu benutzt, um Angewohnheiten, Interessen oder andere Charakteristika von Individuen aufzuzeichnen, um diese Daten für Untersuchungen, Analysen und Berichterstattungen nutzen zu können. Dabei wird nicht versucht Individuen zu identifizieren.
PSD= Informationen werden zur Schaffung oder Erstellung einer Aufzeichnung eines bestimmten Individuums oder Computers, welches mit einer Pseudonym-Kennung (Bezeichnung) verbunden ist, ohne identifizierbare Daten (wie Name, Adresse, Telefonnummer oder Email-Adresse) mit dieser Kennung zu verbinden. Dieses Profil wird dazu benutzt um Entscheidungen, die direkt das Individuum betreffen, zu fällen, aber nicht, um ein bestimmtes Individuum zu identifizieren.
CON = Informationen können dazu benutzt werden, um mit dem Individuum, durch Kommunikationsmittel, außer dem Telefon, in Kontakt zu treten, um Produkte oder Services anzubieten. Dies inkludiert Besucher über Updates der Webseite zu verständigen.
CUS= Dieser Token wurde u.a. in der Compact Policy von Microsoft abgerufen, zu diesem konnte aber auf der offiziellen Seite von W3C keine Definition gefunden werden.
IVA = Informationen können dazu benutzt werden Angewohnheiten, Interessen oder andere Charakteristika des Individuums zu ermitteln und mit identifizierbaren Daten zu kombinieren, um damit Forschungen, Analysen und Berichterstattungen zu machen.

IVD = Informationen können dazu benutzt werden Angewohnheiten, Interessen oder andere Charakteristika des Individuums zu ermitteln und mit identifizierbaren Daten zu kombinieren, um damit Entscheidungen zu fällen, welche direkt das Individuum betreffen.
TEL = Informationen können dazu genutzt werden, um mit dem Individuum via Telefonanruf in Kontakt zu treten, um Produkte oder Services zu bewerben.
HIS = Informationen können archiviert oder gespeichert werden, um die Sozialgeschichte (social history) zu bewahren, wie es von einem existierenden Gesetz oder einer Policy vorgeschrieben wird.
OTP = Informationen können in anderer Weise, als bei den oberen Definition erfasst, genutzt werden.

Empfänger: In diesem Element wird die Frage beantwortet, wer die gesammelten Daten verarbeitet und an wen sie weitergegeben werden.
OUR = Das Unternehmen selbst und/oder juristische Personen welche als deren Agenten handeln oder juristische Personen für die das Unternehmen als Agent arbeitet.
SAM= Juristische Personen die denselben Handelspraktiken folgen.
OTR = Rechtssubjekte welche anderen Praktiken folgen.
DEL = Lieferservices die anderen Praktiken folgen.
UNR = Dritte ohne Bezug, von welchen die Datennutzungspraktiken vom Serviceanbieter nicht bekannt sind.

Retention/Einbehaltung: Das Retentions-Element gibt an, wie lange die Daten der Nutzer gespeichert bleiben.
IND = Informationen werden für unbestimmte Zeit behalten. Das Fehlen einer Retention-Policy würde sich unter dieser Option widerspiegeln.
BUS = Die Beibehaltung der Daten wird in den Geschäftspraktiken angegeben. Eine Webseite muss über eine Policy bezüglich der Dauer der Speicherung verfügen, in der angegeben wird, nach welcher Zeit die Daten vernichtet werden. Diese Policy muss in der für den Menschen lesbaren Datenschutzerklärung inkludiert oder verlinkt sein.
LEG = Die Informationen werden beibehalten, um einen angegebenen Zweck zu erfüllen, aber die Beibehaltungszeit ist länger, weil eine gesetzliche Forderung oder

Haftung dies vorschreibt. Webseiten müssen eine Retention Policy haben, in der der Zeitplan bis zur Löschung der Informationen angegeben werden muss. Diese Policy muss inkludiert oder in der für den Menschen lesbaren Datenschutzerklärung verlinkt sein.
STP = Informationen werden aufbewahrt, um den angegeben Zweck zu erfüllen. Dies benötigt die Löschung der Informationen zur ehest möglichen Zeit. Webseiten müssen eine Retention Policy mit einem Zeitplan der Löschung der Informationen besitzen. Die Policy muss in der für den Menschen lesbaren Datenschutzerklärung inkludiert oder verlinkt sein.

Kategorien: Dieses Element gibt Aufschlüsse über die Nutzung der Daten.
UNI = Bezeichnungen die von der Webseite oder einem anderen Service ausgestellt wurden.
COM = Informationen über das Computersystem welches vom Individuum benutzt wird, um auf das Netzwerk zuzugreifen. Darunter fallen Daten wie die IP-Nummer, der Domain-Name, welcher Browser verwendet wird oder das Betriebssystem.
NAV = Daten die durch das Betrachten der Webseite passiv entstehen. Darunter fallen Informationen darüber welche Seiten besucht und wie lange diese betrachtet wurden.
CNT = Wörter und Ausdrücke die in der Kommunikation aufscheinen, wie zum Beispiel der Text einer Email, Bulletin Board Posts oder Chat Room Kommunikation.
PRE = Daten über Neigungen und Abneigungen eines Individuums, wie zum Beispiel die Lieblingsfarbe oder der Musikgeschmack.
PUR = Informationen die aktiv durch den Kauf eines Produktes oder Services entstehen, einschließlich der Zahlungsmethode.
INT = Daten welche aktiv generiert wurden von oder welche explizite Interaktionen mit dem Service Provider durch die Seite wiederspiegeln, wie zum Beispiel Anfragen an eine Suchmaschine oder Aufzeichnungen der Account-Aktivität.
ONL = Informationen die es ermöglichen ein Individuum im Internet zu kontaktieren oder zu lokalisieren, wie zum Beispiel die Email-Adresse. Oftmals sind diese Informationen unabhängig vom Computer von dem aus auf das Netzwerk zugegriffen wird.
PHY = Informationen die es erlauben ein Individuum in der physischen Welt zu kontaktieren oder zu lokalisieren, wie zum Beispiel die Telefonnummer oder Adresse.

DEM = Daten über Charakteristika eines Individuums, wie zum Beispiel Geschlecht, Alter, Einkommen, etc.
STA = Mechanismen um eine zustandshafte Sitzung[10] mit einem/r NutzerIn beizubehalten oder Nutzer automatisch wiedererkennen zu können, welche eine Seite besucht oder auf einen bestimmten Inhalt zuvor zugegriffen haben, wie zum Beispiel HTTP Cookies.
GOV = Bezeichnungen die von der Regierung zur stetigen Identifizierung eines Individuums ausgegeben werden. (zum Beispiel Sozialversicherungsnummer)
OTC = Andere Datentypen welche nicht durch die obigen Definition erfasst wurden.

3.1.4. Vor- und Nachteile

Ein großer Vorteil für die Internet-Nutzer ist, dass man P3P-Agenten kostenlos im Internet downloaden kann. Dabei gibt es verschiedene technische Konzepte über die man einen P3P-Agenten installieren kann. In den Browser bereits eingebaute P3P-Agenten bieten folgende Browser an z.B. Mozilla Browser ab der Version 1.4, Netscape Navigator ab Version 7.0 oder Microsoft Internet Explorer ab Version 6.0. Ein anderes Konzept wäre der AT&T Privacy Bird, welcher ein Plug-In für den Microsoft Internet Explorer ab Version 5.01 ist, um auch ältere Browsern um die P3P-Funktion zu erweitern. Eine weitere Alternative wäre der P3P-Agent JRC Proxy, der, wie der Name schon andeutet, ein Proxy-Server ist. Nachdem der P3P-Agent installiert wurde, muss der Internet-Nutzer nur noch seine eigenen Datenschutzansprüche festlegen. Bei der Konfiguration sind Ausmaß sowie die Art der Festlegung der Präferenzen davon abhängig, welchen P3P-Agenten man verwendet [Möller, Datenschutz mit P3P, 2003].

Grundsätzlich ist das Anbieten einer Datenschutzerklärung im P3P-Format auch für den Anbieter kostenlos. Es können aber Kosten bei der Erstellung und Umsetzung einer rechtsgültigen Datenschutzerklärung in das P3P-Format entstehen [Möller, Datenschutz mit P3P, 2003].

[10] Zustandshaft bedeutet in diesem Zusammenhang, dass der jeweilige Ist-Zustand gespeichert wird, sodass zuvor getätigte Einstellungen übernommen werden können.
(vgl. http://dict.leo.org/forum/viewUnsolvedquery.php?idThread=31950&idForum=2&lp=ende&lang=de Datum und Uhrzeit der Abfrage: 14. August 2008 14:15)

Folgende Vorteile ergeben sich aus der Benutzung eines P3P-Agenten für Internet-Nutzer [Möller, Datenschutz mit P3P, 2003]:

- Der Nutzer umgeht das oft zeitraubende Durchlesen der Datenschutzerklärung des Anbieters, indem er/sie seine/ihre Präferenzen im Vorhinein festlegt. Der P3P-Agent (bspw. der Browser) zeigt ausschließlich Webseiten an, die mit den Benutzer-Präferenzen übereinstimmen. Werden vom Anbieter mehr Daten gesammelt als der Nutzer im Vorhinein freigegeben hat, gibt der Agent eine Warnmeldung aus und die Seite wird nicht geladen.
- Die Datenschutzerklärung einer Webseite wird für den Menschen lesbar und übersichtlich zusammengefasst.
- Ist die Datenschutzerklärung in einer anderen Sprache verfasst worden, übermittelt der P3P-Agent die Zusammenfassung in der Sprache, die der Internetsurfer eingestellt hat und übersetzt dabei die wichtigsten Aussagen.
- Die oftmals lange dauernde Suche nach der Datenschutzerklärung einer Webseite wird durch die Möglichkeit des Abrufs durch einen Link ersetzt.
- Um bestimmte Rechte geltend machen zu können, wie z.B. einen Widerruf, werden die verantwortlichen Ansprechpartner aufgelistet.
- Sämtliche Softwarefunktionen können aufgrund des maschinenlesbaren Formats der Datenschutzerklärung, anhand der Praktiken des Anbieters in Bezug auf die Verarbeitung der Daten, gesteuert werden, z.B. Annahme von Cookies. Werden Optionen bei den Datenschutzansprüchen seitens des Internetsurfers geändert, werden diese ohne zeitliche Verzögerung übernommen und berücksichtigt.

Die Nutzung von P3P als Webanbieter schafft für die Internet-Nutzer wichtige Transparenz (siehe oben Kapitel 2.3.2 Besonderheit des Vertrauensbegriffs im E-Commerce). Dadurch werden sämtliche Handlungen die mit Datenschutz in Verbindung stehen offengelegt und es wird eine Vertrauensbasis für die Kunden beziehungsweise Besucher der Webseite geschaffen beziehungsweise diese sogar gestärkt. Dabei muss aber berücksichtigt werden, dass die in der P3P-Datenschutzerklärung beschriebene Verarbeitung der personenbezogenen Daten der Internetsurfer den rechtlichen Mindeststandards entsprechen oder wenn möglich sie sogar übersteigen. Dieses Verhalten kann wiederum das Vertrauen steigern. Mithilfe einer unabhängigen rechtlichen Überprüfung kann der Anbieter der Webseite

sich die Konformität bestätigen lassen und diese dann nach außen kommunizieren. Somit ist eine P3P-Datenschutzerklärung eine automatisierte und kostengünstige Maßnahme, im Vergleich zu anderen Marketingmaßnahmen, um das Vertrauen bei den Besuchern der Webseite zu bestärken [Möller, Datenschutz mit P3P, 2003].

P3P ermöglicht den Austausch von Informationen über die Verarbeitung personenbezogener Daten und macht diese dadurch überschaubarer. Zu beachten ist dabei aber, dass die Zulässigkeit der Verarbeitung dabei nicht überprüft wird. Teilweise gibt der P3P-Standard Vorgaben für gewisse Datenverarbeitungspraktiken vor, diese sind dann für den Anbieter der P3P-Datenschutzerklärung bindend. Wird die P3P-Plattform verwendet, muss der Webseitenanbieter eine Konformitätszusage akzeptieren. Das heißt dass P3P zwar eine gute Möglichkeit ist, um dem Nutzer aufzuzeigen welche Praktiken der Webseitenanbieter im Bezug auf die Verarbeitung der personenbezogenen Daten anwendet. Jedoch müssen lediglich die P3P-Standards vom Anbieter eingehalten werden, die zwar oft über die Mindeststandards einiger Länder hinausgehen, aber keinen ausreichenden rechtlichen Schutz bieten [Möller, Datenschutz mit P3P, 2003].

Das derzeitige Ziel von P3P ist es als technischer Standard, ein gewisses Maß an Transparenz über die Datenverarbeitung von Internetnutzern zu ermöglichen sowie Informationen über den Datenschutz einheitlich und automatisiert auszutauschen. Bei der Durchsetzung des Datenschutzrechtes kann P3P insofern helfen, als dass es die Verantwortlichen aufzeigt. Aufsichtsbehörden könnten mithilfe von P3P beispielsweise auch effizientere Online-Überprüfungen durch das automatische Abrufen der Datenschutzerklärungen durchführen [Möller, Datenschutz mit P3P, 2003].

3.1.5. Kritik

Häufig kritisieren Gegner von P3P, dass es den Benutzern keinen direkten Einfluss, wie mit den persönlichen Daten umgegangen wird, ermöglicht. Diesen Anspruch erhebt P3P zwar nicht, aber Benutzer könnten ein zu hohes Vertrauen in Webseiten, die eine P3P-Datenschutzerklärung anbieten, bekommen. Viele Nutzer könnten glauben, dass P3P ein komplettes Datenschutz-Sicherheitspaket darstellt und man sich keinerlei Sorgen mehr über den Schutz der eigenen Privatsphäre machen muss. P3P ist lediglich ein Tool für den Selbstdatenschutz im Internet, welches dem Benutzer Transparenz über die Datenschutzpraktiken von Webseitenanbietern ermöglicht.

Ein weiterer Kritikpunkt an P3P ist auch, dass es ein Selbstkontroll-Tool ist und der Internetsurfer sich darauf verlassen muss, dass der Anbieter der Webseite wahrheitsgemäße Angaben macht und den in der Datenschutzerklärung zugestandenen Schutz beziehungsweise zugesprochene Standards auch einhält. Es werden auch keine Minimumstandards für den Datenschutz seitens P3P festgelegt. P3P behauptet auch gar nicht diesen Schutz, bezogen auf die Kritikpunkte, zu ermöglichen. P3P wird deshalb so stark kritisiert, da es, wie oben schon erwähnt, dem Internet-Nutzer eine falsche Sicherheit suggeriert, die gar nicht vorhanden ist und deren Implementierung auch gar nicht geplant ist [Ulber, 2004; Möller, Datenschutz mit P3P, 2003 und P3PToolbox].

3.2. APPEL

APPEL („ A P3P Preference Exchange Language“) ist eine standardisierte Sprache, die es dem Benutzer ermöglicht seine Präferenzen bezüglich des eigenen Datenschutzes zu beschreiben. Wie P3P stellt APPEL eine weitere Möglichkeit für den Endnutzer dar, um persönlichen Daten aktiv selbst zu schützen. Zu den Unterschieden beziehungsweise Ergänzungen zu P3P siehe die Kapiteln 3.2.1 und 3.2.3, welche auf die Funktionsweise und Ziele von APPEL eingehen. Das W3C publizierte im Jahr 2002 erstmals ein Konzept zu APPEL und stellte es als Ergänzung zur P3P 1.0 Spezifikation vor. Ein Nutzer kann seine Datenschutzpräferenzen mithilfe einer Reihe von Präferenz-Regeln (sog. „Ruleset“) ausdrücken. Diese Rulesets können dann vom User-Agent dazu verwendet werden, um automatisierte oder halb-automatisierte Entscheidungen bezüglich der Akzeptanz der maschinenlesbaren P3P-Datenschutzerklärung einer Webseite zu machen [Cranor, Langheinrich, & Marchiori, 2002].

3.2.1. Funktionsweise

Der Prozess, der die Präferenzen des Nutzers (beispielsweise ein APPEL Ruleset) mit der P3P-Policy des Anbieters vergleicht, wird als “Rule Evaluator” bezeichnet und wird durch eine P3P Applikation aktiviert. Diese Applikation gibt dem Rule Evaluator verschiedene Teile der „Evidence“, das heißt die Datenübersicht der P3P-Policy, falls vorhanden eine nutzerspezifische Datenübersicht und ein Ruleset um diese zu bear-

beiten. Die Evidence beinhaltet ein URI[11] und eine P3P-Policy des Anbieters [Cranor, Langheinrich, & Marchiori, 2002].

Der Geltungsbereich einer „Rule“ (eine formale Bezeichnung für die Nutzerpräferenzen) wird durch das Element <appel:RULE> festgelegt. Der Rule Evaluator fragt das Verhalten der entsprechenden Präferenz mithilfe der Attribute „Behavior“ und „Prompt“ ab. APPEL unterstützt drei Behavior-Attribute: „request“, „limited“ und „block“, sowie ein alternatives „prompt“ Attribut (zum Beispiel wenn keine anwenderspezifische Reaktion vorhanden ist). Der Rule Evaluator kann dann unterschiedlich antworten: er gibt einen Erklärungs-String (explanation string), welcher für den Nutzer übersichtlich dargestellt werden kann, aus, eine Aufforderung an den Nutzer eine Entscheidung zu treffen, den Namen einer Person und/oder die Rule die gepasst hat (the rule that fired). Die entsprechende Applikation interpretiert die Ausgabe des Behaviors folgendermaßen [Cranor, Langheinrich, & Marchiori, 2002]:

- *request*: Die abgerufene Evidence ist akzeptabel. Wenn ein URI vorhanden ist, wird die dazugehörige Ressource abgerufen [Cranor, Langheinrich, & Marchiori, 2002].
- *limited*: Die abgerufene Evidence ist teilweise akzeptabel. Wenn ein URI vorhanden ist, kann auf die Ressource zugegriffen werden. Der Zugriff auf diese Ressource sollte aber insofern limitiert sein, als dass nur die absolut notwendigen „Request Headers“ (Abfrage-Titel) abgerufen und der Rest blockiert wird [Cranor, Langheinrich, & Marchiori, 2002].
- *block*: Das abgerufene Evidence ist nicht akzeptabel. Wenn ein URI vorhanden ist, sollte auf keinen Fall die Ressource abgerufen werden. Wurde jedoch schon beim Abruf der P3P-Policy auf die Ressource zugegriffen, dann muss das verwendete Programm entscheiden, welche Informationen dem Nutzer angezeigt werden [Cranor, Langheinrich, & Marchiori, 2002].

Wie bereits erwähnt, gibt es auch die Möglichkeit eines prompt Attributs, dieses wird von Applikationen folgendermaßen interpretiert:

[11] „URIs werden zur Bezeichnung von Ressourcen (wie Webseiten, sonstigen Dateien, Aufruf von Webservices, aber auch z. B. E-Mail-Empfängern) im Internet und dort vor allem im WWW eingesetzt.“ (vgl. http://de.wikipedia.org/wiki/Uniform_Resource_Identifier Datum und Uhrzeit der Abfrage: 01.Juli 2008 15:50)

- *prompt = „no“:* Das Verhalten welches im Behavior-Attribut festgelegt wurde, wird durchgeführt, ohne dabei den Nutzer nach Eingaben zu fragen. Dennoch können Informationen über die Auswertung der Präferenzen in verschiedenster Art angezeigt werden (zum Beispiel eine Nachricht in der Statusleiste, Audiosignal, etc.) [Cranor, Langheinrich, & Marchiori, 2002].
- *prompt = „yes“:* In diesem Fall muss der Nutzer zu einer Entscheidung über das Verhalten, welches durch die Rule ausgelöst wurde, aufgefordert werden. Der verwendete User-Agent zeigt bei diesem Vorgang immer die passende Nachricht aus dem dazugehörigen „promptmsg“-Attribut an [Cranor, Langheinrich, & Marchiori, 2002].

Die Auswertung der Rules erfolgt in Bezug auf die vorhandene Evidence. Eine Rule wird nur dann als „true“ (richtig) angesehen, wenn alle Ausdrücke erfüllt sind. Jede Rule im Ruleset wird in der Reihenfolge in der sie aufscheint ausgewertet. Wenn eine Rule als true ausgewertet wird, dann wird das dazu passende Verhalten retourniert und die Auswertung endet. Daher sollte der verwendete User-Agent zuerst sämtliche Rules durcharbeiten, bevor die Auswertung beendet wird [Cranor, Langheinrich, & Marchiori, 2002].

Nachfolgend soll ein Anwendungsbeispiel des W3C Working Draft - APPEL1.0 den soeben beschriebenen Prozess verständlicher machen.

3.2.2. Anwendungsbeispiel für die Nutzung von APPLE

Zuerst werden die Präferenzen (zur Erläuterung sind sie sehr simpel gehalten) der Nutzerin für dieses Beispiel aufgelistet:

1. Wenn persönliche Informationen an Dritte weitergegeben werden, soll die Abfrage diese blockieren [Cranor, Langheinrich, & Marchiori, 2002].
2. Die Nutzerin hat nichts gegen die Aufzeichnung des „click-stream“[12] und der Informationen über den User-Agent, vorausgesetzt die Webseite sammelt keine anderen Informationen und es wird eine Absicherung (zum Beispiel Datenschutzgütesiegel, etc.) angeboten [Cranor, Langheinrich, & Marchiori, 2002].

[12] Mit Clickstream-Analyse (click-stream, Web Analytics) „bezeichnet man die Sammlung und Auswertung des Verhaltens von Besuchern auf Websites. Typischerweise wird untersucht, woher die Besucher kommen, welche Bereiche aufgesucht werden und wie oft welche Seiten gesehen werden.“ (vgl. http://de.wikipedia.org/wiki/Web_Analytics Datum und Uhrzeit der Abfrage: 01.Juli 2008 17:12)

3. Die Nutzerin hat kein Problem damit ihren Vor- und Nachnamen preiszugeben, aber nur wenn diese nicht für Marketingzwecke verwendet werden. Sie fordert eine Absicherung von „PrivacyProtect“ und „TrustUs“ bevor sie jeglicher Erklärung glaubt [Cranor, Langheinrich, & Marchiori, 2002].
4. Sie akzeptiert jede Datenabfrage, wenn sie sich auf der Webseite ihre Bank http://www.my-bank.com befindet, solange die Daten nicht an Dritte weitergegeben werden [Cranor, Langheinrich, & Marchiori, 2002].
5. Jede andere Anfrage für einen Datentransfer soll durch eine Warnmeldung an die Nutzerin mitgeteilt werden, um anzuzeigen dass es sich um einen Konflikt mit ihren Datenschutzpräferenzen handelt und wird von Fall zu Fall von der Benutzerin selbst entschieden [Cranor, Langheinrich, & Marchiori, 2002].

In der nachfolgenden Tabelle werden die Datenschutzpräferenzen der Nutzerin gemeinsam mit den passenden Attributen und Aktionen dargestellt. Jede Reihe stellt eine geordnete Rule aus dem Ruleset dar. Zu beachten ist, dass es in der Tabelle sowohl leere Felder als auch Felder mit einem *-Symbol gibt. Wenn eine Zelle vom Nutzer leergelassen wurde, dann besteht kein Interesse beim jeweiligen Attribut, egal ob es in der Policy aufscheint oder nicht. Wenn ein * in einer Zelle zu finden ist, dann ist dem Nutzer egal welchen Wert das Attribut hat, aber es muss zumindest irgendein Wert aufscheinen. Beispielsweise ist die Zelle in der 2. Reihe von Tabelle 2 ohne Wert und daher besteht seitens der Nutzerin kein Interesse bezüglich des Zwecks (purpose) der Sammlung der clickstream Daten. In der Streitfragenspalte (Disputes) wird irgendeine Form von Information verlangt, da dort ein *-Symbol zu finden ist [Cranor, Langheinrich, & Marchiori, 2002].

Tabelle 2: Beispiel einer Datenschutzpräferenz bei APPEL

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

Quelle: [Cranor, Langheinrich, & Marchiori, 2002]

Die in Tabelle 2 dargestellten Präferenzen können in ein APPEL Ruleset umgesetzt werden. Es gibt fünf Regeln, um die Policy des Anbieters zu bearbeiten. Eine „block“-Regel (beispielsweise eine Rule mit dem String „block“ in ihrem Behavior-Attribut) wird jede Policy die spezifiziert, dass persönlichen Daten an Dritte weitergegeben werden, ablehnen. Wenn auf die Webseite www.my-bank.com zugegriffen wird, dann kommt eine zweite Regel zur Geltung, in der diese URL bereits vordefiniert wurde und somit die Daten an die Bank freigegeben werden. Als nächstes wird die Request-Regel überprüfen, ob clickstream Daten die nicht mit der Nutzerin in Verbindung gebracht werden können und/oder Informationen des User-Agents (zum Beispiel Version des Browsers, Betriebssystem, etc.) gesammelt werden und wenn Dispute Informationen vorhanden sind, ohne Warnungen die Abfragen fortsetzen. Eine Request-Rule mit dem Attribut prompt=“yes“ überprüft ob der Name für Nicht-Marketingzwecke abgefragt wird und wird möglicherweise eine Nachricht an die Nutzerin ausgeben, dass eine Webseite ihren Namen unter akzeptablen Umständen sammelt. Sollte keine Rule auf die Anbieter-Policy passen, dann fällt dies in den Geltungsbereich der Limited-Rule (mit dem Attribut prompt=“yes“). Diese lässt die Nutzerin entscheiden ob die Policy akzeptabel ist, mit der Warnung dass keine der aufgestellten Rules gepasst hat [Cranor, Langheinrich, & Marchiori, 2002].

Die nachfolgende Abbildung 8 zeigt ein simples Beispiel einer Ruleset in APPEL aus dem W3C Working Draft - APPEL1.0:

Abbildung 8: Beispiel einer Ruleset in APPEL 1.0

```
001: <appel:RULESET
xmlns:appel="http://www.w3.org/2002/04/APPELv1"
002:              xmlns:p3p="http://www.w3.org/2000/12/P3Pv1"
003:              crtdby="W3C" crtdon="1999-11-03T09:21:32-05:00">

004:   <appel:RULE behavior="block" description="Service collects personal
005:                 data for 3rd parties">
006:     <p3p:POLICY>
007:       <p3p:STATEMENT>
008:         <p3p:DATA-GROUP>
009:           <p3p:DATA>
010:             <p3p:CATEGORIES appel:connective="or">
011:               <p3p:physical/>
012:               <p3p:demographic/>
013:               <p3p:uniqueid/>
014:             </p3p:CATEGORIES>
015:           </p3p:DATA>
016:         </p3p:DATA-GROUP>
017:         <p3p:RECIPIENT appel:connective="or">
018:           <p3p:same/>
019:           <p3p:other-recipient/>
020:           <p3p:public/>
021:           <p3p:delivery/>
022:           <p3p:unrelated/>
023:         </p3p:RECIPIENT>
024:       </p3p:STATEMENT>
025:     </p3p:POLICY>
026:   </appel:RULE>

027:   <appel:RULE behavior="request"
028:              description="My Bank collects data only for itself
029:                          and its agents">
030:     <appel:REQUEST-GROUP>
031:       <appel:REQUEST uri="http://www.my-bank.com/*"/>
032:     </appel:REQUEST-GROUP>
033:     <p3p:POLICY>
034:       <p3p:STATEMENT>
035:         <p3p:RECIPIENT appel:connective="or-exact">
036:           <p3p:ours/>
037:         </p3p:RECIPIENT>
038:       </p3p:STATEMENT>
039:     </p3p:POLICY>
040:   </appel:RULE>

041:   <appel:RULE behavior="request"
042:              description="Service only collects clickstream data">
043:     <p3p:POLICY>
044:       <p3p:STATEMENT>
045:         <p3p:DATA-GROUP appel:connective="or-exact">
046:           <p3p:DATA ref="#dynamic.http.useragent"/>
047:           <p3p:DATA ref="#dynamic.clickstream.server"/>
048:         </p3p:DATA-GROUP>
049:       </p3p:STATEMENT>
050:       <p3p:DISPUTES-GROUP>
051:         <p3p:DISPUTES service="*"/>
```

```
052:      </p3p:DISPUTES-GROUP>
053:    </p3p:POLICY>
054:  </appel:RULE>

055:  <appel:RULE behavior="request" prompt="yes"
056:            promptmsg="Service only collects your name
057:                      for non-marketing purposes (assured)

058:                      Do you want to continue?">
059:    <p3p:POLICY>
060:      <p3p:STATEMENT>
061:        <p3p:PURPOSE appel:connective="or-exact">
062:          <p3p:current/>
063:          <p3p:admin/>
064:          <p3p:customization/>
065:          <p3p:develop/>
066:        </p3p:PURPOSE>
067:        <p3p:DATA-GROUP appel:connective="or-exact">
068:          <p3p:DATA ref="#user.name.*"/>
069:        </p3p:DATA-GROUP>
070:      </p3p:STATEMENT>
071:      <p3p:DISPUTES-GROUP>
072:        <p3p:DISPUTES service="http://www.privacyprotect.com"/>
073:        <p3p:DISPUTES service="http://www.trustus.org"/>
074:      </p3p:DISPUTES-GROUP>
075:    </p3p:POLICY>
076:  </appel:RULE>

077:  <appel:RULE behavior="limited" prompt="yes"
078:    promptmsg="Suspicious Policy.  Do you want to continue (limited access)?">
079:    <appel:OTHERWISE/>
080:  </appel:RULE>

081: </appel:RULESET>
```

Quelle: Cranor, Langheinrich, & Marchiori, 2002

Mithilfe der Zeilennummerierung kann das APPEL Ruleset übersichtlich in Tabelle 3 erklärt werden. An dieser Stelle wird nur kurz auf einige Aspekte zum Aufbau der Ruleset eingegangen.

Tabelle 3: Erklärung des Anwendungsbeispiels einer APPEL Ruleset

Zeile	Erklärung
000 – 081	Dies ist das gesamte APPEL Ruleset. Normalerweise wird ein Ruleset beim User-Agent eingestellt. Das <appel:RULESET> Element kann noch mit weiteren Informationen wie Name des Autors oder Erstellungsdatum ergänzt werden.
004 – 026	Die „block“ Rule: Wie schon weiter oben erwähnt gibt es bei APPEL drei verschiedene Behavior-Regeln: „request“, „block“ und „limited“. Jede Regel

	kann wiederum mit einem Prompt-Attribut (prompt="yes") versehen werden und somit den Nutzer zu einer Entscheidung auffordern. Jede Rule besteht aus einem <appel:RULE> Element welches eine Vielzahl von Ausdrücken ummantelt. Die Rule kann durch ein Set von Attributen angereichert sein. In diesem Beispiel wird das „description field" (Beschreibungsfeld) mit einer für den Menschen lesbaren Erklärung versehen (zum Beispiel „Service only collects clickstream data", dass heißt es werden nur clickstream Daten gesammelt). Wenn die Rule passt, kann diese Nachricht vom User-Agent angezeigt werden. Soll der Nutzer zu einer Entscheidung aufgefordert werden, gibt es ein eigenes Aufforderungselement namens „promptmsg", durch das eine passende Frage festgelegt werden kann.
006 – 025	Die meisten APPEL Rules verfügen über eine P3P-Policy innerhalb des <RULE> Elements. Elemente und Attributswerte welche mit der Rule übereinstimmen sollen, werden in der Policy angeführt. Durch das *-Symbol werden Bereich für die Werte festgesetzt.
007 – 024	Die Regel "block" sollte dann aktiviert werden (die Policy ablehnen) wenn der Service, auf das zugegriffen wird, nach persönlichen Daten (<DATA> Element in den Kategorien „physical", „demographic" oder „uniqueid") fragt, welche an Dritte weitergegeben werden (Das Feld <RECIPIENT> stimmt mit <same/>; <other-recipient/> oder <published/> überein).
027 – 040	Diese "request" Regel fährt mit der Bearbeitung einer Policy nur dann fort, wenn diese aus einer Webressource von www.my-bank.com stammt. Dies funktioniert mithilfe des <appel:REQUEST> Element welches "false" ausgibt, außer wenn der User-Agent eine Ressource vom URI, das aufgelistet wurde, abruft. Dadurch können auf einfache Weise Regeln vom Nutzer geschrieben werden, die nur auf bestimmte Domains beschränkt sind.
041 – 054	In diesem Fall wird die „request" Regel nur dann mit der Abfrage fortfahren, wenn die Anbieter-Policy angibt, dass nur Informationen über den User-Agent und/oder clickstream Daten gesammelt werden. Wie hier gut zu sehen ist, müssen die Elemente <PURPOSE> und <RECIPIENT> nicht angegeben werden, obwohl sie in einer P3P-Policy verlangt werden.
050 –	Der Nutzer verlangt durch das Dispute-Element eine Absicherung seitens

052	einer vertrauenswürdigen Organisation, damit die Services des Anbieters mit der Datenschutzerklärung konform gehen.
055 – 076	Obwohl die Nutzerin mit der Abfrage ihres Namens für Nicht-Marketingzwecke die durch TrustUs und PrivacyProtect abgesichert sind, einverstanden ist, möchte sie mithilfe der „prompt and request“ Regel über jeden Transfer ihrer persönlichen Daten informiert werden.
077 – 080	Die „limited“ Regel wird nur dann aktiviert, wenn alle anderen Regeln nicht mit der Policy des Anbieters übereinstimmen. Dies funktioniert nur durch die spezielle Anordnung im Ruleset.
079	Der Ausdruck <OTHERWISE> soll eine Regel darstellen die immer „true“ ausgibt. Deshalb sollte <OTHERWISE> immer am Ende vom Ruleset angeordnet sein, da alle nachfolgenden Regeln nicht mehr bearbeitet werden. Eine leere Regel wird nie eine Übereinstimmung bringen.

Quelle: [Cranor, Langheinrich, & Marchiori, 2002]

3.2.3. Ziele einer „P3P Preference Exchange Language“

Die P3P 1.0 Spezifikation bietet zwar eine Syntax um Datenschutzerklärungen zu beschreiben und einen Mechanismus der es ermöglicht das diese Erklärungen mit Webressourcen in Verbindung treten, aber es fehlen vor allem Anforderungen an ein grafisches Nutzer-Interface (GUI – graphical user interface) oder die Möglichkeit des Einsatzes von sog. „Trust Engines“. Unter „Trust Engines“ sind Datenbanken zu verstehen, die es dem Nutzer ermöglichen vordefinierte Präferenzen in einer Ruleset-Datei zu importieren und installieren. Nachfolgend werden Vorteile die durch den Einsatz von Nutzer-Interfaces oder Trust Engines möglich sind aufgezeigt [Cranor, Langheinrich, & Marchiori, 2002]:

- *Gemeinsame Benutzung und die Möglichkeit der Installation von Rulesets:* Für Endnutzer kann es recht schwierig sein anspruchsvolle Präferenzen selbst zu bestimmen, auch dann wenn ein ausgeklügeltes Interface ihnen dabei hilft. Eine Organisation könnte nun ein Set von empfehlenswerten Präferenzen für Endnutzer erstellen. Nutzer die dieser Organisation vertrauen, könnten sich das vordefinierte Ruleset installieren und sich somit viel Mühe bei der Festlegung eines eigenen Rulesets ersparen. Aktive Rulesets könnten auf einem Heim-PC ganz einfach geändert oder auf einen neuen PC übertragen werden [Cranor, Langheinrich, & Marchiori, 2002].

- *Kommunikation zu Agents, Suchmaschinen, Proxies oder anderen Servern:* Viele Server jeglicher Art würden gerne ihren Output besser an die Nutzer-Präferenzen, wie sie in deren Ruleset formuliert sind, anpassen. Beispielsweise zeigt eine Suchmaschine nur Links an, die mit dem Ruleset des Nutzers übereinstimmen, welche möglicherweise mit einer Vielzahl an Faktoren wie Qualität, Datenschutz, Altersangemessenheit etc., spezifiziert wurde [Cranor, Langheinrich, & Marchiori, 2002].
- *Übertragbarkeit zwischen den Produkten*: Dieselben Rulesets funktionieren mit jedem Produkt auf dem P3P oder APPEL aktiviert ist [Cranor, Langheinrich, & Marchiori, 2002].

Im Wesentlichen ging es bei der Entwicklung von APPEL darum, dass Nutzer Rulesets, die von Dritten erstellt wurden, importieren und auch die Möglichkeit für sie besteht, die eigenen Ruleset-Dateien zwischen mehreren User-Agents transportieren zu können [Cranor, Langheinrich, & Marchiori, 2002].

3.3. EPAL

Die IBM Enterprise Privacy Authorization Language (EPAL) ist eine formalisierte Sprache, um Datenschutzerklärungen in einem strukturierten Format zwischen Applikationen oder Firmen auszutauschen. Das Leitbild der EPAL Working Group liegt auf der Erschaffung einer kompatiblen Sprache, um die Datenverarbeitungs- sowie Datenschutzpraktiken innerhalb und zwischen Privacy-Tools von Unternehmen zu repräsentieren. Daraus ist zu erkennen, dass EPAL im Gegensatz zu P3P und APPEL für den Einsatz in Unternehmen entwickelt wurde [Ashley, Hada, Karjoth, Powers, & Schunter, Enterprise Privacy Authorization Language (EPAL 1.2), 2003].

Der Kern von EPAL ist ein Autorisierungsschema, welches überprüft ob bestimmte Handlungen erlaubt sind. Dabei ist es unerheblich welches Datenmodell die jeweilige Software verwendet oder welche Zugriffsrechte dem Nutzer zustehen. Die Autorisierung geschieht mittels Regeln die im Vorhinein formuliert werden. Eine EPAL-Datenschutzinformation besteht aus Datenkategorien, Nutzerkategorien, Verarbeitungszwecke und Gruppen von Handlungen, Verpflichtungen und Bedingungen. Daraus werden die w.o. genannten Regeln definiert, welche bestimmen ob die gesammelten persönlichen Informationen verarbeitet werden dürfen oder nicht. Die Au-

torisierung zur Verarbeitung hängt des Weiteren von den Eigenschaften Datum, Nutzer und Zweck ab. Die gesetzlichen Rahmenbedingungen und die Datenverarbeitungspraktiken geben dem Unternehmen vor, wie jeweilig individuell kategorisiert wird [Ashley, Hada, Karjoth, Powers, & Schunter, The Enterprise Privacy Authorization Language (EPAL) - How to Enforce Privacy throughout an Enterprise, 2002; Möller, Enterprise Privacy Authorization Language (EPAL), 2004].

3.3.1. Funktionsweise und Anwendungsbeispiel

Um die Funktionsweise von EPAL besser darstellen zu können, wird hier auf ein Anwendungsbeispiel einer Member Submission des W3C eingegangen. Angenommen die Firma „BestShoesRUs“ verkauft Schuhe [Ashley, Hada, Karjoth, Powers, & Schunter, Enterprise Privacy Authorization Language (EPAL 1.2), 2003]:

1. in Geschäften überall in Nordamerika und Asien,
2. durch Versandkataloge die an Abonnenten verschickt werden,
3. mittels einer 1-800 Hotline (24 Stunden pro Tag) und
4. via Internet (http://www.bestshoesrus.example.com).

Das Unternehmen BestShoesRUs hatte sich schon immer um einen aktiven Datenschutz bemüht. Doch durch das stetige Expandieren wurde es immer schwieriger dies auch zu repräsentieren beziehungsweise eine einheitliche Datenschutzerklärung in allen Teilen des Unternehmens beizubehalten. Die Kunden haben bereits angefangen sich über unerwünschte Marketingzusendungen zu beschweren und einige haben BestShoesRUs bereits vorgeworfen, die privaten Daten der Kunden an Dritte verkauft zu haben [Ashley, Hada, Karjoth, Powers, & Schunter, Enterprise Privacy Authorization Language (EPAL 1.2), 2003].

Um die Datenschutzpraktiken zu verbessern, hat sich BestShoesRUs dazu entschieden im ganzen Unternehmen eine einheitliche EPAL-Policy zu verwenden. Das Ziel der Policy ist es eine Gruppe von gebräuchlichen Regeln für die Verarbeitung von persönlichen Daten die von den Kunden stammen zu definieren. Dies soll gewährleisten, egal wie die Daten auch gesammelt wurden (durch die Filialen, Post, Telefon, Internet, Nordamerika, Asien), dass diese in einer einheitlichen Art und Weise bearbeitet werden [Ashley, Hada, Karjoth, Powers, & Schunter, Enterprise Privacy Authorization Language (EPAL 1.2), 2003].

Um diesen Prozess zu starten, muss zuallererst eine EPAL-Datenschutzerklärung erstellt werden. Dies kann beispielsweise vom CPO (Leiter des Geschäftsprozessmangements) oder dessen Personal gemacht werden. Diese Erklärung sollte einem hohen Standard entsprechen, um den rechtlichen Ansprüchen und den jeweiligen Regulierungen des Industriezweigs Stand zu halten. Der CPO sollte sich auch mit Beratern, die sich auf Datenschutz spezialisiert haben, in Verbindung setzen. Dadurch soll eine für BestShoesRUs maßgeschneiderte Datenschutzerklärung entstehen, die im ganzen Unternehmen einheitlich gilt [Ashley, Hada, Karjoth, Powers, & Schunter, Enterprise Privacy Authorization Language (EPAL 1.2), 2003; Ashley, Hada, Karjoth, Powers, & Schunter, The Enterprise Privacy Authorization Language (EPAL) - How to Enforce Privacy throughout an Enterprise, 2002].

Nachdem die Datenschutzerklärung definiert ist, wird sie auf das IT-System, welches mit den persönlichen Daten der Kunden arbeitet, aufgespielt und somit „zwingend". Folgende Punkte sollten dabei beachtet werden [Ashley, Hada, Karjoth, Powers, & Schunter, The Enterprise Privacy Authorization Language (EPAL) - How to Enforce Privacy throughout an Enterprise, 2002; Ashley, Hada, Karjoth, Powers, & Schunter, Enterprise Privacy Authorization Language (EPAL 1.2), 2003]:

- *Bekanntmachung*: Die Datenschutzerklärung sollte für die Kunden eindeutig formuliert sein. Das heißt die Erklärung wird auf der Webseite von BestShoesRUs (zum Beispiel in Text und P3P) publiziert. Des Weiteren sollte in den Marketingmaterialien und im Versandkatalog die Policy im Textformat erwähnt werden. Die Telefonangestellten müssen bei der Sammlung von persönlichen Daten der Kunden, diese auf die Datenschutzerklärung aufmerksam machen.
- *Einwilligung*: Die Einwilligungserklärung, die durch EPAL definiert wurde, soll für die Kunden dargeboten werden. Diese können die Einwilligung einsehen und die bereits abgegebene Einwilligung aktualisieren. Beispielsweise sollte den Kunden die Möglichkeit gegeben werden, sich ganz aus den Marketingmaßnahmen des Unternehmens austragen zu können („opt-out") oder bestimmte Services wie Postzusendungen, E-Mails etc. auszuwählen. Diese Einwilligungen müssen via Katalogformulare, Internet, Telefon oder in den Geschäften zugänglich sein.

- *Durchsetzung*: An jeder Stelle, wo persönliche Daten der Kunden gesammelt oder genutzt werden, müssen Vorgänge und die verwendete Software die EPAL-Policy durchsetzen können.

Durch neue rechtliche Rahmenbedingungen oder Veränderung von branchenüblichen Praktiken kann sich die EPAL-Policy im Laufe der Zeit verändern und deshalb müssen auch neuere Version erstellt werden. BestShoesRUs wird sich Softwaretools zur Erstellung von Datenschutzerklärungen und zu deren Bekanntmachung, Einwilligung und Durchsetzung anschaffen müssen. Die EPAL-Policy übernimmt dann die Funktion, die Policy zwischen den verwendeten Tools auszutauschen.

Wenn ein Kunde persönliche Daten übermittelt, werden das Datum, die gegenwärtig geltende Datenschutzerklärung und die Nutzerpräferenzen im System gespeichert. Später, wenn diese Daten vom Unternehmen verarbeitet werden, wird das System nur jene Daten freigeben, die mit der Datenschutzerklärung konform gehen [Ashley, Hada, Karjoth, Powers, & Schunter, The Enterprise Privacy Authorization Language (EPAL) - How to Enforce Privacy throughout an Enterprise, 2002].

EPAL kategorisiert die Daten eines Unternehmens und die Regeln, welche die Nutzung der Daten jeder Kategorie steuern. Die Elemente der Datenschutzerklärung werden von EPAL nicht vordefiniert, da diese Sprache in vielen Bereichen einsetzbar sein soll. Deshalb bietet EPAL die Möglichkeit für ein Unternehmen sie selbst zu definieren oder von einer anderen Policy zu importieren. Eine EPAL-Policy besteht aus einer Menge von Datenschutzregeln. Jede dieser „Rules“ besteht aus Entscheidungen, Nutzerdaten, Handlungen, Datenkategorien und Zwecken. Des Weiteren können auch Bedingungen und Pflichten enthalten sein. Jede Rule besitzt eine bestimmte Rangordnung. Eine EPAL-Policy besteht aus drei Hauptabschnitten:

- *Policy Information*: Dieser Abschnitt beinhaltet die Bezeichnung der Policy, da Informationen wie der Name des Herausgebers, Versionsnummer, Anfangs- und Enddatum etc. enthalten sind.
- *Definitions*: In diesem Abschnitt werden alle möglichen Komponenten, die in den Rules verwendet werden können, vordefiniert. Zu diesen Komponenten

zählen Nutzerdaten, Datenkategorie, Zweck, Handlungen, Kontextmodelle, Bedingungen und Pflichten.

- *ALLOW or DENY:* Der 3. Abschnitt beinhaltet die Regeln die definieren ob es einer Person erlaubt (ALLOW) oder verweigert (DENY) wird, auf die persönlichen Daten zuzugreifen. Die Terminologie ist wie folgt:
    - ALLOW (Data User) TO PERFORM (Action) ON (Data Type) FOR (Purpose) IF (Condition) AND CARRY OUT (Obligation).
      oder
    - DENY (Data User) TO PERFORM (Action) ON (Data Type) FOR (Purpose) IF (Condition) AND CARRY OUT (Obligation).

Das nachfolgende Beispiel soll zeigen, wie EPAL eingesetzt werden kann, um Rules für Datenschutzerklärungen auszudrücken:

Tabelle 4: Beispiel für den Einsatz von EPAL

Informelle Datenschutzerklärung (informal privacy policy)	Einem Verkaufsangestellten oder Verkaufsleiter ist es erlaubt, Daten von Kunden, die älter als 13 Jahre alt sind, für die Auftragsabwicklung zu verarbeiten, wenn diese auf die Datenschutzerklärung hingewiesen wurden. Wenn die Daten älter als drei Jahre alt sind, werden sie gelöscht.
Entscheidung (ruling)	Erlauben (allow)
Nutzerkategorie (user category)	Verkaufsabteilung
Handlungen (action)	Speicherung (store)
Datenkategorie (data category)	Kundenaufzeichnungen
Zweck (purpose)	Auftragsabwicklung
Bedingungen (condition)	Der Kunde muss älter als 13 Jahre sein

Pflichten (obligation)	Daten die älter als drei Jahre sind, werden gelöscht

Quelle: [Ashley, Hada, Karjoth, Powers, & Schunter, 2002]

Die bereits erwähnten Rules bestimmen ob eine Abfrage (request) erlaubt oder verweigert wird. Sie beinhaltet immer folgende Parameter: die Nutzerkategorie, eine Handlung, eine Datenkategorie und einen Zweck. Nachfolgend wird das Beispiel mit einer Anfrage fortgesetzt [Ashley, Hada, Karjoth, Powers, & Schunter, The Enterprise Privacy Authorization Language (EPAL) - How to Enforce Privacy throughout an Enterprise, 2002].

Tabelle 5: Beispiel einer EPAL Abfrage

Informelle Abfrage (informal request)	Eine Person, die Verkaufsangestellter der Firma ist, will die E-Mailadresse eines Kunden für die Kaufabwicklung abfragen.
Nutzerkategorie (user category)	Verkaufsabteilung
Handlung (action)	Speicherung (store)
Datenkategorie (data category)	Kundenaufzeichnung
Zweck	Verkaufsabwicklung

Quelle: Ashley, Hada, Karjoth, Powers, & Schunter, The Enterprise Privacy Authorization Language (EPAL) - How to Enforce Privacy throughout an Enterprise, 2002

Die Abfrage des Angestellten wird von der obigen Rule erlaubt. Das bedeutet er könnte die Kundenkontaktinformationen speichern. Zusätzliche Regeln könnten dann eventuell noch steuern, wie diese gespeicherten Daten weitergenutzt werden dürfen. Nachfolgend werden noch weitere Beispiele für Regeln, die in XML geschrieben sind, aufgezeigt [Ashley, Hada, Karjoth, Powers, & Schunter, The Enterprise Privacy Authorization Language (EPAL) - How to Enforce Privacy throughout an Enterprise, 2002]:

Die E-Mailadresse darf für den „Buch des Monats“-Club genutzt werden, wenn es eine Einwilligung dazu gibt und der Kunde älter als 13 Jahre ist. Diese Rule sieht in EPAL folgendermaßen aus [Ashley, Hada, Karjoth, Powers, & Schunter, The Enterprise Privacy Authorization Language (EPAL) - How to Enforce Privacy throughout an Enterprise, 2002]:

```
<rule id="rule1" ruling="allow">
<data-user id="borderless-books"/>
<data-category id="email"/>
<purpose id="book-of-the-month-club"/>
<action id="read"/>
<condition id="consentToBookClub"/>
<condition id="olderThan13"/>
<obligation id="retention">
        <parameter id="days">5</parameter>
</obligation>
```

Sollen die Eltern in alle Daten ihrer Kinder Einsicht nehmen dürfen, würde die Regel lauten [Ashley, Hada, Karjoth, Powers, & Schunter, The Enterprise Privacy Authorization Language (EPAL) - How to Enforce Privacy throughout an Enterprise, 2002]:

```
</rule>
<rule id="rule2" ruling="allow">
<data user id = "parent"/>
        <data category id = "p3p: any category"/>
        <purpose id = "p3p: current"/>
        <action id = "read"/>
</rule>
```

3.3.2. Vor- und Nachteile

Zu den Vorteilen von EPAL zählen:

- EPAL kann Organisationen helfen ihre Datenschutzpraktiken und deren konforme Einhaltung aufzuzeigen,
- die Gemeinkosten sowie die Kosten der Konfiguration und Geltendmachung der Datenschutzerklärung senken und
- bereits existierende Standards und Technologien verbessern und dabei helfen sie wirksam einzusetzen [Ashley, Hada, Karjoth, Powers, & Schunter, Enterprise Privacy Authorization Language (EPAL 1.2), 2003]

Funktionen die EPAL nicht übernehmen kann sind:

- Direkte Programmierung oder Durchsetzung von rechtlichen Rahmenbedingungen bezüglich des Datenschutzes in einer generischen und unternehmensabhängigen Applikation.
- Manipulation von EPAL durch Personen um ihre Präferenzen zu setzen. Zum Beispiel können Personen nicht Informationen über sich bereitstellen, um daraus ein Nutzerpräferenz-Profil basierend auf den Informationen der EPAL-Policy zu erstellen.
- Erstellen von neuen Mechanismen oder Syntax für die Repräsentation von Daten: EPAL bietet keine eigene Syntax um Datenschemata darzustellen.
- EPAL verfügt über eine limitierte Anzahl an Funktionen, um sich leichter an andere Programme oder Tools anzupassen.

[Ashley, Hada, Karjoth, Powers, & Schunter, Enterprise Privacy Authorization Language (EPAL 1.2), 2003]

3.3.3. Verhältnis von EPAL zu P3P

Wie bereits in Kapitel 3.1 erläutert, kann P3P dazu eingesetzt werden, um Datenschutzerklärungen von Webseiten wiederzugeben, es ist aber ungeeignet um eine intern durchsetzbare Policy auszudrücken. EPAL wiederum ist dafür entworfen worden, intern eine Datenschutzerklärung durchzusetzen. Tabelle 6 fasst die Unterschiede zwischen EPAL und P3P übersichtlich zusammen [Ashley, Hada, Karjoth, Powers, & Schunter, The Enterprise Privacy Authorization Language (EPAL) - How to Enforce Privacy throughout an Enterprise, 2002]:

Tabelle 6: Gegenüberstellung von EPAL und P3P

	EPAL	P3P
Datenkategorien (data categories)	Hierarchie	Vordefinierte Listen
Nutzer (user)	Hierarchie	Vordefinierte Listen
Zweck (purposes)	Hierarchie	Vordefinierte Listen
Handlungen (actions)	Liste	„use“
Bedingungen (conditions)	XACML[13]	keine
Pflichten (obligations)	Liste	“retention”
Datenschutz Wahl/Angebot (privacy choices)	Verallgemeinert	+/- purposes/recipient/retention
Eigenschaften (properties)	• Flexibel • Hierarchisch • Zugriffskontrolle • Erzwingbar/Durchsetzbar • Weniger Interoperabel	• Simpel • Interoperabel • Weniger Erweiterbar • Keine Erzwingung / Durchsetzung • Limitiert • „Web-centric“

Quelle: [Ashley, Hada, Karjoth, Powers, & Schunter, 2002]

[13]XACML (eXtensible Access Control Markup Language) ist ein Standard in XML, um Regeln aufzustellen wodurch Zugriffe von Subjekten auf bestimmte Ressourcen eines Systems ausgewertet werden. (vgl. http://de.wikipedia.org/wiki/XACML Datum und Uhrzeit der Abfrage: 22. August 2008 13:20)

- *Kategorien*: P3P verfügt über eine vordefinierte Liste von Datenkategorien. EPAL erlaubt die Definition von eigenen Listen von Datenkategorien und diese können hierarchisch sein.
- *Nutzerdaten*: P3P hat eine vordefinierte Liste von Nutzerdaten. EPAL erlaubt die Definition von eigenen Nutzerdatenlisten und diese können hierarchisch angeordnet werden.
- *Zweck*: P3P verfügt über eine vordefinierte Zweck-Liste. EPAL erlaubt die Definition von eigenen Zweck-Listen und diese können in einer Hierarchie geordnet sein.
- *Handlungen*: P3P definiert nur die Handlung „use“. Beim Einsatz von EPAL kann eine Liste von Handlungen definiert werden.
- Bedingungen: P3P unterstützt keine Bedingungen. EPAL benutzt die XACML-Sprache um Bedingungen zu definieren.
- Pflichten: P3P definiert nur die Pflicht „retention“. EPAL erlaubt den Einsatz einer Liste von Pflichten.
- Wahl: P3P unterstützt nur simple „opt-in/opt-out“-Wahlmöglichkeiten, während EPAL mehr generalisierte Möglichkeiten bietet.

Zusammenfassend kann gesagt werden, dass P3P zur Wiedergabe von hochwertigen Datenschutzerklärungen auf Webseiten eingesetzt werden kann. EPAL dagegen, sollte dann zum Einsatz kommen, wenn Datenschutzerklärungen intern in einem Unternehmen durchgesetzt werden sollen [Ashley, Hada, Karjoth, Powers, & Schunter, The Enterprise Privacy Authorization Language (EPAL) - How to Enforce Privacy throughout an Enterprise, 2002].

3.4. Zusammenfassung und Ausblick

Wie bereits in den obigen Kapiteln erläutert, bietet jedes der vorgestellten Tools einer anderen Zielgruppe gewisse Vor- bzw. Nachteile. P3P und APPEL sind für die Verwendung durch den Endnutzer konzipiert (wobei natürlich der Anbieter jeweils serverseitig eine P3P Policy anbieten muss), während EPAL eine Alternative für Unternehmen darstellt. Jedes dieser Tools verfügt über individuelle Vor- beziehungsweise Nachteile und wie bereits in Kapitel 2.5 erläutert, kann keines für sich allein eine 100%ige Sicherheit in Bezug auf den Schutz von Daten für den jeweiligen Nutzer bieten. Sie stellen aber laut Cranor (2003) eine Möglichkeit dar, um den eigenen akti-

ven Datenschutz zu ergänzen beziehungsweise zu erleichtern. Dabei müssen vor allem die Endnutzer aufgeklärt werden, dass diese Tools die Verantwortung sowie Sorgfalt mit dem Umgang von persönlichen Daten nicht ersetzen können.

II. Empirischer Teil

4. Empirischer Teil

Im empirischen Teil der Arbeit wird zunächst der Einsatz von P3P bei Unternehmen überprüft und anschließend analysiert. Danach werden in Kapitel 4.2 Einflussfaktoren auf das Kaufverhalten im Internet und eventuelle Ängste anhand einer Untersuchung von StudentInnen der Wirtschaftsuniversität Wien mittels eines Fragebogens aufgezeigt.

4.1. Untersuchung des Einsatzes von P3P bei einer Stichprobe der Forbes 400 Unternehmen

Die Analyse des Einsatzes von P3P bei Unternehmen wurde an einer Stichprobe der 400 größten, amerikanischen Unternehmen, welche durch Forbes[14] für das Jahr 2008 ermittelt wurden, durchgeführt. Die analysierten Branchen waren:

- Software und Services
- Telekommunikationsservices
- Medien
- und Einzelhandel.

Dabei wurde mittels „wget“-Befehl in einer Unix Shell die Webseite der Unternehmen abgerufen, um zu überprüfen, ob dieses über eine Compact Policy verfügt (Für nähere Informationen zu Compact Policies und deren Vokabular siehe Kapitel 3.1.3 auf Seite 50).

[14] Forbes ist ein englischsprachiges Wirtschaftsjournal, welches vor allem durch seine Ranglisten erfolgreich wurde. Das Magazin veröffentlicht in regelmäßigen Abständen unterschiedlichste Rankings wie zum Beispiel die 400 größten amerikanischen Unternehmen, die 100 mächtigsten Frauen der Welt, die Milliardäre der Welt, etc. (vgl. http://de.wikipedia.org/wiki/Forbes_Magazine Datum und Uhrzeit der Abfrage: 13. August 2008 16:45)

4.1.1. Analyse des Einsatzes und Interpretation

In den nachfolgenden Tabellen werden die Unternehmen der einzelnen Branchen mit dem Ergebnis der Analyse, ob sie über eine Compact Policy verfügen, aufgelistet.

Tabelle 7: Aus dem Ranking der 400 größten, amerikanischen Unternehmen für die Branche: Software und Services

Name	5 Year total return %	Sales ($ Bil)	Net income ($ Mil)	Compact Policy
Accenture	14.0	19.7	1,243	
Activision	33.5	2.0	157	
Adobe Systems	22.9	2.9	685	
Amdocs	23.2	2.8	365	
Autodesk	43.2	2.1	356	
BMC Software	12.7	1.6	262	
Citrix Systems	25.9	1.3	210	
Cognizant Technology	40.2	2.0	323	
Google	80.4	15.0	4,028	
Intuit	2.1	2.8	478	✓
ManTech International	14.0	1.3	60	
Microsoft	6.3	54.1	14,876	✓
Oracle	11.3	18.9	4,444	
SRA International	15.1	1.3	67	

Quelle: [Forbes 400; Software and Services Companies[15]]

[15] vgl. http://www.forbes.com/lists/2008/88/biz_08platinum_The-400-Best-Big-Companies-Software-Services_7Company.html Datum und Uhrzeit der Abfrage: 11. August 2008 15:35

Tabelle 8: Aus dem Ranking der 400 größten, amerikanischen Unternehmen für die Branche: Telekommunikationsservices

Name	5 Year total return %	Sales ($ Bil)	Net income ($ Mil)	Compact Policy
American Tower	62.5	1.4	80	
AT&T	10.7	104.5	10,753	✓
CenturyTel	7.5	2.6	376	
NII Holdings	95.8	3.0	358	
Verizon Commun	5.6	92.2	5,612	

Quelle: [Forbes 400; Telecommunications Services Companies16]

Tabelle 9: Aus dem Ranking der 400 größten, amerikanischen Unternehmen für die Branche: Medien

Name	5 Year total return %	Sales $ Bil	Net income $ Mil	Compact Policy
Comcast	4.2	29.9	2,375	
DirecTV Group	15.9	16.6	1,459	
Walt Disney	11.8	35.5	4,687	✓
RR Donnelley & Sons	14.3	11.0	243	
John Wiley & Sons	13.9	1.4	118	
McGraw-Hill Cos	11.3	6.8	1,078	
Meredith	6.1	1.6	165	
News Corp	13.3	29.8	3,315	
Omnicom Group	8.6	12.3	939	
EW Scripps	3.2	2.5	388	
Viacom	-2.7	12.8	1,759	
WPP Group	11.5	11.0	645	

Quelle: [Forbes 400; Media Companies17]

[16] vgl. http://www.forbes.com/lists/2008/88/biz_08platinum_The-400-Best-Big-Companies-Telecommunications-Services_7Company.html Datum und Uhrzeit der Abfrage: 11. August 2008 15:41

[17] vgl. http://www.forbes.com/lists/2008/88/biz_08platinum_The-400-Best-Big-Companies-Media_7Company.html Datum und Uhrzeit der Abfrage: 11. August 2008 15:45

Tabelle 10: Aus dem Ranking der 400 größten, amerikanischen Unternehmen für die Branche: Einzelhandel

Name	5 Year total return %	Sales $ Bil	Net income $ Mil	Compact Policy
Aaron Rents	14.7	1.4	84	
Abercrombie & Fitch	27.1	3.7	457	
Aeropostale	34.4	1.5	118	✓
Amazon.com	30.2	13.1	367	
Amer Eagle Outfitters	29.0	3.0	410	
Barnes & Noble	19.0	5.4	148	✓
Bed Bath & Beyond	-2.9	6.9	600	
Best Buy	23.8	38.0	1,355	
CarMax	18.1	7.9	218	
Dick's Sporting Goods	44.2	3.7	150	✓
Dollar Tree Stores	-1.3	4.3	204	
Ebay	14.1	7.2	164	
Fastenal	18.9	2.0	222	
GameStop	42.9	6.5	228	
Guess?	75.2	1.5	163	
Kohl's	-6.2	16.4	1,157	
Longs Drug Stores	24.4	5.2	86	
Men's Wearhouse	26.4	2.1	179	
O'Reilly Automotive	18.8	2.5	194	
PC Connection	13.3	1.7	21	
Penske Automotive	25.0	12.8	129	

Petsmart	9.0	4.5	260	✓
Priceline.com	59.5	1.3	138	
Ross Stores	3.1	5.9	260	
Sherwin-Williams	19.0	7.9	613	
Staples	13.0	19.3	999	
Target	11.9	63.2	2,939	
Tiffany & Co	13.5	2.8	256	
Tractor Supply	12.6	2.6	96	
Urban Outfitters	51.7	1.4	142	
Walgreen	6.6	53.8	2,041	

Quelle: [Forbes 400; Retailers18]

Von den 62 untersuchten Unternehmen, verfügten acht über eine Compact Policy. Die geringe Anzahl kann sich aus der Tatsache ergeben, dass viele der Unternehmen keinen direkten Kundenkontakt haben und deshalb sich nicht um einen aktiven und für den Kunden sichtbaren Datenschutz bemühen müssen. Beispielsweise sind in der Branche Medien große Konzerne zu finden, welche als Investoren oder Mutterunternehmen agieren und aus diesem Grund keine Endverbraucher ansprechen (wollen). Dies ist auch schon anhand der Internetpräsenzen zu erkennen. Die Webseiten verfügen einerseits über keinen Verkauf von Waren, bei denen Kunden sich registrieren müssen und um etwas bestellen zu können, sensible, persönliche Informationen wie zum Beispiel Name, Adresse, Kreditkartennummer etc. preisgeben müssen. Des Weiteren gibt es auch keine Möglichkeiten, dass sich auf den Seiten eine Community, also ein soziales Netzwerk, bilden kann, da dafür essentielle Faktoren wie beispielsweise Foren, Chats, Shoutboxes etc. fehlen. Als Beispiele für Webseiten ohne jegliche Registrierungsmöglichkeiten können die Internetpräsenzen von News Corporation und Omnicom Group genannt werden. Sie bieten eine Vielzahl an werbenden Informationen für Investoren und andere Unternehmen, sowie Stellenausschreibungen, Presseberichte etc., aber es kann keine Sammlung von sensiblen Daten stattfinden, da es keine Registrierungsmöglichkeiten gibt. Bei der Gestaltung

[18] vgl. http://www.forbes.com/lists/2008/88/biz_08platinum_The-400-Best-Big-Companies-Retailing_7Company_2.html Datum und Uhrzeit der Abfrage: 11. August 2008 16.00

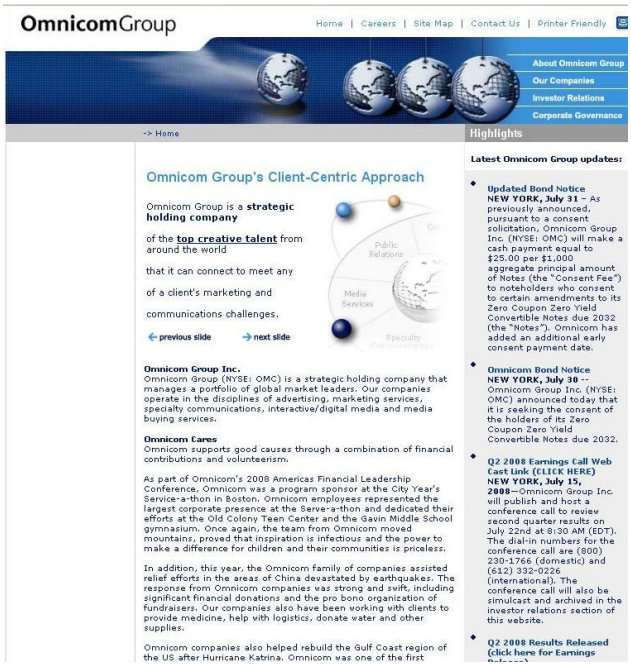
der Seiten fällt auf, dass Farben, Bilder und Videos dezent eingesetzt werden und der informative Gehalt der Texte im Vordergrund steht.

Nachfolgend werden zwei Screenshots zur Veranschaulichung der eben genannten Beispiele gezeigt.

Abbildung 9: Screenshot der Startseite von News Croporation

Quelle:[http://www.newscorp.com Datum und Uhrzeit der Abfrage: 19. August 2008 13:10]

Abbildung 10: Screenshot der Startseite der Omnicom Group



Quelle: [http://www.omnicomgroup.com Datum und Uhrzeit der Abfrage: 19. August 2008 13:12]

Im Gegensatz zu den dezent gestalteten Konzernseiten, sprechen die Webseiten, beispielsweise von Disney oder Petsmart, von der Gestaltung und Aufmachung, eher Endkunden an. Das Layout ist sehr bunt und es befinden sich viele Bilder, animierte Funktionen, Musikdateien und Videos auf den Seiten. Zusätzlich gibt es bei beiden die Möglichkeit einen Account zu erstellen, bei dem man sich mit Vor- und Nachnamen, E-Mailadresse etc. registriert. Da diese Seiten, wie bereits erläutert, Konsumenten ansprechen und P3P für diese Nutzer entwickelt wurde, überrascht es nicht, dass diese Seiten serverseitig diese Technologie einsetzen. Durch die automatisierte Weitergabe der Datenschutzpraktiken an die Endnutzer, vorausgesetzt sie benutzen P3P, wird dieser Prozess wesentlich erleichtert und das Vertrauen nachhaltig gestärkt (siehe für nähere Informationen zu Konsumentenvertrauen im Internet Kapitel 2.3 auf Seite 15).

Die nachfolgenden Screenshots zeigen jeweils die Startseiten der eben genannten Webseitenbeispiele.

Abbildung 11: Screenshot der Startseite von Disney

Quelle: [http://disney.go.com/index Datum und Uhrzeit der Abfrage: 19. August 2008 14:14]

Abbildung 12: Screenshot der Startseite von Petsmart

Quelle: [http://www.petsmart.com/home/index.jsp Datum und Uhrzeit der Abfrage: 19. August 2008 14:15]

4.1.1. Vergleich der Compact Policies mit den, für den Menschen lesbaren, Datenschutzerklärungen

In diesem Kapitel werden die, durch die Abfragen erhaltenen, Compact Policies mit den korrespondieren Datenschutzerklärungen der jeweiligen Unternehmen verglichen und interpretiert. Damit der Informationsgehalt der Analyse überschaubar bleibt, wurde für das Unternehmen Intuit die Compact Policy und der Vergleich mit der Datenschutzerklärung vollständig ausformuliert. Für die danach folgenden Unternehmen werden die Ergebnisse zusammengefasst dargestellt.

4.1.1.1. Intuit

Intuit Inc. ist ein amerikanischer Entwickler von Standardanwendungssoftware mit Sitz in Kalifornien. Weltweit beschäftigt das Unternehmen knapp 7.000 MitarbeiterInnen und erzielte im Jahr 2006 rund 2,3 Milliarden Dollar an Umsatz[19].

Die Abfrage des HTTP Response Headers bei Intuit ergab folgende Compact Policy: `policy-ref="http://www.intuit.com/commerce/common/fragments/popup/popup.jhtml?content=privacy", CP="NOI DSP CURa ADMa DEVa TAIa PSAa PSDa OUR IND UNI COM NAV"` Für eine Erläuterung der einzelnen Token siehe Kapitel 3.1.3.

Vergleich der Compact Policy mit der, für den Menschen lesbaren, Datenschutzerklärung[20]

Zugriff:

Gemäß der Compact Policy werden keine identifizierbaren Daten gesammelt. Dies steht im Gegensatz zu den Angaben von Intuit in ihrer Datenschutzerklärung. Dort findet man mehrere Anzeichen dafür, dass eine Sammlung von persönlichen Daten stattfinden kann. *„We work to protect your personal information from loss, misuse or unauthorized alteration by using industry-recognized security safeguards.*“ Es wird erläutert, dass die persönlichen Informationen vor Verlust, Missbrauch und unerlaub-

[19] (vgl. http://de.wikipedia.org/wiki/Intuit Datum und Uhrzeit der Abfrage: 19. August 2008 17:33)
[20] Die Datenschutzerklärung von Intuit findet man unter:
http://www.intuit.com/commerce/common/fragments/popup/popup.jhtml?content=privacy
Datum und Uhrzeit der Abfrage: 17. August 2008 14:00

ter Abänderung mithilfe von anerkannten Sicherheitstools der Wirtschaft geschützt werden. Diese Anmerkung steht im Gegensatz zu der in der Compact Policy erklärten Nicht-Sammlung von persönlichen Daten. Des Weiteren heißt es in der Datenschutzerklärung: *„When ordering online, we offer you the option of creating an Intuit "My Account" to store your contact, billing, shipping, and payment information so that you do not have to enter it each time you make a purchase."* Wodurch sich zeigt, dass schon aus der Natur des Verkaufs von Services im Internet, persönliche Daten abgefragt werden müssen, da der Anbieter die Zahlungsmodalitäten und Kontaktinformationen braucht, um überhaupt seine Dienstleistung erbringen zu können.

Schlichtstellen:
In der Compact Policy wird eine Schlichtstelle angegeben, in der Datenschutzerklärung wird TRUSTe, eine unabhängige Non-Profit Organisation, welche als Datenschutz-Gütesiegel fungiert, erwähnt. Nutzer welche einen Verstoß gegen die Datenschutzerklärung feststellen, können dies bei TRUSTe melden. Erwähnenswert ist, dass das Gütesiegel nur die konforme Datensammlung durch die Webseite versichert und nicht die eventuelle Sammlung durch heruntergeladene Software der Seite. *„The TRUSTe program covers only information that is collected through this Web site and does not cover information that may be collected through software downloaded from the site."*

Zweck und Kategorien: (Die Elemente wurden für die Interpretation zusammengefasst, da in der Datenschutzerklärung öfters auf beide Elemente in einem Satz beziehungsweise Abschnitt bezug genommen wurde)

In der Datenschutzerklärung wird erläutert, dass Kunden ein Profil auf der Webseite erstellen können, den sog. Intuit „My Account" (wie w.o. bereits erwähnt). Durch diesen Account wird es den Kunden ermöglich ihre persönliche Informationen (wie bspw. Kontakt-, Rechnungs-, Lieferungs- und Zahlungsinformationen) abzuspeichern, damit diese Informationen nicht bei jedem Einkauf erneut eingetragen werden müssen. Intuit nutzt die übermittelten Kundendaten, um Produkte oder Services zu bewerben, an denen ein mögliches Interesse seitens des Kunden besteht. Von diesem Service kann man sich jederzeit austragen „*We may also provide you informa-*

tion about products or services we believe you may be interested in unless you have asked us not to contact you."

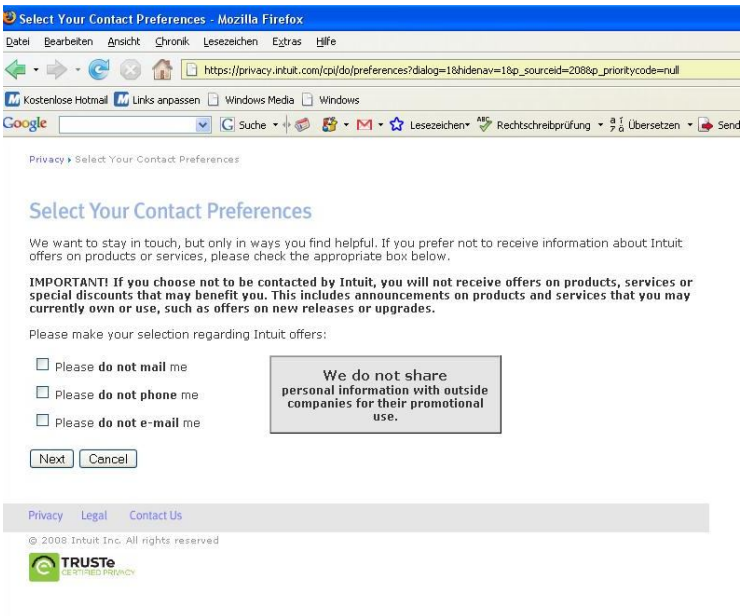
Auf der Webseite werden laut Datenschutzerklärung Cookies eingesetzt, um den/die NutzerIn wiederzuerkennen und die Webseite kundenspezifisch zu gestalten. *„Like many Web sites, we use technology, such as cookies, that allow us to make your visit to our Web site easier by recognizing you when you return and help to provide you with a customized experience."* Dabei wird die Nutzung der Seite, welche Bereiche betrachtet wurden, aufgezeichnet und daraus die Lieblingsbereiche ermittelt. *„Cookies allow us to track overall site usage and determine areas users prefer."* Das Akzeptieren der Cookies kann vom Nutzer im Browser ausgestellt werden, wobei aber bestimmte Bereiche der Seite nicht betrachtet werden können. *„You can choose to decline cookies while at our Web site, however, this may limit your ability to access certain areas of the Web site."* (für nähere Informationen zu dem Thema Cookies siehe Kapitel 2.4.5 Sonderfälle des Datenschutzes im Internet)

Intuit speichert die IP-Adresse, der Browsertyp und -version sowie die Seiten, welche betrachtet wurden. Des Weiteren wird aufgezeichnet, von welcher Seite man auf die Webseite von Intuit kommt und welchen Link man benutzt, wenn man die Seite wieder verlässt. Nach dem Verlassen, wird der Kunde, laut den Angaben von Intuit, nicht weiter im Internet verfolgt. Es werden auch nicht die URLs, die in den Browser eingetippt werden, gespeichert. Die Aufzeichnungen dienen laut Datenschutzerklärung dafür, dass der Kunde seine Daten nicht immer wieder eingeben muss und um technische Supportprobleme zu lösen. Des Weiteren können die Informationen dazu verwendet werden die Webseite für den jeweiligen Kunden maßgeschneidert darzustellen und Angebote kundenspezifisch zu gestalten. Der Kunde kann sich jederzeit von den Marketingmaßnahmen austragen.

Um das Verhalten des Kunden auf der Webseite überwachen zu können, werden laut der Datenschutzerklärung Web Bugs (siehe dazu Kapitel 2.4.5. Sonderfälle des Datenschutzes im Internet) eingesetzt. Des Weiteren werden Web Bugs auch bei E-Mails von Intuit eingesetzt, welche an Kunden versandt werden. Erklärtes Ziel ist es, das Clickverhalten der Nutzer aufzuzeichnen, damit Werbematerial kundenspezifisch gestaltet werden kann.

Wenn ein Kunde sich aus den Werbemaßnahmen von Intuit austragen möchte, kann dies auf der Datenschutz-Seite des Unternehmens durchgeführt werden. Nachfolgend zeigt Abbildung 13 einen Screenshot der entsprechenden Seite.

Abbildung 13: Opt-out Webseite des Unternehmens Intuit



Quelle: [https://privacy.intuit.com/cpi/do/preferences?dialog=1&hidenav=1&p_sourceid=208&p_prioritycode=null; Datum und Uhrzeit der Abfrage: 17. August 2008 15:17]

Empfänger:

Empfänger laut Compact Policy ist die Firma Intuit selbst, was auch in der Datenschutzerklärung angegeben wird. *„We do not sell or rent your personal information to anyone. We do not share your personal information with anyone outside of Intuit for their promotional, including marketing, use."* Intuit erklärt, dass die persönlichen Informationen der Kunden nicht an Dritte für Marketing- oder Werbekampagnen, verkauft oder vermietet werden. Es wird von Intuit eingeräumt, dass sie teilweise aufgrund beispielsweise von Kundenbestellungen auch Informationen an Dritte weitergeben, um diese Anfragen zu bearbeiten. Das Unternehmen garantiert, dass diese Drittunternehmen vertraglich dazu verpflichtet sind, die persönlichen Informationen nur für den jeweiligen Auftrag und nur zu dessen Abwicklung zu verwenden und nicht für eigene Marketingzwecke weiterzuverarbeiten. *„Sometimes, we enter into contracts with third parties who assist us in servicing you such as filling customer orders or providing customer service. The contracts outline the appropriate use and handling of your information and prohibit third parties from using any of your personal informa-*

tion for purposes unrelated to the product or service for which they've been contracted."

Retention/Einbehaltung:

In der Compact Policy, als auch in der Datenschutzerklärung, werden keine Angaben zur zeitlichen Einbehaltung der gesammelten Informationen gemacht.

Nachfolgend werden die Ergebnisse des Vergleichs der Compact Policy mit der Datenschutzerklärung in Tabelle 11 übersichtlich zusammengefasst.

Tabelle 11: Vergleich der Compact Policy mit der Datenschutzerklärung für das Unternehmen Intuit

Token	*Übereinstimmung der Compact Policy mit der Datenschutzerklärung?*
NOI	Nein, wenn man einen Online-Kauf tätigt, müssen persönliche Daten übermittelt werden. Dieser Token ist falsch.
DSP	Ja. Es wurde ein Datenschutz-Gütesiegel erwähnt.
CURa	Ja. Beispielsweise beim Online-Kauf.
ADMa	Ja. Mithilfe von Cookies
DEVa	Ja. Mithilfe von Cookies
TAIa	Ja. Mithilfe von Cookies
PSAa	Ja. Mithilfe von Web Bugs
PSDa	Ja. Mithilfe von Web Bugs
OUR	Ja. Es werden zwar persönliche Informationen an Dritte weitergegeben, aber nur zur Bearbeitung von Services und nicht für Marketingzwecke.
IND	Ja. Weder in der Compact Policy noch in der Datenschutzerklärung konnte eine Retention Policy gefunden werden.
UNI	Ja, wenn ein Account erstellt wird
COM	Ja. Durch Aufzeichnung seitens der Webseite
NAV	Ja. Durch Aufzeichnung seitens der Webseite
STA	Nein. In der Datenschutzerklärung wird der Einsatz von Cookies und Web Bugs erklärt, obwohl die Angabe des Tokens in der Compact Policy fehlt.

Quelle: Eigene Darstellung

4.1.1.2. Microsoft

Die Microsoft Corporation wurde im Jahr 1975 gegründet und ist ein multinationaler Softwareentwickler mit Sitz in Redmond, Washington. 2007 beschäftigte das Unternehmen rund 19.000 MitarbeiterInnen und erzielte einen Umsatz von 51 Milliarden Dollar[21].

Die Abfrage des HTTP Response Headers bei Microsoft ergab folgende Compact Policy:
`P3P: CP="ALL IND DSP COR ADM CONo CUR CUSo IVAo IVDo PSA PSD TAI TELo OUR SAMo CNT COM INT NAV ONL PHY PRE PUR UNI"` Für Informationen zu den einzelnen Token siehe Kapitel 3.1.3.

Vergleich der Compact Policy mit der, für den Menschen lesbaren, Datenschutzerklärung[22]

Nachfolgend werden die Ergebnisse des Vergleichs der Compact Policy mit der Datenschutzerklärung in Tabelle 12 übersichtlich zusammengefasst.

Tabelle 12: Vergleich der Compact Policy mit der Datenschutzerklärung für das Unternehmen Microsoft

Token	*Übereinstimmung der Compact Policy mit der Datenschutzerklärung?*
ALL	Ja. Die Compact Policy gibt an, dass Microsoft Zugriff auf alle zierbaren Daten hat. Dies spiegelt sich auch in der Datenschutzerklärung wider. Dort wird erläutert, dass in manchen Fällen persönliche onen von der Webseite abgefragt werden können. Dabei werden de Daten gesammelt: E-Mailadresse, Name, Wohnadresse, nummer und demografische Informationen wie Postleitzahl, Alter, Geschlecht, Vorlieben und Interessen. Wenn der/die NutzerIn sich für einen Kauf entscheidet oder sich für ein bezahltes Service anmeldet, werden darüber hinaus auch die Kreditkartennummer und Rechnungsadresse

[21] (vgl. http://de.wikipedia.org/wiki/Microsoft#cite_note-2007financials-0 Datum und Uhrzeit der Abfrage: 20. August 2008 14:20)
[22] Die Datenschutzerklärung von Microsoft findet man unter: http://www.microsoft.com/info/privacy/fullnotice.mspx Datum und Uhrzeit der Abfrage: 11. August 2008 16:07

	abgefragt.
IND	Ja. Sowohl in der Compact Policy als auch in der Datenschutzerklärung sind keine Angaben über die Dauer der Speicherung der gesammelten Daten zu finden. In der für den Menschen lesbaren Policy wird zwar angegeben, dass persönliche Daten gespeichert und weiterverarbeitet werden, aber es fehlt die Information darüber, wie lange diese Daten im Unternehmen verweilen. „*Personal information collected on Microsoft sites and services may be stored and processed in the United States or any other country in which Microsoft or its affiliates, subsidiaries or service providers maintain facilities."*
DSP	Ja. Das Gütesiegel TRUSTe wird in der Datenschutzerklärung genannt.
COR	Ja. In der Datenschutzerklärung wird erläutert, dass im Falle einer Überschreitung der Angaben in der Datenschutzerklärung, der/die NutzerIn sich mit Microsoft in Verbindung setzen kann. Sollte die Anfrage nicht in angemessener Zeit oder Ausmaß bearbeitet werden, kann man dies bei TRUSTe melden. Die Organisation versucht dann, gemeinsam mit Microsoft den Streitfall zu schlichten.
ADM	Ja. Siehe Token DEV.
CONo	Ja. Die persönlichen Daten des Kunden werden auch für Kommunikationszwecke genutzt. Dazu zählen zwingend notwendige Kommunikation wie Willkommensbriefe, Zahlungsaufforderungen, Informationen über technische Serviceprobleme und Sicherheitsankündigungen. Zusätzlich können auch Produktumfragen oder Werbemails an die Nutzer versendet werden.
CUR	Ja.
IVAo	Ja. Siehe Tokens TAI und DEV.
IVDo	Ja. Siehe Token TAI.
PSA	Ja. Siehe Tokens TAI und DEV.
PSD	Ja. Siehe Token TAI.
TAI	Ja. In der Datenschutzerklärung wird erklärt, dass für eine sche Gestaltung der Interaktionen mit Microsoft, Informationen melt und miteinander kombiniert werden. Diese Kombination von Infor-

	mationen kann auch mithilfe von nicht identifizierbaren Daten, welche beispielsweise auch von anderen Firmen stammen können, stattfinden. Als Beispiel wird ein Service genannt, mit dem die geografische Herkunft des Nutzers mithilfe der IP Adresse ermittelt werden kann. *„In order to offer you a more consistent and personalized experience in your interactions with Microsoft, information collected through one Microsoft service may be combined with information obtained through other Microsoft services. We may also supplement the information we collect with information obtained from other companies. For example, we may use services from other companies that enable us to derive a general geographic area based on your IP address in order to customize certain services to your geographic area."*
TELo	Nein. In der Datenschutzerklärung wird keine konkrete Angabe zu einem etwaigem Telefonkontakt zum Nutzer gemacht. Es wird lediglich die Möglichkeit der Registrierung einer Live ID mit der Telefonnummer erläutert.
OUR	Ja. Siehe Token SAMo.
SAMo	Ja. Als Empfänger, der gesammelten Daten, werden Microsoft und dessen Geschäftspartner, welche nach den Anweisungen von Microsoft handeln, genannt. Bei letzterem können sich die Nutzer von der Verwendung ihrer Daten ein- oder austragen. Dritte, an die bestimmte Services ausgelagert werden, übernehmen die Bearbeitung und Versendung von Postsendungen, bieten Kundensupport, Websitehosting, Transaktionsbearbeitung oder führen eine statistische Analyse der Microsoft-Services durch. Diese Dienstleistungsunternehmen sind vertragsmäßig daran gebunden die an sie übermittelten persönlichen Informationen vertraulich zu behandeln und es ist ihnen verboten sie für andere Zwecke zu nutzen. *„We occasionally hire other companies to provide limited services on our behalf, such as handling the processing and delivery of mailings, providing customer support, hosting websites, processing transactions, or performing statistical analysis of our services. (…) They are required to maintain the confidentiality of the information and are prohibited from using it for any other purpose."*

CNT	Nein, in der für den Menschen lesbaren Policy wird nicht erwähnt, dass die Kommunikation des Nutzers gespeichert wird.
COM	Ja. Microsoft sammelt Informationen über die Interaktionen des Nutzers auf der Microsoft Webseite und den Services. Des Weiteren werden Browserdaten aufgezeichnet. Dies inkludiert von welcher Seite man gekommen ist, welche Suchmaschinen und Keywords benutzt wurden, um die Seite zu finden, welche Seiten der Webseite angeschaut, welche Browser-Addons benutzt werden und die Darstellungsauflösung des Browsers. Darüber hinaus werden IP Adresse, Browsertyp und Sprache, sowie Zugriffszeit und die verweisende Webseitenadresse aufgezeichnet. Diese Angaben sind sowohl in der Compact Policy als auch in der Datenschutzerklärung zu finden.
INT	Ja. Siehe Token COM.
NAV	Ja. Siehe Token COM.
ONL	Ja. Microsoft sammelt (wie unter dem Token ALL w.o. bereits erwähnt) eine Vielzahl an persönlichen Informationen, welche sowohl in der Compact Policy als auch in der Datenschutzerklärung zu finden sind. *„At some Microsoft sites, we ask you to provide personal information, such as your e-mail address, name, home or work address, or telephone number. We may also collect demographic information, such as your ZIP code, age, gender, preferences, interests and favorites. If you choose to make a purchase or sign up for a paid subscription service, we will ask for additional information, such as your credit card number and billing address, which is used to create a Microsoft billing account."*
PHY	Ja. Siehe Token ONL.
PRE	Ja. Siehe Token ONL.
PUR	Ja. Siehe Token ONL.
UNI	Ja. Damit auf bestimmte Services von Microsoft zugegriffen werden kann, müssen Nutzer sich mit ihrer E-Mailadresse oder ihrer Telefonnummer registrieren. Dadurch wird dem Nutzer eine sog. Windows Live ID zugeschrieben.
DEM	Nein. Der Token fehlt in der Compact Policy, wird aber in der Datenschutzerklärung erwähnt. Siehe Token ONL.

STA	Nein. In der Datenschutzerklärung wird der Einsatz von Cookies und Web Bugs erklärt, obwohl die Angabe des Tokens in der Compact Policy fehlt. Diese Technologien werden eingesetzt, um Informationen darüber zu sammeln welche Seiten angeschaut, welche Links benutzt und welche anderen Aktionen auf der Webseite oder bei den Services durchgeführt wurden.
DEV	Nein. In der für den Menschen lesbaren Policy wird erklärt, dass Informationen zum Betreiben und zur Verbesserung der Seite und Services benutzt werden. Dazu gehört eine Verbesserung der Effizienz des Kundenservices, der Wegfall der erneuten Eingabe von kundenspezifischen Information wodurch eine Erleichterung in der Handhabung der Seite und Services zum Ergebnis kommt, Durchführung von Untersuchungen und Analysen, um Produkte, Services und Technologien zu verbessern und des Weiteren die Darstellung des Inhalts und der Werbung welche auf die Interessen und Präferenzen des *„Microsoft collects and uses your personal information to operate and improve its sites and services. These uses may include providing you with more effective customer service; making the sites or services easier to use by eliminating the need for you to repeatedly enter the same information; performing research and analysis aimed at improving our products, services and technologies; and displaying content and advertising that are customized to your interests and preferences."*

Quelle: Eigene Darstellung

Im sogenannten „Profile Center" können Nutzer der Microsoft Webseite jederzeit ihre persönlichen Informationen einsehen oder bearbeiten. Im Center können sie sich auch von der Zusendung von Werbematerial, der Weitergabe von Kontaktinformationen von Dritten und vom Newsletter ein- beziehungsweise austragen. Nachfolgend zeigt Abbildung 14 einen Screenshot des Profile Centers.

Abbildung 14: Screenshot des Profile Centers von Microsoft

Quelle: [https://profile.microsoft.com/RegSysProfileCenter/default.aspx?lcid=1033 Datum und Uhrzeit der Abfrage: 20. August 2008 14:30]

Des Weiteren gibt es auch eine spezielle Seite, um sich von der personalisierten Werbung von Microsoft auszutragen. Abbildung 15 zeigt einen Screenshot der soeben genannten Webseite.

Abbildung 15: Screenshot der Opt-out Seite bezüglich personalisierter Werbung von Microsoft

Quelle: [https://choice.live.com/advertisementchoice/Default.aspx Datum und Uhrzeit der Abfrage: 20. August 2008 14:35]

4.1.1.3. AT&T

Die AT&T Inc. wurde 1885 gegründet und ist ein amerikanischer Telekommunikationskonzern mit Sitz in San Antonio, Texas. Zu den Kunden von AT&T zählen Unternehmen, Privatkunden und Regierungsorganisationen. Die vom Unternehmen angebotenen Leistungen umfassen Telefon-, Daten- und Videotelekommunikation, sowie Mobilfunk und Internetdienstleistungen. Im Jahr 2007 erzielte das Unternehmen einen Umsatz von 118 Milliarden US-Dollar und beschäftigte 2006 179.420 Mitarbeiter.[23]

Die Abfrage des HTTP Response Headers bei Microsoft ergab folgende Compact Policy:
`P3P: policyref="http://www.att.com/w3c/p3p.xml",CP="CAO DSP COR LAW CURa ADMa DEVa TAIa PSAa PSDa IVAo IVDo CONo TELo OUR OTRi IND PHY ONL UNI PUR COM NAV INT DEM CNT STA PRE GOV"` Informationen zu den einzelnen Token können Kapitel 3.1.3 entnommen werden.

Vergleich der Compact Policy mit der für den Menschen lesbaren, Datenschutzerklärung:[24]

Nachfolgend werden die Ergebnisse des Vergleichs der Compact Policy mit der Datenschutzerklärung in Tabelle 13 übersichtlich zusammengefasst.

Tabelle 13:Vergleich der Compact Policy mit der Datenschutzerklärung für das Unternehmen AT&T

Token	*Übereinstimmung der Compact Policy mit der Datenschutzerklärung?*
CAO	Ja. Es werden laut Datenschutzerklärung persönliche Informationen der Kunden gesammelt. Dazu zählen Informationen die von den Nutzern selbst übermittelt werden, Informationen die durch die Kundenbeziehung hen und Daten aus anderen Quellen. Als Beispiele werden genannt: Name, Adresse, E-Mailadresse, Telefonnummer, Gebührenerfassung, Bezahlung, Nutzung, Kredit und Transaktionsinformationen (dazu gehört die

[23] (vgl. http://de.wikipedia.org/wiki/AT%26T Datum und Uhrzeit der Abfrage: 26. August 2008 14:35)
[24] Die Datenschutzerklärung von AT&T findet man unter: http://www.att.com/gen/privacy-policy?pid=7666#3 Datum und Uhrzeit der Abfrage: 22. August 2008 13:38

	tennummer, Kontonummer und/oder Sozialversicherungsnummer) und demografische Informationen.
DSP	Ja. Es werden TRUSTe und BBBOnLine als Konfliktstellen in der Datenschutzerklärung genannt.
COR	Ja. Als Rechtsmittel werden AT&T und die Gütesiegel genannt.
LAW	In der Datenschutzerklärung konnten keine Angaben zu einem Recht gefunden werden, welches gilt, wenn es zu einem Bruch der Datenschutzerklärung kommt.
CURa	Ja.
ADMa	Ja. Siehe Token DEVa.
DEVa	Ja. Siehe auch Token PSAa. Laut Datenschutzerklärung werden die von den Kunden übermittelten Daten zur Überwachung und Lösung von Problemen mit der Qualität, sowie zur Weiterentwicklung und zum Verkauf der Produkte und Services von AT&T verwendet.
TAIa	Ja. Siehe auch Tokens STA und PSAa. Um den Kunden eine maßgeschneiderte Webseite zu bieten und um diese auch verbessern zu können, werden Cookies eingesetzt. Des Weiteren werden auch Web Bugs zur Kontrolle der Aktivitäten auf der Webseite oder zur Verbesserung des Einsatzes von Cookies genutzt.
PSAa	Ja. Siehe auch Token STA. Die Informationen die aus der Nutzung der Seite gesammelt werden, werden gemäß AT&T dazu genutzt, um Trends abschätzen zu können und um Design, Kontrolle und eine leichtere Nutzung der Seite, sowie eine effizientere Marketingkommunikation zu ermöglichen. Dabei können auch aggregierte Informationen über das Kundenverhalten gesammelt werden. Diese kombinierten Informationen sollen dem Unternehmen helfen, kundenspezifische Features, Services und Werbung zu implementieren.
PSDa	Ja. Siehe Token PSAa.
IVAo	Ja. Siehe auch Token STA. Laut Datenschutzerklärung werden persönliche, identifizierbare Informationen verschiedener Kunden zusammengefasst, um Daten von Gruppen oder Kategorien von Services, Kunden oder Besuchern der Webseite zu erhalten. Bei dieser Datensammlung wird es nicht möglich sein, persönliche

	Informationen von einem bestimmten Nutzer wieder herzustellen.
IVDo	Ja. Siehe Token PSAa.
CONo	Ja. Gemäß der Datenschutzerklärung erhalten die Kunden, in periodischen Abständen, Werbeemails über bestimmte Services, Produkte oder Sonderangebote von AT&T. In diesen E-Mails ist immer ein „Opt-out"-Link enthalten, mit dem sich die Nutzer von diesem Service jederzeit austragen können.
TELo	Ja. AT&T gibt den Kunden die Möglichkeit sich von den Telefonmarketing-maßnahmen des Unternehmens auszutragen.
OUR	Ja. Das Unternehmen AT&T erklärt in seiner Datenschutzerklärung, dass keine persönlich, identifizierbaren Informationen an Dritte für Marketingzwecke weitergegeben werden. In der Policy heißt es weiter, dass persönliche Daten an Dritte weitergegeben werden, um bestimmte Funktionen oder Services im Auftrag von AT&T zu erfüllen. Diesen Unternehmen ist es untersagt, die an sie übermittelten Informationen für andere Zwecke, als den ihnen aufgetragenen, zu nutzen. *„When we provide such personal identifying information to third parties to perform such functions or services on our behalf, we require that they protect personal identifying information consistent with this policy and do not allow them to use such information for other purposes."*
OTRi	Nein. Es konnte keine Erklärung, in der für den Menschen lesbaren Policy, über die Weitergabe von persönlichen Daten an Dritte, die nicht den Handelspraktiken von AT&T folgen, gefunden werden.
IND	Ja. Weder in der Compact Policy noch in der Datenschutzerklärung sind Informationen über die Dauer der Speicherung der gesammelten Daten zu finden.
PHY	Ja. Siehe Token CAO.
ONL	Ja. Siehe Token CAO.
UNI	Ja. Den Kunden von AT&T wird eine sog. CPNI zugeschrieben, eine ID welche die gekauften Telekommunikationsservices, deren Nutzung und die dazugehörigen Zahlungsinformationen beinhaltet. Daten wie Telefonnummer, Name und Adresse werden in der CPNI nicht gespeichert.
PUR	Ja. Siehe Token CAO.

COM	Ja. In der Datenschutzerklärung wird erläutert, dass durch die Nutzung der Webseite automatisch die IP-Adresse, der Browsertyp, das Betriebssystem und die Webseite, von der aus die Seite von AT&T angesteuert wurde, aufgezeichnet werden.
NAV	Ja. Siehe Token STA.
INT	Ja. Siehe Token STA.
DEM	Ja. Siehe Token CAO.
CNT	Nein. Es konnten keine Angaben in der Datenschutzerklärung, über die Aufzeichnung der Kommunikation des Kunden, gefunden werden.
STA	Ja. Der Einsatz von Cookies und Web Bugs wird in der für den Menschen lesbaren Policy erläutert. Dabei sollen vor allem Informationen über das Surfverhalten der Nutzer, Präferenzen und Effizienz der Marketingkampagnen und E-Mailkommunikation gesammelt werden. *„Cookies can contain a variety of information, such as a simple count of how often you visit a Web site or information that allows us to customize our Web site for your use. Web beacons (also known as "clear gifs" or "one-pixel gifs") are small graphic images on a Web page or in an e-mail that allow us to monitor the activity on our Web sites or to make cookies more effective. (…) We also use cookies to store user preferences, complete online order activity and keep track of transactions.“*
PRE	Ja. Siehe Token STA.
GOV	Ja. Die Sozialversicherungsnummer wird beim Kauf verlangt.

Quelle: Eigene Darstellung

4.1.1.4. The Walt Disney Company

1923 wurde The Walt Disney Company (umgangssprachlich nur Disney genannt) von den Brüdern Walt und Roy Disney gegründet. Disney ist heute ein amerikanischer Medienkonzern mit Sitz in Burbank, Kalifornien. Weltweite Bekanntheit erlangte der Konzern durch seine Produktion von Zeichentrick- und Unterhaltungsfilmen für Kinder. 2008 beschäftigt das Unternehmen rund 137.000 MitarbeiterInnen und erzielte 2007 einen Umsatz von 35,51 Milliarden US-Dollar[25].

[25] (vgl. http://de.wikipedia.org/wiki/Disney ,Datum und Uhrzeit der Abfrage: 26. August 2008 14:45)

Die Abfrage des HTTP Response Headers bei Disney ergab folgende Compact Policy:

```
CP="CAO DSP COR CURa ADMa DEVa TAIa PSAa PSDa IVAi IVDi CONi
OUR SAMo OTRo BUS PHY ONL UNI PUR COM NAV INT DEM CNT STA PRE"
```

Eine Definition der einzelnen Token befindet sich in Kapitel 3.1.3.

Vergleich der Compact Policy mit der für den Menschen lesbaren, Datenschutzerklärung[26]

Nachfolgend werden die Ergebnisse des Vergleichs der Compact Policy mit der Datenschutzerklärung in Tabelle 14 übersichtlich zusammengefasst.

Tabelle 14: Vergleich der Compact Policy mit der Datenschutzerklärung für das Unternehmen Disney

Token	*Übereinstimmung der Compact Policy mit der Datenschutzerklärung?*
CAO	Ja. In der Datenschutzerklärung von Disney wird erläutert, dass persönlich identifizierbare Informationen von den Gästen selbst an sie übermittelt werden. Dazu zählen Name, Adresse, E-Mailadresse, Telefonnummer. Darüber hinaus werden Geschlecht, Alter, Anzahl der Kinder und persönliche Interessen aufgezeichnet.
DSP	Ja. Es wird TRUSTe als Konfliktstelle in der Datenschutzerklärung genannt.
COR	Ja. Sollte es zu einem Bruch der Angaben der Datenschutzerklärung kommen, kann laut Compact Policy und Datenschutzerklärung das Unternehmen selbst kontaktiert werden. Sollte die Anfrage nicht ordnungsgemäß bearbeitet oder erfüllt werden, dann können sich Nutzer auch an TRUSTe wenden. *„If you have questions or wish to send us comments about this Privacy Policy, please send an e-mail with your questions or comments to ms_support@help.go.com or write us."* (Anmerkung: Adresse wurde gelöscht).
CURa	Ja.

[26] (vgl. http://disney.go.com/corporate/privacy/pp_wdig.html Datum und Uhrzeit der Abfrage: 11.August 2008 16:11)

ADMa	Ja. Siehe Token TAIa.
DEVa	Ja. Siehe Token TAIa.
TAIa	Ja. Siehe auch Token IVAi. Durch den Einsatz von technischen Hilfsmitteln zur Analyse der Aktivitäten auf der Webseite werden gemäß der Datenschutzerklärung von Disney die Inhalte an die Nutzer angepasst, das Surfverhalten verfolgt und die Wahrnehmung der Webseite verbessert. *„We may use the information collected through these technical methods for many purposes, including delivering content, tracking and enhancing our guests' experience on our Web sites."*
PSAa	Ja. In der Datenschutzerklärung werden Analysen mit nicht-identifizierbaren Daten erwähnt. *"The Walt Disney Family of Companies may take your personally identifiable information and make it non-personally identifiable, either by combining it with information about other individuals or by removing characteristics that make the information personally identifiable to you."*
PSDa	Ja. Siehe Token TAIa.
IVAi	Ja. Gemäß Datenschutzerklärung werden die gesammelten IP-Adressen mit persönlichen Daten kombiniert, um Analysen darüber machen zu können, wie häufig bestimmte Webseiten von einem Nutzer angesehen werden. Darüber hinaus werden auch die an die Nutzer versendeten E-Mails zur Beobachtung des Verhaltens genutzt. Dabei wird aufgezeichnet, ob die E-Mails geöffnet oder weitergeleitet wurden und ob Links benutzt wurden. Diese Analysen sollen helfen, Werbung und Inhalte der Nachrichten kundenspezifisch gestalten zu können und zu analysieren, ob die Marketingmaßnahmen erfolgreich waren.
IVDi	Ja. Siehe Token IVAi.
CONi	Ja. Die von den Nutzern übermittelten Kontaktinformationen werden von Disney und Dritten dazu genutzt, um Werbung zu versenden. Die Werbesendungen können via Post, E-Mail oder anderen Mitteln durchgeführt werden.

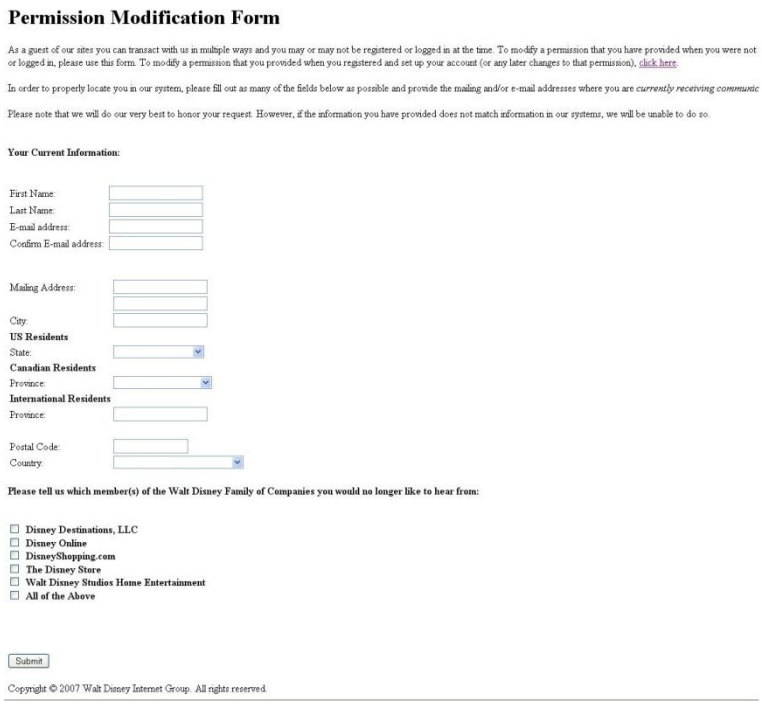
	„The Walt Disney Family of Companies may use your personal information to send you promotional materials about goods and services (including special offers and promotions) either offered by The Walt Disney Family of Companies or offered by third parties. These promotional materials may be sent to you by postal mail, e-mail or other means. You may opt out of receiving these communications as provided below."
OUR	Ja. Empfänger gemäß Datenschutzerklärung sind Disney selbst, Dritte die als Agenten agieren und daher den Handelspraktiken von Disney folgen sowie Dritte die keine Agenten sind. In der Datenschutzerklärung wird erläutert, dass persönlich identifizierbare Informationen, welche an Disney übermittelt wurden, im ganzen Unternehmen für Marketingzwecke genutzt werden („The Walt Disney Family of Companies") und auch an Dritte für Marketingzwecke weitergeleitet werden. Dabei wird aber sofort auf die Opt-out Möglichkeit von Werbezusendungen hingewiesen. *„As described in detail below, The Walt Disney Family of Companies may use your personally identifiable information in many ways, including sending you promotional materials, and sharing your information with third parties so that these third parties can send you promotional materials. As outlined below, you may "opt out" of certain uses of your personal*
SAMo	Ja. Siehe Token OUR.
OTRo	Ja. Siehe Token OUR.
BUS	Nein. Eine Erklärung über die Dauer der Speicherung der Daten konnte in der für den Menschen lesbaren Policy nicht gefunden werden, obwohl dies in der Compact Policy erklärt wird.
PHY	Ja. Siehe Token CAO.
ONL	Ja. Siehe Token CAO.
UNI	Ja.
PUR	Ja. In der Datenschutzerklärung wird die Sammlung beziehungsweise Aufzeichnung von Informationen aus dem Kauf eines Produktes oder Services (zum Beispiel Kreditkartennummer), Ausdrücke in Chats, Message Boards, etc. und Präferenzen der Kunden genannt. *(…) If you purchase products or services from us or another member of The*

	Walt Disney Family of Companies, we'll note, for example, credit card formation, the type of services or products ordered or purchased, and the date of the order or purchase. (...) Finally, our Web sites may offer sage boards, conversation pages, chat rooms, social community ments, profile pages, and other Public Forums (…), as well as other tures in which you may provide us with User Submissions. If you provide personal information when you use any of these features, that personal information may be publicly posted and otherwise disclosed without limitation as to its use by a third party."
COM	Ja. Gemäß der Datenschutzerklärung werden Informationen über das Computersystem des Nutzers automatisch gesammelt. „*(…)For instance, when you come to one of our sites, we collect your IP address."*
NAV	Ja. Siehe Token STA.
INT	Ja.
DEM	Ja. Siehe Token CAO.
CNT	Ja. Siehe Token PUR.
STA	Ja. Der Einsatz von Cookies und Web Bugs wird in der Datenschutzerklärung erläutert. Durch diese technischen Hilfsmittel sollen die Seiten ermittelt werden, die von den Nutzern häufig angeschaut werden. *„We also may use technical methods to analyze the traffic patterns on our Web sites, such as the frequency with which our users visit various parts of our Web sites."*
PRE	Ja. Siehe Tokens CAO und PUR.

Quelle: Eigene Darstellung.

Disney bietet in der Datenschutzerklärung eine Opt-out Webseite, um sich von der Unternehmensgruppe austragen zu können. Nachfolgend stellt Abbildung 16 einen Screenshot der Webseite dar.

Abbildung 16: Screenshot der Opt-out Webseite von Disney



Permission Modification Form

As a guest of our sites you can transact with us in multiple ways and you may or may not be registered or logged in at the time. To modify a permission that you have provided when you were not or logged in, please use this form. To modify a permission that you provided when you registered and set up your account (or any later changes to that permission), click here.

In order to properly locate you in our system, please fill out as many of the fields below as possible and provide the mailing and/or e-mail addresses where you are *currently receiving communic*

Please note that we will do our very best to honor your request. However, if the information you have provided does not match information in our systems, we will be unable to do so.

Your Current Information:

First Name:
Last Name:
E-mail address:
Confirm E-mail address:

Mailing Address:
City:
US Residents
State:
Canadian Residents
Province:
International Residents
Province:

Postal Code:
Country:

Please tell us which member(s) of the Walt Disney Family of Companies you would no longer like to hear from:

- **Disney Destinations, LLC**
- **Disney Online**
- **DisneyShopping.com**
- **The Disney Store**
- **Walt Disney Studios Home Entertainment**
- **All of the Above**

Submit

Copyright © 2007 Walt Disney Internet Group. All rights reserved.

Quelle: [https://register.go.com/global/nrtOptInOptOut/optOut Datum und Uhrzeit der Abfrage: 28. August 2008-08-28 13:40]

4.1.1.5. Barnes & Noble

Die Barnes & Noble Inc. ist einer der größten amerikanische Buchhändler und wurde ursprünglich 1873 von Charles M. Barnes in Illinois gegründet. Der Firmensitz befindet sich nun in New York. Das Unternehmen beschäftigte 2007 rund 51.000 MitarbeiterInnen und erzielte im Jahr 2006 einen Umsatz von 5,3 Milliarden US-Dollar.[27]

Die Abfrage des HTTP Response Headers bei Barnes & Noble ergab folgende Compact Policy:
`P3P: CP="CAO DSP COR ADM DEV TAI PSA IVDo CONo HIS TELo DEL SAMo UNRo LEG PRE"` Informationen zu den einzelnen Token sind in Kapitel 3.1.3 zu finden.

Nachfolgend werden die Ergebnisse des Vergleichs der Compact Policy mit der Datenschutzerklärung[28] in Tabelle 15 übersichtlich zusammengefasst.

[27] (vgl. http://en.wikipedia.org/wiki/Barnes_and_noble; Datum und Uhrzeit der Abfrage: 26. August 14:57)
[28] Die Datenschutzerklärung von Barnes & Noble findet man unter:
http://www.barnesandnoble.com/help/cds2.asp?PID=8104&
Datum und Uhrzeit der Abfrage: 11. August 2008 16:12

Tabelle 15: Vergleich der Compact Policy mit der Datenschutzerklärung für das Unternehmen Barnes & Noble

Token	*Übereinstimmung der Compact Policy mit der Datenschutzerklärung?*
CAO	Ja. Je nachdem welche Services auf der Webseite genutzt werden, kann es zu einer Sammlung von persönlichen Daten kommen. *„The information that we receive and collect depends on what you do when you visit Barnes & Noble.com.*
DSP	Nein. In der Datenschutzerklärung konnte keine Schlichtstelle ausfindig gemacht werden.
COR	Ja. Sollte man Fragen bezüglich der Datenschutzerklärung haben, kann man sich an eine spezielle Datenschutz E-Mailadresse von Barnes & Noble wenden.
ADM	Ja. Siehe Token DEV.
DEV	Ja. Es werden Informationen gesammelt, um die Webseite zu verbessern und die Nutzung zu erleichtern. *“We use cookies to enhance the browsing and shopping experience on the Barnes & Noble.com site.”*
TAI	Ja. Durch den Einsatz von Cookies, werden Werbung und Inhalt der Webseite auf die Kunden maßgeschneidert. *“If you turn off the third-party distributor's cookies, you will still see banners on our site; however, the banners will not be tailored to your shopping experience.”*
PSA	Ja. Es werden automatisch Daten gesammelt, um Analysen zu machen ohne dass dabei persönliche Informationen verbunden werden. *„All of the information we automatically capture provides us with the ability to enhance our customers' search and shopping experiences and to determine aggregate information about our user base and usage patterns.”*
IVDo	Ja. Die Werbung auf der Webseite wird auf die Präferenzen des Kunden angepasst.
CONo	Ja. Es wird Werbung an die Kunden verschickt.

	"Occasionally, Barnes & Noble.com uses Personal Customer Information to market products and services."
HIS	Nein. Informationen über die Speicherung der gesammelten Informationen zur Bewahrung der Sozialgeschichte konnten in der Datenschutzerklärung nicht gefunden werden.
TELo	Ja. Die Kontaktaufnahme via Telefon wird in der Compact Policy und in der Datenschutzerklärung erwähnt. *"As a Barnes & Noble.com account holder, we communicate via e-mail, postal mail and outbound telephone calls depending upon your settings in you Communications Preferences; as a purchaser without a Barnes & Noble.com account, we may communicate to you via e-mail."*
DEL	Ja. Es wird in beiden Policies erwähnt, dass Services und Produkte auch von Drittanbietern stammen und Informationen aus diesem Grund weitergegeben werden. *"We send Personal Customer Information to third-party providers of goods and services that you may purchase from time to time on our site (e.g., prints and posters). Like subcontractors, these third parties do not have the right to use the Personal Customer Information beyond what is necessary to assist us. They are contractually obligated to maintain the confidentiality and security of the Personal Customer Information and are restricted from using such information in any way not expressly authorized by Barnes & Noble.com."*
SAMo	Ja. Sowohl in der Compact Policy als auch in der Datenschutzerklärung wird die Weitergabe von persönlichen Daten an Dritte, welche nach den Handelspraktiken von Barnes & Noble handeln, erwähnt. *"We send Personal Customer Information to third-party subcontractors and agents that work on our behalf to provide certain services. These third ties do not have the right to use the Personal Customer Information beyond what is necessary to assist us. They are contractually obligated to maintain the confidentiality and security of the Personal Customer Information and*

	are restricted from using such information in any way not expressly authorized by Barnes & Noble.com."
UNRo	Ja. Die Weitergabe von persönlichen Informationen wird in beiden Policies erwähnt. Auch die Möglichkeit der Austragung aus dem Service wird in der Datenschutzerklärung angegeben. *"From time to time, on limited basis, we may share with entities affiliated with Barnes & Noble.com (e.g., Barnes & Noble Booksellers and Barnes & Noble Membership) contact information of our account holders and individuals that makes purchase without an account so that such entities can promote special offers, events, new products and services."*
LEG	Nein. Informationen über die Dauer der Speicherung von persönlichen Informationen konnten in der Datenschutzerklärung nicht gefunden werden.
PRE	Ja. Siehe Token TAI.
STA	Nein, der Einsatz von Cookies und Web Bugs wird nicht in der Compact Policy, aber in der Datenschutzerklärung angegeben. (siehe Token DEV für ein Zitat über den Einsatz von Cookies aus der Datenschutzerklärung)
COM	Nein, die Speicherung von Informationen über das Computersystem des Nutzers wird in der Compact Policy nicht angegeben. In der Datenschutzerklärung wird aber erläutert, dass Domainname, Host, IP-Adresse, Computeradresse, Browsertyp und Betriebssystem, sowie Datum und Uhrzeit des Zugriffs auf die Webseite und die Internetadresse von der aus man die Seite besucht, aufgezeichnet werden. *"We receive and collect the name of the domain and host from which you access the Internet; the Internet protocol (IP) address of the computer you are using; the browser software you use and your operating system; the date and time you access our site; and the Internet address of the web site from which you linked directly to our site."*
OUR	In der Compact Policy fehlt dieser Token, obwohl in der Datenschutzerklärung erläutert wird, dass beispielsweise bei der Erstellung eines Accounts Name und E-Mailadresse angegeben werden müssen. *"You can create a password-protected Barnes & Noble.com account to*

	complete an order or to save items in your Wish List. To create an account, we require that you provide us with the following Personal Customer Information: your email address (…) and your first and last names."
PUR	Nein. Dieser Token fehlt in der Compact Policy, obwohl in der Datenschutzerklärung erwähnt wird, dass Daten beim Kauf eines Produktes oder Services gespeichert werden. *„If you have a Barnes & Noble.com account that you want to use to complete an order, we will require you to access that account. We will then use the Personal Customer Information stored in that account to complete the order, or require you to input additional Personal Customer Information such as payment information."*

Quelle: Eigene Darstellung

4.1.1.6. Aéropostale

Aéropostale ist ein amerikanischer Einzelhändler für Bekleidung mit Sitz in New York. Die Zielgruppe des Unternehmens sind Teenager im Alter von 14 bis 17 Jahren. 2006 erwirtschaftete Aéropostale einen Umsatz von 1,2 Milliarden US-Dollar und beschäftigte 2007 mehr als 10.500 MitarbeiterInnen[29].

Die Abfrage des HTTP Response Headers bei Aeropostale ergab folgende Compact Policy:
`P3P: CP="PHY ONL CAO CURa ADMa DEVa TAIa PSAa PSDa IVAo IVDo CONo HISa TELo OTPo OUR DELa STP BUS UNI COM NAV INT DEM OTC",policyref="/w3c/p3p.xml"` Die Bedeutungen der einzelnen Token findet man in Kapitel 3.1.3.

Nachfolgend werden die Ergebnisse des Vergleichs der Compact Policy mit der Datenschutzerklärung[30] in Tabelle 16 übersichtlich zusammengefasst.

[29] (vgl. http://en.wikipedia.org/wiki/A%C3%A9ropostale_%28clothing%29; Datum und Uhrzeit der Abfrage: 26. August 2008 15:55)
[30] Die Datenschutzerklärung von Aéropostale findet man unter:
http://www.aeropostale.com/helpdesk/index.jsp?display=safety&subdisplay=privacy
Datum und Uhrzeit der Abfrage: 02. September 2008 14:01

Tabelle 16: Vergleich der Compact Policy mit der Datenschutzerklärung für das Unternehmen Aéropostale

Token	*Übereinstimmung der Compact Policy mit der Datenschutzerklärung?*
PHY	Ja. Es werden sowohl physische als auch online Kontaktinformationen gesammelt. *"For example, when you open an account or place an order, we collect and store some or all of the following information that you provide: name, billing address, shipping address, email address, telephone number, credit card number and expiration date ("Personal Information")."*
ONL	Ja. Siehe oben Token PHY.
CAO	Ja. Siehe oben Token PHY.
CURa	Ja.
ADMa	Ja. Siehe weiter unten Token COM.
DEVa	Ja. Siehe auch weiter unten Token COM. *"Cookies help us to identify account holders and to optimize their shopping experience."*
TAIa	Ja. Siehe weiter unten Token COM.
PSAa	Ja. Siehe weiter unten Token COM.
PSDa	Ja. Siehe weiter unten Token COM.
IVAo	Ja. Siehe weiter unten Token COM.
IVDo	Ja. Siehe weiter unten Token COM.
CONo	Ja. Gemäß Compact Policy und Datenschutzerklärung werden persönliche Informationen dazu genutzt, um dem Kunden Werbung zuzusenden. *"Some of this information also may be used to contact you about sales, special offers, and new site features, unless you have opted not to receive promotional communications in connection with this Web Site."*
HISa	In der Datenschutzerklärung konnten keine Angaben zur Speicherung der Daten zum Zweck der Sozialgeschichte gefunden werden.
TELo	Ja. Werbung via Telefon wird in der Datenschutzerklärung erwähnt.
OTPo	Aus der Datenschutzerklärung ist nicht genau ersichtlich welcher anderer Zweck zur Datensammlung durch dieses Token repräsentiert wird.

OUR	Ja. Auf die persönlichen Daten der Nutzer haben nur Aéropostale und deren Tochterunternehmen sowie Unternehmen, welche Dienstleistungen an sie erbringen, Zugriff. Die Daten dürfen von den Dienstleistungsunternehmen nicht für andere Zwecke verwendet werden. *"We may share personal information that you provide to us through this Web Site or through this Web Site's Customer Service Department with our affiliates and with our service providers. These service providers are authorized to use this personal information only in connection with the services they are engaged to perform."*
DELa	Ja. Siehe oben Token OUR.
STP	Nein. In der Datenschutzerklärung konnte keine Retention Policy ausfindig gemacht werden.
BUS	Nein. In den Nutzungsbedingungen konnten keine Angaben über die Dauer der Speicherung der Daten gefunden werden.
UNI	Ja. Bei der Erstellung eines Accounts.
COM	Ja. Es werden Informationen über den Computer des Nutzers automatisch gesammelt. *„We collect and store certain other information automatically whenever you interact with this Web Site. For example, we collect your IP address, browser information and reference site domain name every time you visit this Web Site. We also collect information regarding customer traffic patterns and site usage. This information is used to analyze and improve this Web Site and to provide our customers with a fulfilling shopping experience."*
NAV	Ja. Siehe oben Token COM.
INT	Ja. *"Cookies help us to identify account holders and to optimize their shopping experience. Cookies also allow us to hold selections in a shopping cart when a user leaves this Web Site without checking out."*
DEM	Man findet keine eindeutigen Angaben zur Sammlung demografischer ten in der Datenschutzerklärung. Es gibt lediglich die Angabe, dass Infor-

	mationen von Drittanbietern gesammelt und abgespeichert werden, um die Datenbank zu ergänzen. *“We also may collect and store information about you that we receive from other sources, to enable us to update and correct the information contained in our database and to provide product recommendations and special offers that we think will interest you.”*
OTC	Das Zitat unter Token DEM (siehe oben) könnte sich aber auch auf die Sammlung anderer Daten beziehen, welche durch den Token OTC gekennzeichnet werden.
PUR	Nein. Dieser Token fehlt in der Compact Policy. Siehe oben Token PHY.
STA	Nein. Der Einsatz von Cookies wird zwar in der Datenschutzerklärung erläutert, der entsprechende Token fehlt aber in der Compact Policy. *“Also, like many Web sites, we use "cookies", which are files stored on your computer's hard drive by your browser.”*

Quelle: Eigene Darstellung

4.1.1.7. Dick’s Sporting Goods

Dick’s Sporting Goods ist ein amerikanischer Sportartikelhändler mit Firmensitz in Pittsburgh, Pennsylvania. Das Unternehmen wurde 1948 von dem damals 18jährigen Dick Stack gegründet und verkauft seine Waren primär in der östlichen Hälfte der USA in rund 348 Geschäften. 2007 wurde ein Umsatz von 3,88 Milliarden US-Dollar erzielt und rund 20.000 MitarbeiterInnen[31] beschäftigt.

Die Abfrage des HTTP Response Headers bei Dick’s Sporting Goods ergab folgende Compact Policy:
`P3P: CP="PHY ONL CAO CURa ADMa DEVa TAIa PSAa PSDa IVAo IVDo CONo HISa TELo OTPo OUR DELa STP BUS UNI COM NAV INT DEM OTC",policyref="/w3c/p3p.xml"` Eine Erläuterung zu den einzelnen Bedeutungen der Tokens sind in Kapitel 3.1.3 nachzuschlagen.

[31] (vgl. http://en.wikipedia.org/wiki/Dick%27s_Sporting_Goods sowie http://en.wikipedia.org/wiki/Dick%27s_Sporting_Goods Datum und Uhrzeit der Abfrage: 26. August 2008 16:00)

Nachfolgend werden die Ergebnisse des Vergleichs der Compact Policy mit der Datenschutzerklärung[32] in Tabelle 17 übersichtlich zusammengefasst.

Tabelle 17: Vergleich der Compact Policy mit der Datenschutzerklärung für das Unternehmen Dick's Sporting Goods

Token	*Übereinstimmung der Compact Policy mit der Datenschutzerklärung?*
PHY	Ja. Sowohl physische als auch online Kontaktinformationen werden beim Kauf eines Produktes oder Services gespeichert.
ONL	Ja. Siehe oben Token PHY.
CAO	Ja. Siehe oben Tokens PHY und weiter unten OTPo.
CURa	Ja.
ADMa	Ja. Siehe Tokens TAIa, COM und STA
DEVa	Ja. Siehe Tokens TAIa, COM und STA
TAIa	Ja. Siehe auch Tokens COM und STA Anhand der Kaufgewohnheiten werden Produktempfehlungen an den Kunden angepasst. *"From time to time, we may use the purchases you make to customize our product recommendations. We also track customer traffic patterns and site usage. Traffic and usage data is used only to improve our site's design and provide our customers with a fulfilling shopping experience."*
PSAa	Ja. Siehe Tokens TAIa, COM und STA. *"Additionally, we may share non-personal, non-individual statistical information with our marketing partners, advertisers or other third parties for research purposes. That is, we will not tell our marketing partners that you purchased a specific product, but we may tell them how many customers purchased that product."*
PSDa	Ja. Siehe Tokens TAIa, COM, PSAa und STA.
IVAo	Ja. Siehe Tokens TAIa, COM, PSAa und STA.
IVDo	Ja. Siehe Tokens TAIa, COM, PSAa und STA.

[32] Die Datenschutzerklärung von Dick's Sporting Goods findet man unter: http://www.dickssportinggoods.com/helpdesk/index.jsp?display=safety&subdisplay=privacy Datum und Uhrzeit der Abfrage: 02. September 2008 14:04

CONo	Ja. Dem Kunden werden beispielsweise Produktempfehlungen geschickt. (Siehe oben Token TAIa) Des Weiteren werden Informationen über Ausverkäufe, Sonderangebote oder neue Funktionen der Webseite via E-Mails an die Nutzer versendet. *"From time to time, we may contact you about sales, special offers and new site features if you agreed to be included in our email lists when you completed a purchase transaction with us."*
HISa	In der Datenschutzerklärung konnten keine Angaben zur Speicherung der Daten zum Zweck der Sozialgeschichte gefunden werden.
TELo	Ja. Siehe unten Token OTPo.
OTPo	Es konnten keine konkreten Angaben zu anderen Zwecken der Datensammlung in der für den Menschen lesbaren Policy gefunden werden.
OUR	Ja. Die persönlichen Informationen der Nutzer werden nur im Unternehmen selbst und an Dritte welche den Anweisungen von Dick's Sporting Goods unterstehen, weitergegeben. *„Certain vendors of ours may provide customer order fulfillment and shipping services on our behalf. These vendors have access only to information needed to accurately fulfill and ship orders, which are processed through such vendors. These vendors have agreed to not use any personally identifiable information of customers for any other purpose."*
DELa	Ja. Siehe oben Token OUR.
STP	Nein. In der Datenschutzerklärung konnte keine Retention Policy gefunden werden.
BUS	Nein. Siehe oben Token STP.
UNI	Ja. Bei der Erstellung eines Accounts auf der Webseite.
COM	Ja. Informationen über den Computer des Nutzers, mit dem die Webseite besucht wird, werden automatisch aufgezeichnet. *"Your IP address, browser and reference site domain name are logged every time you visit the Web Store. This data is used strictly for the analysis of load information and maximizing the efficiency of our servers."*
NAV	Ja. Siehe Tokens COM und STA.

INT	Ja. Siehe Tokens COM und STA.
DEM	Es gibt keine genaue Angabe zur Sammlung von demografischen Daten in der Datenschutzerklärung. Bei der Erstellung eines Accounts auf der Webseite werden zusätzliche freiwillig zu beantwortende Fragen gestellt. Dabei könnte es sein, dass auch demografische Daten gesammelt werden. (siehe Token OTC)
OTC	Ja. Wenn ein Nutzer sich auf der Webseite für einen Account registriert, werden optionale Fragen gestellt, um zusätzliche Informationen zu sammeln. *"We require your name, billing address, shipping address, email address and telephone number to open an account for you. We may also ask some additional optional questions to help us better serve you."*
STA	Nein. Der Einsatz von Cookies und Web Bugs wird zwar in der Datenschutzerklärung erläutert, aber der entsprechende Token fehlt in der Compact Policy. *"These cookies help us identify our account holders and optimize their shopping experience. They do not include any data that will identify you personally."* *"We may use third-party advertising companies to serve ads on our behalf. These companies may employ cookies and action tags (also known as single pixel gifs or web beacons) to measure advertising effectiveness. Any information that these third parties collect via cookies and action tags is completely anonymous."*
PUR	Nein. Dieser Token fehlt in der Compact Policy, obwohl in der Datenschutzerklärung darauf eingegangen wird. *„When you order from the Web Store, we need your name, email address, shipping address, phone number and credit card number/expiration date. We use this data to process your order, ship it and send you order and shipping confirmations via email."*

Quelle: Eigene Darstellung

4.1.1.8. Petsmart

Die Petsmart Inc. ist der führende Einzelhändler für Haustierbedarf und -services in den USA und Kanada. Das Unternehmen hat seinen Firmensitz in Phoenix, Arizona und wurde 1990 gegründet. 2007 verfügte Petsmart über 1.008 Filialen und beschäftigte 43.177 MitarbeiterInnen. Seit 1994 übernahmen die Kunden des Unternehmens 3.261.349 Tiere. 2007 wurde ein Umsatz von 4,5 Milliarden US-Dollar erzielt.[33]

Die Abfrage des HTTP Response Headers bei Petsmart ergab folgende Compact Policy:
`P3P: CP="PHY ONL CAO CURa ADMa DEVa TAIa PSAa PSDa IVAo IVDo CONo HISa TELo OTPo OUR DELa STP BUS UNI COM NAV INT DEM OTC",policyref="/w3c/p3p.xml"` Informationen zu den einzelnen Token sind in Kapitel 3.1.3 zu finden.

Nachfolgend werden die Ergebnisse des Vergleichs der Compact Policy mit der Datenschutzerklärung[34] in Tabelle 18 übersichtlich zusammengefasst.

Tabelle 18: Vergleich der Compact Policy mit der Datenschutzerklärung für das Unternehmen Petsmart

Token	*Übereinstimmung der Compact Policy mit der Datenschutzerklärung?*
PHY	Ja. Es werden sowohl physische als auch online Kontaktinformationen gesammelt. *„We want you to know that we value your privacy and are committed to responsible handling of your personal information (such as your name, physical address, e-mail address, and phone number), and we want you to know how we handle your information."*
ONL	Ja. Siehe oben Token PHY.
CAO	Ja. Siehe oben Token PHY.
CURa	Ja.

[33] (vgl. http://en.wikipedia.org/wiki/Petsmart und http://media.corporate-ir.net/media_files/IROL/93/93506/2007_AR.pdf Datum und Uhrzeit der Abfrage: 26. August 2008 16:25)
[34] Die Datenschutzerklärung von Petsmart findet man unter: http://www.petsmart.com/helpdesk/index.jsp?display=safety&subdisplay=privacy Datum und Uhrzeit der Abfrage: 02. September 2008 14:45

ADMa	Ja. *“We may also use that information to identify or resolve technical problems or customer service issues as necessary (…).”*
DEVa	Ja. Siehe Tokens CONo, PSAa, NAV, COM und TAIa.
TAIa	Ja. Siehe auch Tokens CONo und PSAa. Wenn Nutzer sich auf der Seite registrieren, werden Bestellformulare automatisch ausgefüllt und Angebote an die Präferenzen des Kunden angepasst. *“We may use your registration information to help make your online experience more enjoyable and orders quicker and easier, by pre-filling certain parts of your information.”* *“We use this information to administer the program; provide customer service; offer new products and services; measure and improve our marketing endeavors and service offerings; tailor our offerings to your preferences; and send you PetSmart Marketing Communications.”*
PSAa	Ja. Siehe auch Token TAIa und NAV. *“We may combine the personal information you provide to us (on our Site, at our stores, through our programs) with publicly available information and information we receive from or cross-reference with our marketing partners and others. We use the combined information to enhance and personalize your experience with us; improve the accuracy of our customer database (such as the U.S. Post Office to verify accuracy of addresses); increase our understanding of our customers; identify potential customers; and send PetSmart Marketing Communications.”*
PSDa	Ja. Siehe Tokens TAIa, PSAa und NAV.
IVAo	Ja. Siehe Tokens TAIa, PSAa und NAV.
IVDo	Ja. Siehe Tokens TAIa, PSAa und NAV.
CONo	Ja. Gemäß Datenschutzerklärung werden persönliche Informationen u.a. dazu genutzt, um Sonderangebote für Produkte und Services an die Kunden zu senden. Die Marketingmaßnahmen werden via Post, E-Mail und Telefon durchgeführt.

	„We may use your personal information to better assist you when you visit or call us again and to send you special offers for products and services that may be of interest to you. We do this by print advertising, including regular mail, by e-mail, by telephone, and with general marketing communications for product or service-specific information (collectively, "PetSmart Marketing Communications").”
HISa	In der Datenschutzerklärung konnten keine Angaben zur Speicherung der Daten zum Zweck der Sozialgeschichte gefunden werden.
TELo	Ja. Siehe Token CONo.
OTPo	Aus der Datenschutzerklärung sind keine anderen Gründe für die Sammlung von persönlichen Daten zu finden.
OUR	Ja. Die persönlichen Daten werden im Unternehmen selbst genutzt und nur an Dritte weitergegeben, die nach den Anweisungen von Petsmart arbeiten. *“We may share your personal information with carefully selected third-party service providers in order to provide services to you, such as to fulfill orders (..); process payments; provide customer service (…); monitor Site activity; conduct surveys; maintain our customer database; (…). We will share your personal information with our carefully selected third-party services providers on a confidential basis. These service providers are prohibited from using your personal information for any purpose other than providing PetSmart services.”*
DELa	Ja. Siehe oben Token OUR.
STP	Nein. In der Datenschutzerklärung konnte keine Retention Policy gefunden werden.
BUS	Nein. Siehe oben Token STP.
UNI	Ja. Wenn ein Account auf der Webseite erstellt wird, erhält man eine Nummer.
COM	Ja. Es werden Informationen über den Computer, mit dem die Webseite betrachtet wird, gesammelt. *“Our Site server may automatically collect the address of the Website that you came from before visiting our Site, which Web browser you used to*

	view our Site, and any search terms you have entered on our Site. Our Site may also use other technologies to track pages of our Site viewed by tors, commonly referred to as "tracer tags". This non-identifiable "click-stream" data helps us understand how visitors use our Site. "Click-stream" is the sequence of clicks or pages requested as a visitor explores a Web-site."
NAV	Ja. Es werden sowohl aktiv als auch passiv entstehende Daten durch das Betrachten der Webseite gesammelt. Siehe oben Token COM. *„For your information, we have carefully selected Omniture, a company that will assist us in better understanding your use of our Site. Omniture will place cookies on your computer to collect information on our behalf that will educate us on such things as search engine referral, how you navigate around our Site, responses to e-mail, unique visitor identification, and product browsing and purchasing information. Omniture is contractually prohibited from using our data for any other purposes. Omniture is required to maintain all information collected and its analysis in confidence."*
INT	Ja. Siehe oben Token NAV und COM.
DEM	Es gibt keine genaue Angabe zur Sammlung von demografischen Daten in der Datenschutzerklärung. Bei der Teilnahme an Umfragen oder Gewinnspielen werden zusätzliche, freiwillig zu beantwortende Fragen gestellt, dabei könnten auch demografische Daten gesammelt werden. Siehe Token PRE.
OTC	Ja. Siehe Zitat in Token PRE.
PUR	Nein. Der Token fehlt in der Compact Policy, obwohl in der Datenschutzerklärung darauf eingegangen wird. *„We may collect personal information when you: shop or take advantage of our products and/or services (…)"* *"When shopping our stores, if you use a credit/debit card for your purchases, we will collect your credit/debit card information in order to process your purchases and may use your information to keep a history of your purchases."*
PRE	Nein. Auf diesen Token wird in der Datenschutzerklärung insofern

	gangen, als dass Angebote an die Präferenzen der Kunden angepasst werden. Darüber hinaus wird in Token STA (siehe unten) auf die Sammlung der Präferenzen mittels Cookies eingegangen. Des Weiteren werden auch beispielsweise bei Gewinnspielen oder Umfragen zusätzliche Informationen gesammelt, wobei möglicherweise auch Präferenzen abgefragt werden. *"When participating in other PetSmart activities, such as entering a contest or sweepstake, registering for programs, or participating in a survey, or when you contact PetSmart with a question or concern, we may ask you to provide your name, physical address, phone number, e-mail address and other information about yourself and your pets to administer the activity and deliver PetSmart Marketing Communications to you."*
STA	Der Einsatz von Cookies wird zwar in der Datenschutzerklärung erläutert, das entsprechende Token fehlt aber in der Compact Policy. *"Our Site uses "cookie" technology. (…) Our Site uses cookies to simulate a continuous connection-cookies let us "remember" information about your preferences and session and allow you to move within areas of our Site without reintroducing yourself. No personally identifiable information is stored in these cookies."*

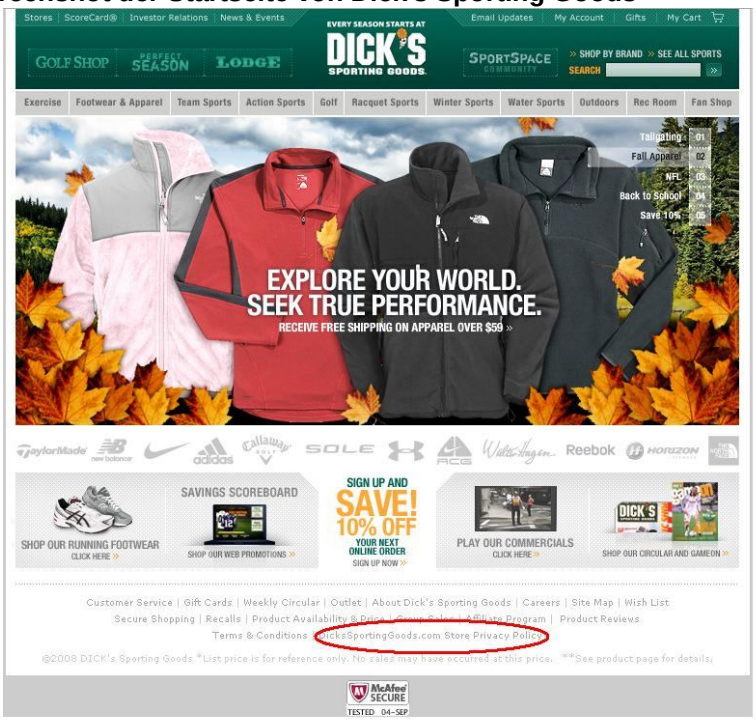
Quelle: Eigene Darstellung

4.1.2. Zusammenfassung der Ergebnisse

Der allgemeine Eindruck zu den untersuchten Datenschutzerklärungen war generell negativ, denn die Datenschutzerklärungen konnten oft auf der Seite der Unternehmen schwer ausfindig gemacht werden. Wie in Abbildung 17 sehr gut zu erkennen ist, wurde der Link zur Policy auf der Webseite von Dick's Sporting Goods in der allerletzten Zeile und zusätzlich in einer schwer lesbaren Farbe platziert. Des Weiteren sind die Datenschutzerklärungen im Allgemeinen sehr ausführlich geschrieben, was einerseits als positiv angesehen werden kann, aber sicherlich viele Nutzer abschreckt, diese überhaupt ganz zu lesen und zusätzlich das Verstehen des Textes auch erschwert. Zu dieser Problematik kommt darüber hinaus noch die Tatsache hinzu, dass die Erklärungen oft mit einer sehr großen Anzahl an Links verknüpft sind,

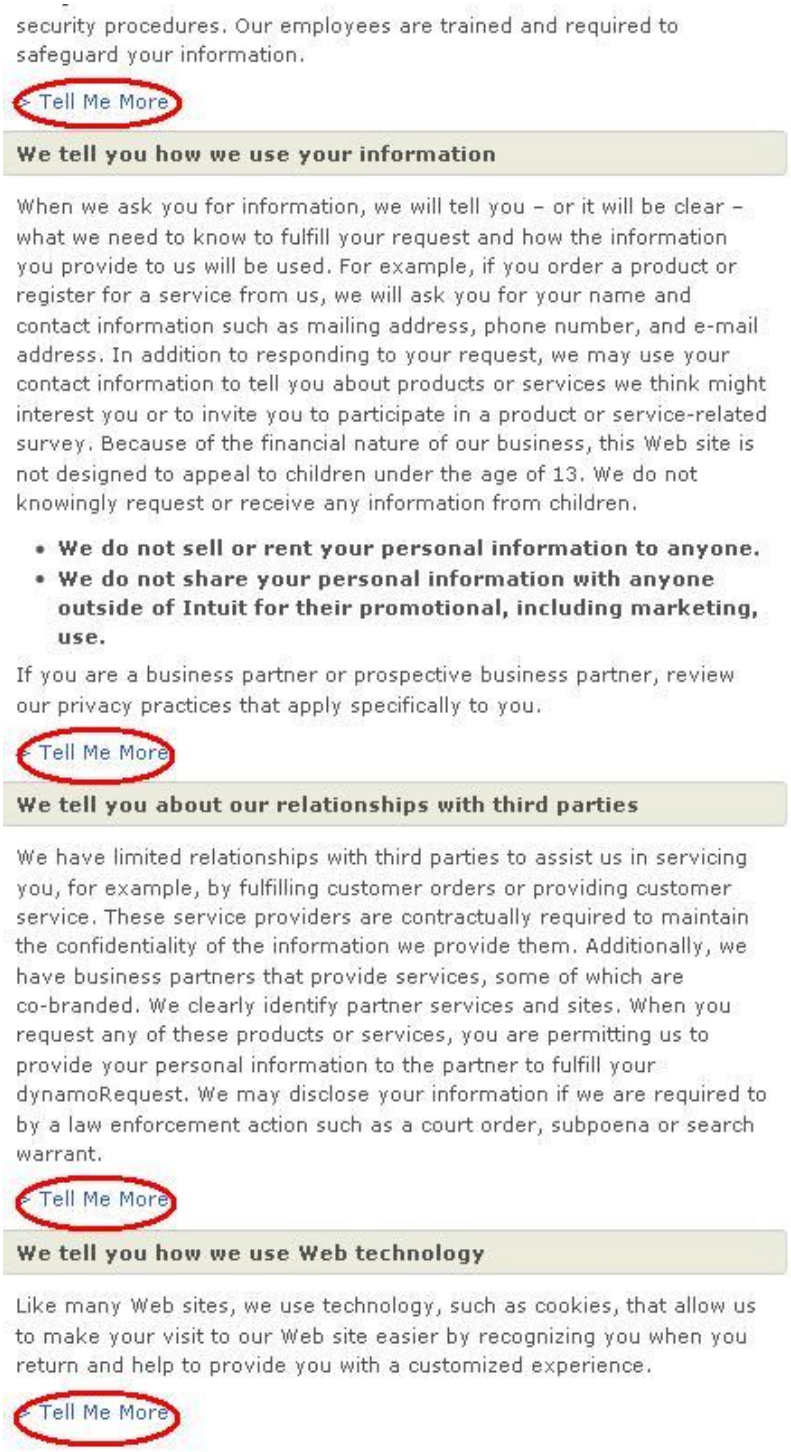
die den Nutzer, bei zusätzlichen Fragen, weiterleiten sollen, wodurch aber sehr leicht der Überblick verloren werden kann. Abbildung 19 zeigt ein Beispiel für die große Anzahl an Links anhand eines Screenshots der Datenschutzerklärung von Intuit.

Abbildung 17: Screenshot der Startseite von Dick's Sporting Goods



Quelle: [http://www.dickssportinggoods.com/home/index.jsp; Datum und Uhrzeit der Abfrage: 04. September 200]

Abbildung 18: Screenshot der Datenschutzerklärung von Intuit



security procedures. Our employees are trained and required to safeguard your information.

> Tell Me More

We tell you how we use your information

When we ask you for information, we will tell you – or it will be clear – what we need to know to fulfill your request and how the information you provide to us will be used. For example, if you order a product or register for a service from us, we will ask you for your name and contact information such as mailing address, phone number, and e-mail address. In addition to responding to your request, we may use your contact information to tell you about products or services we think might interest you or to invite you to participate in a product or service-related survey. Because of the financial nature of our business, this Web site is not designed to appeal to children under the age of 13. We do not knowingly request or receive any information from children.

- **We do not sell or rent your personal information to anyone.**
- **We do not share your personal information with anyone outside of Intuit for their promotional, including marketing, use.**

If you are a business partner or prospective business partner, review our privacy practices that apply specifically to you.

> Tell Me More

We tell you about our relationships with third parties

We have limited relationships with third parties to assist us in servicing you, for example, by fulfilling customer orders or providing customer service. These service providers are contractually required to maintain the confidentiality of the information we provide them. Additionally, we have business partners that provide services, some of which are co-branded. We clearly identify partner services and sites. When you request any of these products or services, you are permitting us to provide your personal information to the partner to fulfill your dynamoRequest. We may disclose your information if we are required to by a law enforcement action such as a court order, subpoena or search warrant.

> Tell Me More

We tell you how we use Web technology

Like many Web sites, we use technology, such as cookies, that allow us to make your visit to our Web site easier by recognizing you when you return and help to provide you with a customized experience.

> Tell Me More

Quelle: [http://www.intuit.com/privacy/; Datum und Uhrzeit der Abfrage: 04. September 2008 16:00]

Die nachfolgende Tabelle 19 zeigt einen grafischen Überblick der Unterschiede beim Vergleich der Compact Policy mit der Datenschutzerklärung. Die dazugehörige Legende gibt Auskunft über die eingefärbten Zellen.

Tabelle 19: Grafische Darstellung der Unterschiede von Compact Policy und Datenschutzerklärung der Stichprobe

Token	*Intuit*	*Microsoft*	*AT&T*	*Disney*	*Barnes & Noble*	*Aéropostale*	*Dick's Sporting Goods*	*Petsmart*
BUS				O		O	O	O
CNT		O	O					
COM					--			
DEM		--				O	O	O
DEV		--						
DSP					O			
HIS					O	O	O	O
LAW			O					
LEG					O			
NOI	X							
OTC						O		
OTP						O	O	O
OTR			O					
OUR					--			
PRE								--
PUR					--	--	--	--
STA	--	--			--	--	--	--
STP						O	O	O
TEL		O						

Legende:

X	Es wurde ein falscher Token in der Compact Policy verwendet. In der Datenschutzerklärung wird ein andere Sammlung, Zweck, etc. angegeben.
O	Der entsprechende Token scheint in der Compact Policy auf, fehlt aber in der Datenschutzerklärung
--	Der entsprechende Token fehlt in der Compact Policy, wird aber in der Datenschutzerklärung erwähnt.

Quelle: Eigene Darstellung

Bei der Analyse der Stichprobe fällt auf, dass sechs von acht Unternehmen in der Datenschutzerklärung angeben, dass sie Cookies und/oder Web Bugs einsetzen, der entsprechende Token aber in der Compact Policy fehlt. Als möglicher Grund dafür könnten die Standardeinstellungen einiger Browser (beispielsweise Internet Explorer) genannt werden, bei denen Cookies in diesem Fall automatisch blockiert und deshalb Seiten gar nicht oder fehlerhaft angezeigt werden. Die automatische Blockierung von Cookies ist bei vielen Browsern deshalb als Standard eingestellt, da viele Nutzer sich mit diesen Themen nicht beschäftigen wollen oder können. Darüber hinaus haben Cookies im Laufe der Zeit auch einen negativen Ruf erhalten und werden deshalb von vielen nicht akzeptiert (siehe zum Thema Cookies Kapitel 2.4.5). Um die Warnung des P3P Agenten zu umgehen, könnte es durchaus sein, dass die analysierten Unternehmen bewusst auf den Token STA verzichten, damit mehr Nutzer ihre Seite betrachten (können).

Bei der Hälfte der analysierten Organisationen fehlte darüber hinaus auch der Token PUR, welcher angibt, dass Daten gesammelt werden, welche aufgrund der Durchführung eines Online-Kaufs entstehen. Dies kann darauf zurückzuführen sein, dass beim Kauf sehr viele sensible Daten der Kunden (beispielsweise Name, Adresse, Kreditkartennummer, etc.) abgefragt werden müssen und ebendiese von den Nutzern, welche P3P oder APPEL einsetzen, im Vorhinein blockiert werden. Wenn diese Nutzer auf die Webseiten der Unternehmen kommen, würde ein Signal sie davor warnen, dass sensible Daten gesammelt werden, aber ohne den Zusatz dass dies nur beim Kauf von Produkten beziehungsweise Services geschieht. Daraus resultiert, dass die soeben beschriebenen Nutzer sofort die Webseite verlassen. Dies könnte ein Grund dafür sein, dass die untersuchten Unternehmen diesen Token in ihrer Compact Policy bewusst nicht angeben, damit mehr Nutzer auf ihre Seite kommen.

Intuit war das einzige der untersuchten Unternehmen, bei dem ein Token der Compact Policy nicht mit den Angaben der Datenschutzerklärung übereinstimmte. Bei Disney wurde nur eine Unstimmigkeit zwischen den beiden Policies entdeckt und zwar konnte keine Angabe zur Dauer der Speicherung in der Datenschutzerklärung gefunden werden.

Des Weiteren sind die abgefragte Compact Policy als auch die Unstimmigkeiten mit der Datenschutzerklärung bei den Unternehmen Aéropostale, Dick's Sporting Goods und Petsmart bis auf zwei kleinere Unterschiede identisch. Diese Ähnlichkeiten fallen besonders in der grafischen Darstellung in Tabelle 19 auf. Für Aéropostale und Dick's Sporting Goods kann dies darauf zurückzuführen sein, dass die Onlineshops beider Organisationen vom E-Commerce Unternehmen GSI Commerce betrieben werden. Ob Petsmart auch von GSI Commerce betreut wird, konnte leider nicht ermittelt werden, aber aufgrund der Ähnlichkeiten ist dies durchaus denkbar.

4.2. Analyse der Kundenseite

Um Einflussfaktoren auf das Kaufverhalten von Kunden im Internet zu ermitteln und eventuell vorhandene Ängste aufzuzeigen, wird in diesem Kapitel mithilfe eines Fragebogens eine empirische Untersuchung durchgeführt. Weiters soll in der Befragung der Einfluss und die Wahrnehmung von Datenschutzerklärungen und -zertifikaten auf die Kundenseite untersucht werden. Als Stichprobe wurden die Studenten und Studentinnen der Wirtschaftsuniversität Wien gewählt. Bevor die gewählte Stichprobe mittels Fragebogen untersucht werden konnte, wurden folgende Hypothesen aufgestellt:

1. Internetaffine Personen (damit sind Personen gemeint, die das Internet vorwiegend privat nutzen) kaufen regelmäßig in Internetshops ein und sind vorwiegend männlich. Alter und Berufstätigkeit spielen dabei keine Rolle, nur das Geschlecht.
2. Das Einkommen spielt bei der Angst vor Zahlungsmittelmissbrauch keine Rolle, sowohl Personen mit niedrigem als auch höherem Einkommen sind von der Angst gleichermaßen betroffen.
3. Personen die noch nie im Internet eingekauft haben, sind vor allem um die Sicherheit ihrer Daten besorgt. An zweiter Stelle ist die Angst vor dem Missbrauch des Zahlungsmittels.
4. Ein Großteil der Personen die bereits im Internet einkauften, werden die Datenschutzklausel des Internetshops nicht gelesen haben. Dabei spielt es auch eine Rolle, dass sie schwer auffindbar ist.

5. Eine gut geschriebene Datenschutzklausel hat keinen Einfluss auf das Kaufverhalten (sowohl bei regelmäßigem Einkauf im Internet, als auch bei Personen die noch nie eingekauft haben).
6. Es werden vorwiegend kostengünstige Artikel über das Internet gekauft, da dabei die Gefahr eines Fehlkaufs am Geringsten ist und die Gefahr dass man bezahlt aber kein Gut erhält nicht so kostenintensiv ist.
7. Ein besserer Preis als im regulären Geschäft beziehungsweise die Weiterempfehlung von Freunden/Bekannten sind das ausschlaggebende Argument um in einem Internetshop einzukaufen.
8. Selbst Personen die regelmäßig im Internet einkaufen haben Bedenken bezüglich der Sicherheit ihrer Daten.
9. Das am Meisten genutzte Zahlungsmittel ist die Vorkasse.
10. Beim Großteil der Personen die im Internet bereits eingekauft hatten, wurde nicht speziell auf die Datenschutzklausel des Shopbetreibers hingewiesen.
11. Datenschutzzertifikate haben mehr Einfluss auf Personen. die noch nie im Internet eingekauft haben, als bei regelmäßigen Einkäufern, da der Shop entweder empfohlen wurde oder der Preis das ausschlaggebende Argument für den Kauf war.
12. Faktoren wie bekannte Marke/Hersteller und Weiterempfehlung haben den größten Einfluss auf das Kaufverhalten sowohl von Nichtkäufern als auch auf Käufer.

Nachdem die Hypothesen für die Untersuchung formuliert wurden, war der nächste Schritt die Erstellung des Fragebogens. Der gesamte Fragebogen ist im Anhang am Ende der Arbeit zu finden. Nachdem der Fragebogen fertiggestellt war, wurden die Hypothesen in folgende Konstrukte in Tabelle 20 kategorisiert, um die Auswertung und Interpretation der Hypothesen zu erleichtern:

Tabelle 20: Kategorisierung der Hypothesen in Konstrukte

Konstrukt-nummer	Name des Konstrukts	
1	Allgemeine Personendaten	Fragen: 1, 2
2	Verfügbares Einkommen und Berufstätigkeit	Fragen: 3, 4
3	Internetnutzung allgemein	Fragen: 5, 6
4	Internetnutzung verknüpft mit persönlichen Daten (Hypothese 1)	Konstrukte: 1, 2, 3
5	Angst vor Missbrauch von Zahlungsmitteln	Fragen: 8, 14, 15
6	Angst vor Zahlungsmittelmissbrauch verknüpft mit Einkommen und Berufstätigkeit (Hypothese 2)	Konstrukte: 2, 6
7	Vertrauen in die Sicherheit von Online-Käufen	Fragen: 8, 13
8	Angst vor Missbrauch von persönlichen Daten	Fragen: 12, 13
9	Häufigkeit der Online-Käufe	Fragen: 7, 9
10	Kaufverhalten und Ängste (Hypothese 3)	Konstrukte: 5, 7, 8, 9
11	Erfahrungen beim Online-Kauf	Fragen: 16, 17
12	Wahrnehmung der Datenschutzklausel	Fragen: 18, 19, 20, 21, 22, 23
13	Kaufverhalten verknüpft mit der Wahrnehmung der Datenschutzklausel (Hypothese 4)	Konstrukte: 9, 12
14	Einflüsse auf das Kaufverhalten	Fragen: 24, 25
15	Einfluss von Datenschutzklauseln auf das Kaufverhalten (Hypothese 5)	Konstrukte: 9, 12
16	Preissegment des Online-Kaufs	Frage: 10
17	Gründe für den Online-Kauf und Gründe für Nicht-Kauf	Fragen: 8, 11
18	Wahl der Güter verknüpft mit Gründen für den Einkauf (Hypothese 6)	Konstrukte: 16, 17
19	Analyse der Gründe für Online-Käufe (Hypothese 7)	Konstrukt: 17
20	Regelmäßige Online-KäuferInnen und ihre Ängste (Hypothese 8)	Konstrukte: 5, 8, 9
21	Analyse der gewählten Zahlungsmittel verknüpft	Fragen: 14, 15

	mit den Gründen der Wahl (Hypothese 9)	
22	Überprüfung ob Internetkäufer speziell auf Datenschutzklauseln hingewiesen werden (Hypothese 10)	Fragen: 7, 9, 21
23	Analyse des Einflusses von Datenschutzzertifikaten auf Online-KäuferInnen oder Nicht-KäuferInnen (Hypothese 11)	Fragen: 7, 11, 24, 25
24	Allgemeine Einflüsse auf Online-KäuferInnen und Nicht-KäuferInnen (Hypothese 12)	Fragen: 7, 8, 11, 24, 25

Quelle: Eigene Darstellung

Die entstandenen Konstrukte wurden danach durch Mapping auf die Hypothesen übertragen. Die nachfolgende Tabelle 21 zeigt in der rechten Spalte die Konstrukte, mit der die jeweilige Hypothese (linke Spalte) gemessen wird.

Tabelle 21: Mapping der Konstrukte auf die Hypothesen

Hypothese	Konstrukte
1	1, 2, 3, 4
2	2, 5, 6
3	5, 8, 9, 10
4	9, 12, 13
5	9, 12, 14, 15
6	16, 17, 18
7	17, 19
8	5, 8, 9, 20
9	21
10	22
11	23
12	24

Quelle: Eigene Darstellung

Nach dem Mapping der Konstrukte auf die Hypothesen wurde ein Online-Fragebogen mittels der Applikation Limesurvey[35] erstellt. Als nächster Schritt folgte eine Anfrage an das Vizerektorat für Lehre, um eine Bewilligung zur Versendung einer E-Mailumfrage an alle WU-StudentInnen zu erhalten. Nachdem die Umfrage bewilligt wurde, versendete das Zentrum für Informatikdienste der WU den Link zum Fragebogen gemeinsam mit einem kurzen Informationstext an alle E-Mailadressen der WU-StudentInnen. Insgesamt wurden 1450 Fragebögen ausgefüllt, wovon 1.333 komplett und 117 unvollständig waren.

In den nachfolgenden Kapiteln werden die gesammelten Daten aus der Befragung analysiert und die Hypothesen anhand der Ergebnisse überprüft. Für jede Hypothese wurde ein Kurztitel für das jeweilige Kapitel gewählt.

4.2.1. Internetaffine Personen

Hypothese 1: Internetaffine Personen (damit sind Personen gemeint, die das Internet vorwiegend privat nutzen) kaufen regelmäßig in Internetshops ein und sind vorwiegend männlich. Alter und Berufstätigkeit spielen dabei keine Rolle, nur das Geschlecht.

Wie in Tabelle 23 zu sehen ist, gaben von den 1.333 befragten Personen, 776 an, dass sie gemäß ihrer Einschätzung das Internet am Meisten für private Zwecke nutzen. Von diesen 776 Befragten, haben 100% bereits Online-Einkäufe getätigt. Daraus ergibt sich, dass von den Online-Einkäufern, die vorwiegend das Internet für private Zwecke nutzen, 52% männlich und 48% weiblich sind (siehe Tabelle 25). Nach der Durchführung eines Chi-Quadrat Tests[36] kommt man zu folgenden Ergebnissen:

[35] Die Webseite der Applikation lautet: http://www.limesurvey.org

[36] Für nähere Informationen zur Berechnung des Chi-Quadrat-Wertes siehe beispielsweise http://de.wikipedia.org/wiki/Chi-Quadrat-Test Datum und Uhrzeit der Abfrage: 05. November 2008

Tabelle 22: Chi-Quadrat-Werte der Hypothese 1

Vorwiegend private Nutzung des Internets	Testgröße	Freiheitsgrade	Signifikanz
Chi² Männer	4,5	1	95%
Chi² Frauen	3,9	1	95%
Chi² Männer und Frauen	8,4	1	97,5%

Quelle: Eigene Darstellung

Aus den Signifikanzwerten in Tabelle 22 kann geschlossen werden, dass mit einer Wahrscheinlichkeit von 97,5% Hypothese 1 in diesem Punkt zutrifft und das Geschlecht Einfluss auf das Online-Kaufverhalten hat.

In den nachfolgenden Tabellen 23, 24 und 25 werden jeweils die absoluten Zahlen in der linken Spalte und die entsprechenden Prozentwerte in der rechten Spalte dargestellt.

Tabelle 23: Anzahl der Befragten Online-Käufer die das Internet für private Zwecke nutzen

Anzahl Online-Käufer bei privater Nutzung (in %)
776 (100%)
Anzahl Nicht-Käufer bei privater Nutzung (in %)
0 (0%)
Summe (in %)
776 (100%)

Quelle: Eigene Darstellung

Tabelle 24: Geschlechterverteilung der gesamten Stichprobe

Anzahl männliche Befragte (in %)
621 (46,62%)
Anzahl weibliche Befragte (in %)
711 (53,38%)
Summe (in %)
1332 (100%)

Quelle: Eigene Darstellung

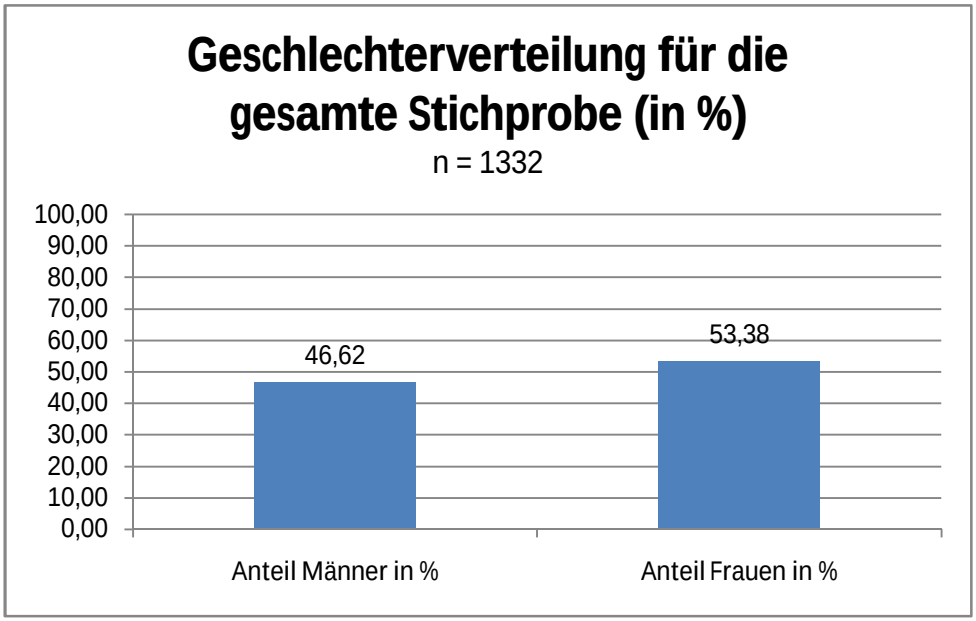
Tabelle 25: Geschlechterverteilung bei privater Nutzung des Internets

Anzahl männliche Online-Käufer bei privater Nutzung (in %)
402 (51,80%)
Anzahl weibliche Online-Käufer bei privater Nutzung (in %)
374 (48,20%)
Summe (in %)
776 (100%)

Quelle: Eigene Darstellung

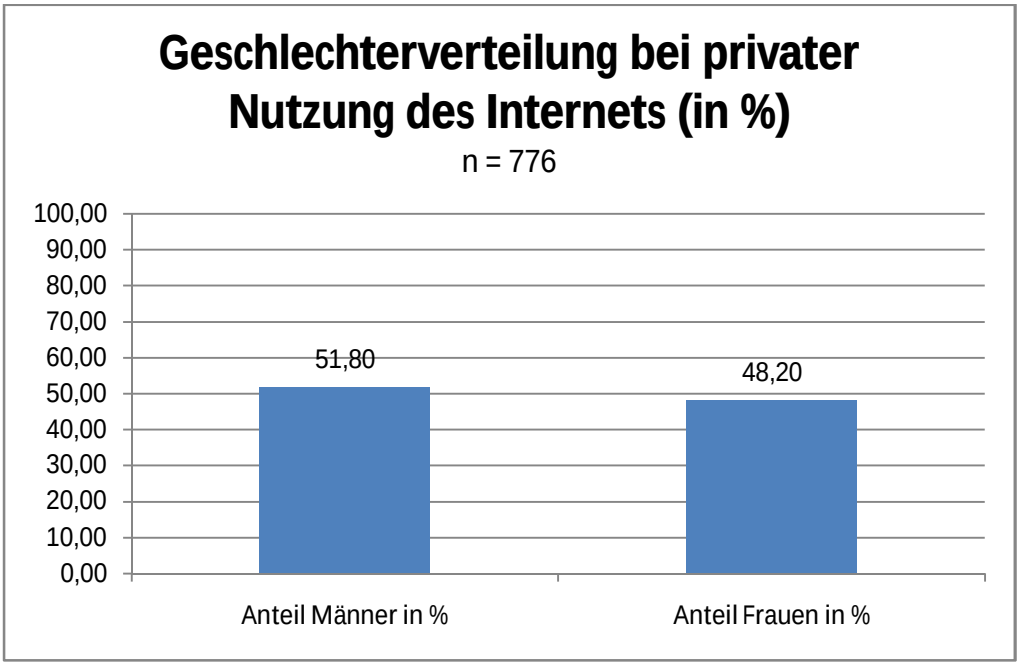
Die nachfolgenden Abbildungen 20 und 21 zeigen eine grafische Darstellung der Geschlechterverteilung bei der gesamten Stichprobe und bei privater Nutzung des Internets.

Abbildung 19: Geschlechterverteilung in % gesamte Stichprobe



Quelle: Eigene Darstellung

Abbildung 20: Geschlechterverteilung in % bei privater Nutzung des Internets



Quelle: Eigene Darstellung

Aufgrund der Homogenität der ausgewählten Stichprobe in Bezug auf Alter und Berufstätigkeit werden die Ergebnisse aus der Umfrage nicht in die Annahme beziehungsweise Ablehnung der Hypothese einfließen. Die nachfolgenden Tabellen 26 und 27 zeigen die Ergebnisse der Untersuchung.

Tabelle 26: Prozentuelle Werte für die gesamte Stichprobe anhand der Merkmale Berufstätigkeit und Käufer

Berufstätige gesamte Stichprobe (in %)	Nicht-Berufstätige gesamte Stichprobe (in %)
803 (60,29%)	529 (39,71%)
Berufstätige Online-Käufer (in %)	Nicht-Berufstätige Online-Käufer (in %)
735 (61,76%)	455 (38,24%)

Quelle: Eigene Darstellung

Tabelle 27: Altersklassen der gesamten Stichprobe und der Online-Käufer

Altersklassen	Alter Internetkäufer (in %)	Alter gesamte Stichprobe (in %)
< 20 Jahre	49 (4,12%)	182 (13,67%)
21-25 Jahre	603 (50,71%)	685 (51,47%)
26-30 Jahre	363 (30,53%)	314 (23,59%)
31-35 Jahre	103 (8,66%)	83 (6,24%)
36-40 Jahre	52 (4,37%)	47 (3,53%)
41-45 Jahre	10 (0,84%)	10 (0,75%)
46-50 Jahre	7 (0,59%)	7 (0,53%)
> 50 Jahre	2 (0,17%)	3 (0,23%)
Summe	1189 (100%)	1331 (100%)

Quelle: Eigene Darstellung

Hypothese 1 konnte bei der Befragung bestätigt werden, da das Geschlecht einen Einfluss auf die Bereitschaft zur Tätigung von Internetkäufen hat. Bei der Analyse der Daten viel des Weiteren auf, dass alle (100%) internetaffinen Personen, bereits im Internet Käufe getätigt haben.

4.2.2. Angst vor Zahlungsmittelmissbrauch

Hypothese 2: Das Einkommen spielt bei der Angst vor Zahlungsmittelmissbrauch keine Rolle, sowohl Personen mit niedrigem als auch höherem Einkommen sind von der Angst gleichermaßen betroffen.

Tabelle 28 zeigt, dass prozentuell bei den Einkommensgruppen: weniger als 100€, 750-900€ und mehr als 900€, sichtbare Unterschiede festzustellen sind, zwischen denen die Angst vor Zahlungsmittelmissbrauch haben und der gesamten Stichprobe. Bei den letzteren zwei Einkommensklassen ist die absolute Anzahl der Befragten, die Angst haben, sehr gering (1; 3) und bei den Einkommensklassen 100-300€; 350-500€ und 550-700€ sind prozentuell keine größeren Unterschiede zwischen den Befragten die Angst haben und der gesamten Stichprobe festzustellen. Auffällig war nur die Einkommensgruppe der mehr als 900€-Verdiener, da diese die geringste Angst (~5%) hat.

Tabelle 28: Prozentueller Vergleich der Befragten die Angst vor Zahlungsmittelmissbrauch haben mit der gesamten Stichprobe

Einkommen	Befragte die Angst vor Zahlungs-mittelmissbrauch haben (in %)	Anzahl gesamte Stichprobe (in %)
weniger als 100€	11 (16,67%)	80 (6,02%)
100-300€	23 (34,85%)	407 (30,62%)
350-500€	18 (27,27%)	368 (27,69%)
550-700€	10 (15,15%)	173 (13,02%)
750-900€	1 (1,52%)	98 (7,37%)
mehr als 900€	3 (4,55%)	203 (15,27%)
Summe	66 (100%)	1329 (100%)

Quelle: Eigene Darstellung

In der nachfolgenden Tabelle 29 können die berechneten Chi-Quadrat-Werte für die einzelnen Preissegmente entnommen werden. Die letzte Zeile zeigt, dass die Signifikanz aller Preissegmente 99,50% ist, somit muss Hypothese 2 verworfen werden. Das Einkommen hat keinen Einfluss auf die Angst vor Zahlungsmittelmissbrauch.

Tabelle 29: Chi-Quadrat-Werte der Hypothese 2

Angst vor Zahlungsmittelmissbrauch	Testgröße	Freiheitsgrade	Signifikanz
weniger als 100€	12,43	1	99,99%
100-300€	0,38	1	<90%
350-500€	0,00	1	<90%
550-700€	0,23	1	<90%
750-900€	3,07	1	90%
mehr als 900€	4,97	1	95%
Alle Preissegmente	21,10	6	99,5%

Quelle: Eigene Darstellung

4.2.3. Ängste der Nicht-Käufer im Internet

Hypothese 3: Personen die noch nie im Internet eingekauft haben, sind vor allem um die Sicherheit ihrer Daten besorgt. An zweiter Stelle ist die Angst vor dem Missbrauch des Zahlungsmittels.

Insgesamt haben 142 der Befragten noch nie über das Internet eingekauft. Wie man in Tabelle 30 sehen kann, ist an erster Stelle für die Gründe warum noch nie eingekauft wurde, mit ~21% die Bevorzugung des „traditionellen“ Einkaufs, bei dem die Waren selbst Vorort begutachtet werden können, angegeben. An zweiter Stelle mit

~14% wurde als Grund für den Nicht-Kauf über das Internet, Bedenken bezüglich der Sicherheit der Daten genannt und an dritter Stelle mit ~12% die Unsicherheit der Zahlungsmethoden. Hypothese 3 hat sich bestätigt, mit der Ergänzung dass an erster Stelle die Präferenz zum traditionellen Einkauf als Gegenargument zum Kauf im Internet steht.

Tabelle 30: Gründe warum die Befragten noch nie über das Internet eingekauft haben

Warum hast Du noch nie etwas über das Internet etwas gekauft beziehungsweise ersteigert?	Anzahl (in %)
Ich kaufe lieber auf die traditionelle Art ein, das heißt ich sehe mir lieber die Ware selbst an	115 (20,57%)
Ich habe Bedenken aufgrund der Sicherheit meiner Daten	77 (13,77%)
Die Zahlungsmethoden sind mir zu unsicher	66 (11,81%)
Ich hätte Bedenken aufgrund der Eigenschaften der Ware (zum Beispiel Qualität, Funktionalität, Größe bei Kleidung, etc.)	63 (11,27%)
Hat sich noch nicht ergeben, bin aber durchaus daran interessiert	46 (8,23%)
Ich habe kein Vertrauen in Internetshops	43 (7,69%)
Ich hätte Angst, dass mir wesentliche Faktoren (zum Beispiel Umtauschmöglichkeiten, Lieferzeit) unklar sind	35 (6,26%)
Ich befürchte, dass meine Daten an Dritte weitergegeben werden	34 (6,08%)
Ich lasse mich lieber von einem/r VerkäuferIn persönlich beraten	29 (5,19%)
Ich habe kein Vertrauen in elektronische Auktionshäuser	27 (4,83%)
Ich wollte schon öfters online einkaufen, habe aber dann den Kaufprozess vorzeitig abgebrochen, weil mir etwas unklar war	14 (2,50%)
Other	10 (1,79%)
Summe	559 (100%)

Quelle: Eigene Darstellung

4.2.4. Wahrnehmung der Datenschutzklausel

Hypothese 4: Ein Großteil der Personen, die bereits im Internet einkauften, werden die Datenschutzklausel des Internetshops nicht gelesen haben. Dabei spielt es auch eine Rolle, dass diese schwer auffindbar ist.

Die Befragung ergab, dass lediglich 35% der Befragten sich die Datenschutzklausel beim Online-Kauf durchlesen (siehe Tabelle 31). In diesem Punkt konnte Hypothese 4 bestätigt werden.

Tabelle 31: Befragte die nicht die Datenschutzklausel gelesen haben

	Anzahl Befragte die nicht die Datenschutzklausel gelesen haben
Absolute Zahl	768
In %	64,65%
	Anzahl Befragte die PP durchgelesen haben
Absolute Zahl	420
In %	35,35%

Quelle: Eigene Darstellung

Wie in Tabelle 32 zu sehen ist, gaben 10% der Befragten an, welche die Datenschutzklausel nicht gelesen haben, dass sie diese nicht gefunden und deshalb nicht gelesen haben. Hypothese 4 konnte in diesem Punkt nicht bestätigt werden. Ein interessanter Punkt hierbei ist, dass 80% der Befragten angaben, sie hätten die Datenschutzklausel nicht verstanden und dass sie daher nicht genau wussten was mit ihren Daten geschieht. Dieses Ergebnis deckt sich mit Kapitel 2 in dem bereits auf die schwere Verständlichkeit von Datenschutzklauseln hingewiesen wurde.

Tabelle 32: Befragte die nicht die Datenschutzklausel gelesen haben, weil sie nicht gefunden wurde

	Befragte die nicht die Datenschutzklausel gelesen haben, weil diese nicht gefunden wurde
Absolute Zahl	79
In %	10,29%
	Datenschutzklausel wurde nicht verstanden
Absolute Zahl	337
In %	80,24%

Quelle: Eigene Darstellung

4.2.5. Einfluss von Datenschutzklauseln

Hypothese 5: Eine gut geschriebene Datenschutzklausel hat keinen Einfluss auf das Kaufverhalten (sowohl bei regelmäßigem Einkauf im Internet, als auch bei Personen die noch nie eingekauft haben).

Rund 26% der Befragten, die noch nie im Internet eingekauft haben, stimmen 100%ig damit überein, dass eine verständliche Datenschutzerklärung Einfluss auf ihr

Kaufverhalten hat. Des Weiteren stimmten 40% großteils damit überein und 24% weniger. Lediglich 9% stimmen gar nicht damit überein (siehe Tabelle 33).

Tabelle 33: Bewertung einer verständlichen Datenschutzerklärung durch die Befragten (in %)

Wie oft eingekauft?	stimme gar nicht überein % (absolute Zahl)	stimme weniger überein % (absolute Zahl)	stimme großteils überein % (absolute Zahl)	stimme 100%ig überein % (absolute Zahl)	Summe (absolute Zahl)
mind. 1mal in 3 Monaten	9,76% (41)	39,52% (166)	39,29% (165)	11,43% (48)	100% (420)
mind. 1mal pro Monat	15,92% (32)	35,32% (71)	34,83% (70)	13,93% (28)	100% (201)
weniger als alle 3 Monate	10,09% (58)	30,26% (174)	43,13% (248)	16,52% (95)	100% (575)
nie	8,76% (12)	24,09% (33)	40,88% (56)	26,28% (36)	100% (137)

Quelle: Eigene Darstellung

Personen, die weniger als alle drei Monate einkaufen, zeigen ähnliche prozentuelle Wert auf. 17% stimmten 100%ig, rund 43% der Befragten stimmten großteils, 30% weniger und 10% gar nicht überein. Bei den Befragten, die mindestens einmal pro Monat und mindestens einmal in drei Monaten einkaufen, sind die prozentuellen Werte auch ähnlich.

Zur einfacheren Berechnung des Chi-Quadrat-Wertes wurden die Ergebnisse zusammengefasst. Unter der Gruppe „Regelmäßige Käufer“ wurden Personen subsummiert die mindestens einmal in drei Monaten und mindestens einmal pro Monat einkaufen. Personen die weniger als alle drei Monate einkaufen werden als „unregelmäßige Käufer“ bezeichnet. Des Weiteren wurden die Werte für „stimme großteils überein“ und „stimme 100%ig überein“ für die Berechnung zusammengefasst. In der nachfolgenden Tabelle 34 können die jeweiligen Werte entnommen werden.

Tabelle 34: Chi-Quadrat-Werte der Hypothese 5

Datenschutzklausel hat einen Einfluss	Testgröße	Freiheitsgrade	Signifikanz
Regelmäßige Käufer	3,84	1	95%
Unregelmäßige Käufer	1,4	1	<90%
Keine Käufer	3,06	1	90%
Regelmäßigkeit des Einkaufes	8,3	3	95%

Quelle: Eigene Darstellung

Hypothese 5 kann mit einer Wahrscheinlichkeit von 95% abgelehnt werden, da eine gut geschriebene Datenschutzklausel einen Einfluss auf die Befragten hat, unabhängig von der Regelmäßigkeit ihrer Online-Käufe.

4.2.6. Preissegmente des Online-Kaufs

Hypothese 6: Es werden vorwiegend kostengünstige Artikel über das Internet gekauft, da dabei die Gefahr eines Fehlkaufs am Geringsten ist und die Gefahr dass man bezahlt aber kein Gut erhält nicht so kostenintensiv ist.

Gemäß Selbsteinschätzung kauften knapp 50% der Befragten Artikel im niedrigen (<50 Euro) und rund 35% im mittleren Preissegment (55-150 Euro) ein. Lediglich 9% der Befragten kauften im höheren (155-300 Euro) und 6% im hohen Preissegment (>300 Euro) (siehe Tabelle 35). Damit konnte Hypothese 6 bestätigt werden, die Befragten kaufen vorwiegend im niedrigen und mittleren Preissegment bis 150 Euro ein. Einkäufe mit einem Warenwert von mehr als 150 Euro werden anscheinend weiterhin primär auf dem traditionellen Weg erledigt.

Tabelle 35: Einordnung des letzten Online-Kaufs in Preissegmente

Einschätzung der Befragten	Absolut Zahlen (in %)
niedriges Preissegment (< 50 Euro)	592 (49,79%)
Mittleres (55-150 Euro)	419 (35,24%)
Höheres (155-300 Euro)	104 (8,75%)
Hohes (> 300 Euro)	74 (6,22%)
Summe	1189 (100%)

Quelle: Eigene Darstellung

4.2.7. Argumente für den Online-Kauf

Hypothese 7: Ein besserer Preis als im regulären Geschäft beziehungsweise die Weiterempfehlung von Freunden/Bekannten sind das ausschlaggebende Argument, um in einem Internetshop einzukaufen.

Ausschlaggebendes Argument für die Entscheidung zum Onlinekauf war bei den Befragten mit 100%iger Übereinstimmung:

- die Bekanntheit der Marke beziehungsweise des Herstellers
- an zweiter Stelle die Bekanntheit des Shops und

- eine schnelle Lieferung an dritter Stelle.

Bei großteils Übereinstimmung ist auf dem

- ersten Platz als ausschlaggebendes Argument die Empfehlung des Shops
- gefolgt von einer schnellen Lieferung
- und am dritter Platz eine seriöse Homepage.

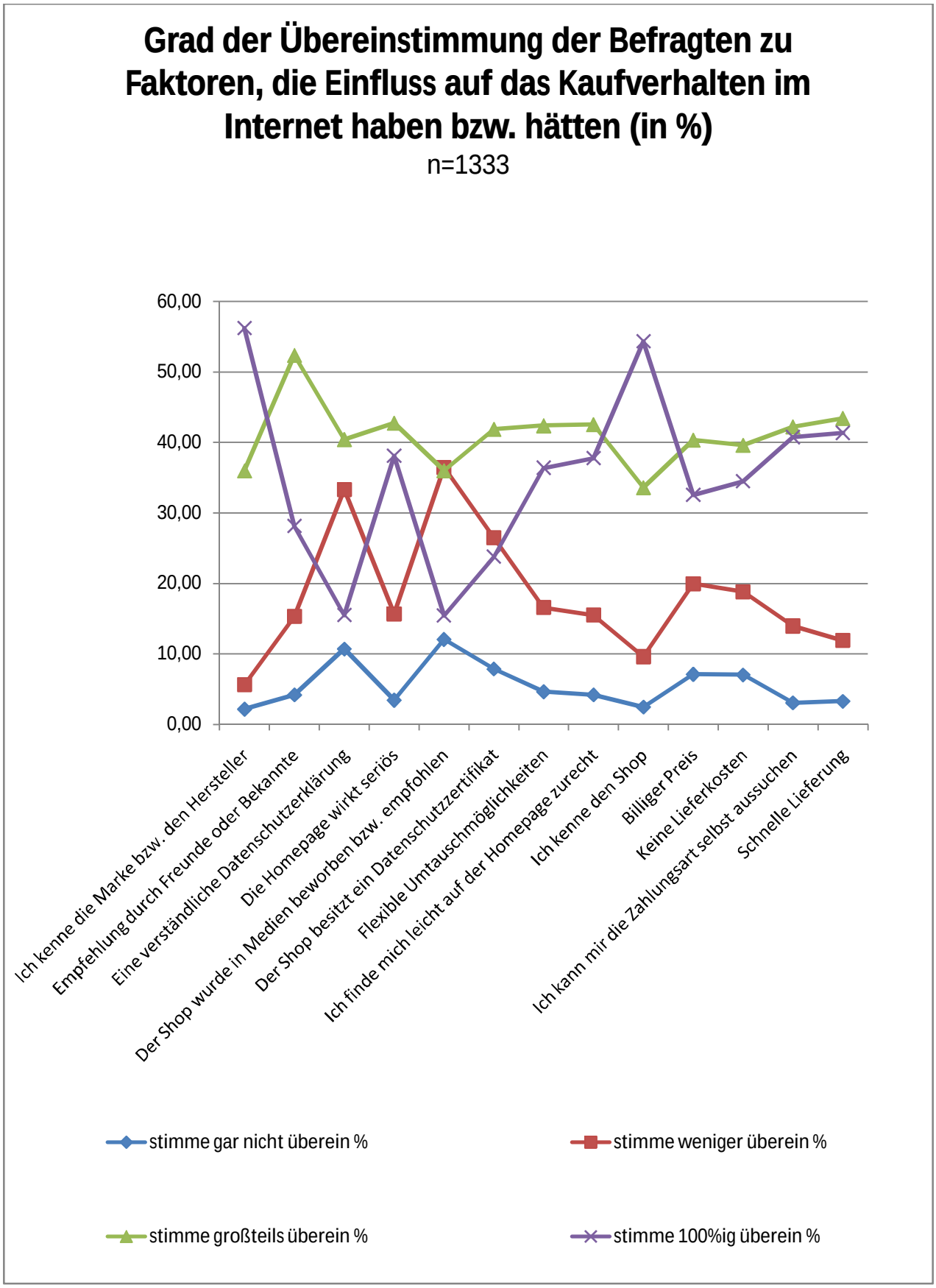
In der nachfoglenden Tabelle 36 wurden diese Daten übersichtlich zusammengefasst. Der Grad der Übereinstimmung zu den Faktoren, die Einfluss auf das Kaufverhalten haben beziehungsweise hätten wird in Abbildung 22 grafisch dargestellt.

Tabelle 36: Übereinstimmung der Befragten zu Faktoren die das Einkaufsverhalten beeinflussen (in %)

	stimme gar nicht überein	stimme weniger überein	stimme großteils überein	stimme 100%ig überein
Ich kenne die Marke beziehungsweise den Hersteller	2,18%	5,63%	36,01%	56,19%
Empfehlung durch Freunde oder Bekannte	4,20%	15,30%	52,36%	28,13%
Eine verständliche Datenschutzerklärung	10,73%	33,31%	40,44%	15,53%
Die Homepage wirkt seriös	3,45%	15,68%	42,76%	38,11%
Der Shop wurde in Medien beworben beziehungsweise empfohlen	12,08%	36,46%	36,01%	15,45%
Der Shop besitzt ein Datenschutzzertifikat	7,88%	26,48%	41,86%	23,78%
Flexible Umtauschmöglichkeiten	4,65%	16,58%	42,39%	36,38%
Ich finde mich leicht auf der Homepage zurecht	4,20%	15,53%	42,54%	37,73%
Ich kenne den Shop	2,48%	9,60%	33,61%	54,31%
Billiger Preis	7,13%	19,95%	40,36%	32,56%
Keine Lieferkosten	7,05%	18,83%	39,61%	34,51%
Ich kann mir die Zahlungsart selbst aussuchen	3,08%	13,95%	42,24%	40,74%
Schnelle Lieferung	3,30%	11,93%	43,44%	41,34%

Quellle: Eigene Darstellung

Abbildung 21: Grad der Übereinstimmung zu Faktoren, die Einfluss auf das Online-Kaufverhalten haben beziehungsweise hätten



Quelle: Eigene Darstellung

Tabelle 37: Chi-Quadrat-Werte der Hypothese 7

Einfluss auf das Kaufverhalten	Testgröße	Freiheitsgrade	Signifikanz
Ich kenne die Marke beziehungsweise den Hersteller	45,84	1	99,99%
Empfehlung durch Freunde oder Bekannte	3,5	1	90%
Eine verständliche Datenschutzerklärung	70,59	1	99,99%
Die Homepage wirkt seriös	4,11	1	95%
Der Shop wurde in Medien beworben beziehungsweise empfohlen	105,81	1	99,99%
Der Shop besitzt ein Datenschutzzertifikat	18,92	1	99,99%
Flexible Umtauschmöglichkeiten	1,32	1	<90%
Ich finde mich leicht auf der Homepage zurecht	3,15	1	90%
Ich kenne den Shop	24,8	1	99,99%
Billiger Preis	1,7	1	<90%
Keine Lieferkosten	0,64	1	<90%
Ich kann mir die Zahlungsart selbst aussuchen	8,45	1	97,5%
Schnelle Lieferung	13,4	1	99,99%

Quelle: Eigene Darstellung

Mit einer Signifikanz von 99,99% (siehe Tabelle 37) wurden folgende Einflussfaktoren bei der Befragung festgestellt:

- Ich kenne die Marke beziehungsweise den Hersteller
- Eine verständliche Datenschutzerklärung
- Der Shop wurde in Medien beworben beziehungsweise empfohlen
- Der Shop besitzt ein Datenschutzzertifikat
- Ich kenne den Shop
- Schnelle Lieferung

Hypothese 7 konnte nicht bestätigt werden, da die Einflussfaktoren mit einer Signifikanz von 99,99% nicht mit denen der Hypothese übereinstimmen.

4.2.8. Bedenken der Befragten beim Online-Kauf

Hypothese 8: Selbst Personen die regelmäßig im Internet einkaufen haben Bedenken bezüglich der Sicherheit ihrer Daten.

Wie in Tabelle 38 zu sehen ist, ergab die Berechnung des Mittelwerts bei den regelmäßigen Einkäufern[37], dass die größte Angst der Befragten die Übermittlung der Daten ist, an zweiter Stelle steht die Angst vor Spammails. Im ersten Punkten gibt es eine Übereinstimmung mit den Ängsten der Käufer die weniger als alle drei Monate einkaufen. An zweiter Stelle steht, bei den unregelmäßigen Käufern, die Angst davor, dass ihre Daten abgefangen werden könnten. Bei den regelmäßigen Einkäufern ist an dritter Stelle die Angst vor Werbezusendung an die Postadresse und bei unregelmäßigen Käufern ist an dieser Stelle die allgemeine Angst beim Online-Kauf.

[37] Unter regelmäßigen Käufern werden die Befragten aus den Häufigkeitsklassen mindestens einmal in drei Monaten und mindestens einmal pro Monat subsummiert. Als unregelmäßige Käufer werden die Befragten welche weniger als alle drei Monate im Internet einkaufen bezeichnet.

Tabelle 38: Gründe für Bedenken der Befragten beim Online-Kauf (in %)

Häufigkeit des Online-Kaufs	Ich wusste nicht was der Shopbetreiber mit meinen Daten macht (zum Beispiel Nicht autorisierte Weitergabe oder Verkauf der Daten an Dritte, etc.	Habe ich immer, wenn ich Daten über das Internet übermitteln muss	Ich habe Angst davor, dass jemand meine Daten abfängt (Hacker)	Ich befürchte, dass ich Spammails erhalte	Ich befürchte, dass ich nicht erwünschte Werbung an meine Postadresse erhalte	Habe ich immer beim ersten Einkauf bei einem neuen Shop	Habe ich generell immer wenn ich online einkaufe	Ich befürchte, dass ich unaufgefordert Newsletter erhalte	Other
mind. einmal in 3 Monaten	35,71	65,48	44,05	46,43	33,33	21,43	46,43	21,43	8,33
mind. einmal pro Monat	42,31	69,23	42,31	69,23	61,54	19,23	42,31	38,46	7,69
weniger als alle 3 Monate	30,81	75,14	52,97	37,30	32,43	12,43	42,16	20,54	1,08
Mittelwert regelmäßige Käufer	39,01	67,35	43,18	57,83	47,44	20,33	44,37	29,95	8,01
Rang regelmäßige Käufer	6	1	5	2	3	8	4	7	9
Rang unregelmäßige Käufer	6	1	2	4	5	8	3	7	9

Quelle: Eigene Darstellung

Nachfolgend werden die Ängste der Befragten beim Online-Kauf nochmals übersichtlich nach Plätzen zusammengefasst:

Im Durchschnitt:

- Erster Platz: Angst habe ich immer, wenn ich Daten über das Internet übermitteln muss
- Zweiter Platz: Ich befürchte, dass ich Spammails erhalte
- Dritter Platz: Ich habe Angst davor, dass jemand meine Daten abfängt (Hacker)

Bei regelmäßigen Käufern:

- Erster Platz: Angst habe ich immer, wenn ich Daten über das Internet übermitteln muss
- Zweiter Platz: Ich befürchte, dass ich Spammails erhalte
- Dritter Platz: Ich befürchte, dass ich nicht erwünschte Werbung an meine Postadresse erhalte

Bei unregelmäßigen Käufern:

- Erster Platz: Angst habe ich immer, wenn ich Daten über das Internet übermitteln muss
- Zweiter Platz: Ich habe Angst davor, dass jemand meine Daten abfängt (Hacker)
- Dritter Platz: Habe ich generell immer wenn ich online einkaufe

Hypothese 8 konnte bestätigt werden, da die Befragung ergeben hat, dass selbst regelmäßige Online-Käufer am Meisten Angst vor der Übermittlung ihrer Daten und deren Sicherheit haben.

4.2.9. Wahl der Zahlungsmittel

Hypothese 9: Das am Meisten genutzte Zahlungsmittel ist die Vorkasse.

Die Befragten gaben an, dass der Shopbetreiber beim Online-Kauf am Meisten die Kreditkarte, an 2. Stelle die Vorkasse und auf dem 3. Platz einen Zahlschein als Zahlungsmittel verlangte. Hypothese 9 konnte bei der Befragung nicht bestätigt werden, da die Kreditkarte eindeutig am Meisten verlangt wurde (siehe Tabelle 39; 45% die Kreditkarte im Vergleich zur Vorkasse mit 20%).

Tabelle 39: Auswahlgründe für Zahlungsmittelarten (in %)

Zahlungs-mittelart	Anzahl Befragte	Wurde vom Shopbetreiber vorgegeben	Aufgrund der Sicherheit der Zahlungsart	War für mich persönlich am Bequemsten	War die einzige Möglichkeit für mich	Einfach so	Other
Nachnahme	11,53	10,24	17,82	9,84	16,03	12,00	13,89
Zahlschein	15,83	11,81	24,75	12,84	12,98	16,00	5,56
Vorkasse	13,56	20,28	10,15	11,61	17,56	8,00	16,67
Kreditkarte	45,06	45,28	31,68	49,86	39,69	56,00	36,11
Paypal	6,63	8,07	10,64	7,51	4,96	4,00	0,00
Paysafe	0,23	0,39	0,25	0,27	0,00	0,00	0,00
Moneybookers	0,08	0,20	0,25	0,14	0,00	0,00	0,00
Online-Überweisung	0,00	0,00	0,00	0,00	0,00	0,00	0,00
Other	7,08	3,74	4,46	7,92	8,78	4,00	27,78

Quelle: Eigene Darstellung

4.2.10. Hinweis auf die Datenschutzklausel

Hypothese 10: Beim Großteil der Personen die im Internet bereits eingekauft hatten, wurde nicht speziell auf die Datenschutzklausel des Shopbetreibers hingewiesen.

Die Hypothese hat sich nicht bestätigen können. Wie in Tabelle 40 zu sehen ist, wurde bei 70% der Befragten beim Kauf im Internet auf die Datenschutzklausel hingewiesen.

Tabelle 40: Anzahl der Befragten bei denen auf die Datenschutzklausel hingewiesen wurde

Anzahl d Befr bei denen auf PP hingewiesen wurde (in %)	Kein Hinweis (in %)	n
831 (69,95%)	357 (30,05%)	1188 (100%)

Quelle: Eigene Darstellung

4.2.11. Einfluss von Datenschutzzertifikaten

Hypothese 11: Datenschutzzertifikate haben mehr Einfluss auf Personen. die noch nie im Internet eingekauft haben, als bei regelmäßigen Einkäufern, da der Shop entweder empfohlen wurde oder der Preis das ausschlaggebende Argument für den Kauf war.

In Tabelle 41 wurden die erfassten Zahlen der Befragung in Bezug auf den Einfluss von Datenschutzzertifikaten zusammengefasst.

Tabelle 41: Einfluss von Datenschutzzertifikaten auf Online-Käufer und Nicht-Käufer

Anzahl	Datenschutzzertifikat hat Einfluss (in %)	Datenschutzzertifikat hat keinen Einfluss (in %)	Wussten nicht was ein Datenschutzzertifikat ist (in %)	Summe (in %)
Online-Käufer	676 (56,76%)	298 (25,02%)	217 (18,22%)	1191 (100%)
Keine Online-Käufer	77 (54,23%)	39 (27,46%)	26 (18,31%)	142 (100%)

Quelle: Eigene Darstellung

In der nachfolgenden Tabelle 42 werden die berechneten Werte des Chi-Quadrat-Tests dargestellt.

Tabelle 42: Chi-Quadrat-Werte der Hypothese 11

Einfluss von Datenschutzzertifikaten	Testgröße	Freiheitsgrade	Signifikanz
Online-Käufer	0,02	1	<90%
Keine Online-Käufer	0,13	1	<90%
Summe	0,14	2	<90%

Quelle: Eigene Darstellung

Die Signifikanz des Einflusses von Datenschutzzertifikaten sowohl auf Online-Käufer als auch Nicht-Käufer ist kleiner als 90%. Somit kann Hypothese 11 in dieser Hinsicht nicht bestätigt werden.

An erster Stelle der Gründe für den Online-Kauf der Befragten war der gute Preis mit 22%, gefolgt von der Bequemlichkeit mit 19% und an dritter Stelle die Zeitersparnis mit 16% (siehe Tabelle 43). Das heißt, dass zwar der Preis ein ausschlagendes Ar-

gument für den Online-Kauf ist, aber die Weiterempfehlung nicht, damit konnte Hypothese 11 zumindest in diesem Punkt bestätigt werden.

Tabelle 43: Gründe für den Online-Kauf

Gründe für den Online Kauf	Absolute Zahlen (in %)
Guter Preis	798 (22,45%)
Bequemlichkeit	682 (19,19%)
Zeitersparnis	581 (16,35%)
Direkter Preisvergleich möglich	404 (11,37%)
Ausschließliche Verfügbarkeit	396 (11,14%)
Größere Auswahl als im herkömmlichen Geschäft	358 (10,07%)
Man hat mehr Ruhe als im Geschäft	161 (4,53%)
Other	55 (1,55%)
Empfehlung des Shops durch Freunde/Bekannte	45 (1,27%)
Neugier	34 (0,96%)
Ich wollte bei einer Online-Auktion teilnehmen (Unterhaltungswert der Auktion)	32 (0,90%)
Der Shop wurde in den Medien empfohlen	8 (0,23%)

Quelle: Eigene Darstellung

4.2.12. Einflüsse auf das Kaufverhalten

Hypothese 12: Faktoren wie bekannte Marke/Hersteller und Weiterempfehlung haben den größten Einfluss auf das Kaufverhalten sowohl von Nichtkäufern als auch auf Käufer.

Jeweils 100%ige Übereinstimmung sowohl von Nicht-Käufern als auch von Käufern fand der Faktor, dass die Marke beziehungsweise der Hersteller bekannt sind. An zweiter Stelle stand jeweils, dass der Shop gekannt wird. Lediglich der dritte Platz der Einflüsse auf das Kaufverhalten unterscheidet sich bei Online-Käufern (schnelle Lieferung) und Nicht-Käufern (Zahlungsart kann selbst ausgewählt werden). An erster Stelle bei der großteils Übereinstimmung von Nicht-Käufern und Käufern ist die Empfehlung des Shops durch Freunde oder Bekannte. An zweiter Stelle ist jedoch bei den Nicht-Käufern eine schnelle Lieferung, gefolgt von der Möglichkeit die Zah-

lungsart selbst zu wählen. Bei den Online-Käufern steht hingegen jeweils an zweiter Stelle eine seriöse Homepage und eine schnelle Lieferung als Kaufargument.

Tabelle 44: Top 3 Ranking der Einflüsse auf das Kaufverhalten von Nicht-Käufern

Nicht-Käufer	In %	Gründe für einen möglichen Online-Kauf
stimme großteils überein	52,82%	Empfehlung durch Freunde oder Bekannte
	47,18%	Schnelle Lieferung
	44,37%	Ich kann mir die Zahlungsart selbst aussuchen
stimme 100%ig überein	47,18%	Ich kenne die Marke beziehungsweise den Hersteller
	42,96%	Ich kenne den Shop
	36,62%	Ich kann mir die Zahlungsart selbst aussuchen

Quelle: Eigene Darstellung

Tabelle 45: Top 3 Ranking der Einflüsse auf das Kaufverhalten von Online-Käufern

Online-Käufer	In %	Gründe für einen möglichen Online-Kauf
stimme großteils überein	52,31%	Empfehlung durch Freunde oder Bekannte
	42,99%	Die Homepage wirkt seriös
	42,99%	Schnelle Lieferung
stimme 100%ig überein	57,26%	Ich kenne die Marke beziehungsweise den Hersteller
	55,67%	Ich kenne den Shop
	43,74%	Schnelle Lieferung

Quelle: Eigene Darstellung

Bei der Berechnung der Chi-Quadrat-Werte wurden zur Vereinfachung die absoluten Werte der Kategorien „stimme großteils überein“ und „stimme 100%ig überein“ in der Gruppe „stimme zu“ zusammengefasst. Des Weiteren wurden nur die Werte für die Einflussfaktoren „Empfehlung durch Freunde oder Bekannte“, „Schnelle Lieferung“ und „Ich kenne die Marke beziehungsweise den Hersteller“ berechnet. In der nachfolgenden Tabelle 46 werden die berechneten Werte dargestellt.

Tabelle 46: Chi-Quadrat-Werte der Hypothese 12

Empfehlung durch Freunde oder Bekannte	Testgröße	Freiheitsgrade	Signifikanz
Online-Käufer	0,1	1	<90%
Keine Online-Käufer	0,82	1	<90%
Schnelle Lieferung	Testgröße	Freiheitsgrade	Signifikanz
Online-Käufer	0,54	1	<90%
Keine Online-Käufer	4,54	1	95%
Ich kenne die Marke beziehungsweise den Hersteller	Testgröße	Freiheitsgrade	Signifikanz
Online-Käufer	0,01	1	<90%
Keine Online-Käufer	0,07	1	<90%
Summe	6,07	6	<90%

Quelle: Eigene Darstellung

Aus den Signifikanzwerten in Tabelle 46 kann geschlossen werden, dass es im Bezug auf die Einflussfaktoren für einen Online-Kauf keine signifikanten Unterschiede zwischen Online-Käufern und Nicht-Online-Käufern gibt.

4.2.13. Zusammenfassung der Ergebnisse

Bei der durchgeführten Befragung konnten sechs der insgesamt zwölf Hypothesen bestätigt werden. Das Geschlecht der Befragten hatte einen Einfluss auf deren Kaufverhalten. Des Weiteren hat die Höhe des Einkommens keinen Einfluss auf die Angst vor Zahlungsmittelmissbrauch. Bei der Befragung konnten folgende Gründe für den Nicht-Kauf über das Internet festgestellt werden:

- Bevorzugung des traditionellen Einkaufs
- Bedenken aufgrund der Sicherheit der Daten
- Unsicherheit der Zahlungsmittel.

65% der Befragten lesen sich bei einem Online-Kauf die Datenschutzerklärung nicht durch, was einerseits nicht überraschend, aber trotzdem erschreckend ist. Von den Personen, welche die Klausel sich durchgelesen hatten, haben 65% laut eigenen Angaben diese nicht verstanden, was wiederum bestätigt, dass die mangelnde Verständlichkeit ein großes Problem darstellt. Lediglich 10% der Befragten gaben an,

dass sie die Datenschutzerklärung nicht gelesen hatten, weil sie nicht gefunden wurde. Dieser Punkt ist als positiv anzusehen, da die Annahme war, dass mehr Nutzer die Erklärung nicht finden. Eine gut geschriebene Datenschutzklausel hat des Weiteren sowohl auf regelmäßige als auch auf unregelmäßige Online-Käufer und auf potentielle Käufer den selben Einfluss. Bei der Befragung ergab sich, dass vor allem im niedrigen und mittleren Preissegment im Internet eingekauft wird. Des Weiteren konnte anhand der Befragung ermittelt werden, dass als ausschlaggebende Kaufargumente für die Befragten folgende Faktoren gelten:

- Ich kenne die Marke beziehungsweise den Hersteller
- Eine verständliche Datenschutzerklärung
- Der Shop wurde in Medien beworben beziehungsweise empfohlen
- Der Shop besitzt ein Datenschutzzertifikat
- Ich kenne den Shop
- Schnelle Lieferung

Darüber hinaus konnte festgestellt werden, dass die befragten Online-Käufer am Meisten Angst vor der Übermittlung ihrer Daten und deren Sicherheit haben. Dies könnte auch auf die schwere Verständlichkeit der Datenschutzerklärungen der Shopbetreiber zurückzuführen sein. Die am Meisten genutzten Zahlungsmittel beim Online-Kauf sind die Kreditkarte, die Vorkasse und der Zahlschein. Als Gründe für den Online-Kauf wurde an erster Stelle der gute Preis, an zweiter Stelle die Bequemlichkeit und auf der dritten Stelle die Zeitersparnis genannt.

5. Zusammenfassung und Ausblick

Diese Arbeit beschäftigte sich zuerst mit der Definition von Datenschutz und Privatsphäre. Dabei wurde die Frage beantwortet, wozu Unternehmen sich mit dem Thema Datenschutz auseinandersetzen sollten. Als Gründe wurden nicht nur rechtliche Standards, die jedes Unternehmen erfüllen muss, sondern auch ökonomische Determinanten aufgezeigt. Aufgrund der Besonderheit des Konsumentenvertrauens im Internet ist es für Anbieter von Produkten und Dienstleistungen besonders wichtig, eine transparente Datenverarbeitung präsentieren zu können und den Kunden eine Vertrauensgrundlage zu bieten.

In Kapitel 2.4. wurden die rechtlichen Grundlagen zum Thema Datenschutz zusammengefasst. Dabei wurde das österreichische Datenschutzgesetz (DSG 2000), die Datenschutzrichtlinie 95/46/EG und die Vorratsdatenspeicherungs-Richtlinie 2006/24/EG der Europäischen Union, sowie das Telekommunikationsgesetz (TKG 2003) vorgestellt. Des Weiteren wurden Sonderfälle des Datenschutzes im Internet aufgezeigt. Hierbei wurden Cookies, Logfiles, Web-Bugs, der Schutz von E-Mails und die Auskunftspflicht des Access-Providers erläutert.

In einem weiteren Schritt wurden die datenschutzfreundlichen Technologien (in dieser Arbeit mit PET bezeichnet) vorgestellt. Unter PETs sind Technologien zu verstehen, die Nutzern helfen sollen. die eigenen persönlichen Daten im Internet zu schützen. Es wurden Funktionen vorgestellt, die von PETs übernommen werden können, sowie Merkmale zur Evaluierung von Datenschutzstandards einer Webseite aufgezeigt. Anschließend wurde die Funktionsweise einiger PETs im Detail vorgestellt und deren Vor- und Nachteile sowie Verbesserungspotentiale erläutert. Dieses Kapitel sollte vor allem eine Wissensgrundlage für den/die LeserIn sein, um ein leichteres Verständnis für Kapitel drei zu gewährleisten.

Kapitel drei beschäftigte sich im Detail mit den PETs P3P, APPEL und EPAL. Zunächst wurde die Funktionsweise, ein Anwendungsbeispiel sowie Vor- und Nachteile des jeweiligen Tools vorgestellt. Wesentlicher Unterschied der im Detail vorgestellten PETs ist, dass P3P und APPEL primär für die Nutzung durch den Endnutzer konzipiert wurden und EPAL eine Alternative für Unternehmen darstellt.

Der empirische Teil gliedert sich in zwei Unterkapitel. Das erste Unterkapitel beschäftigte sich mit dem Einsatz von P3P durch Unternehmen. Zuerst wurden Unternehmen aus der Forbes 400 Liste der Branchen Software und Services, Telekommunikationsservices, Medien und Einzelhandel ausgewählt. Danach konnte untersucht werden, ob diese auf ihren Webseiten eine P3P Compact Policy einsetzen. In einem weiteren Schritt wurde dann die Compact Policy mit der für den Menschen lesbaren Datenschutzerklärung verglichen, um etwaige Abweichungen aufzudecken. Dabei konnten teilweise erhebliche Diskrepanzen zwischen den beiden Erklärungen festgestellt werden.

Das zweite Kapitel des empirischen Teils beschäftigte sich mit der Kundenseite. Es zwar sollten Einflussfaktoren auf das Kaufverhalten im Internet und eventuelle Ängste sowie der Einfluss und die Wahrnehmung von Datenschutzerklärungen und -zertifikaten auf die Kundenseite untersucht werden. Zuerst wurden 12 Hypothesen formuliert und nachdem diese in Konstrukte kategorisiert wurden, konnte ein Online-Fragebogen erstellt werden. Der Link zu dem Online-Fragebogen wurde dann per E-Mail an StudentInnen der Wirtschaftsuniversität Wien versandt. Es wurden insgesamt 1.450 Fragebögen ausgefüllt, wovon 117 unvollständig waren. Bei der Befragung ergab sich, dass zwar die Datenschutzerklärungen leicht zu finden waren, aber von 65% der Befragten nicht verstanden wurde. In dieser Hinsicht müssten die Shopbetreiber noch einiges ändern und die Erklärungen hinsichtlich des Verständnisses für die Konsumenten überarbeiten. Unsicherheiten bezüglich der persönlichen Daten und Zahlungsmittel sind darüberhinaus ausschlaggebende Gründe warum die Befragten nicht im Internet ihre Einkäufe tätigen. Dabei konnte bei der Befragung ein Einfluss des Geschlechtes festgestellt werden, während die Höhe des Einkommens keine Rolle bei der Angst vor Zahlungsmittelmissbrauch spielt. Bei der Befragung ergab sich des Weiteren, dass eine gut geschriebene Datenschutzklausel sowohl auf regelmäßige als auch auf unregelmäßige Online-Käufer den selben Einfluss hat.

Ein Verbesserungspotential im Hinblick auf PETs ist mit Sicherheit in einer besseren Handhabung der Tools zu sehen, wodurch es für die Endnutzer einfacher sein soll diese zu bedienen. Dies könnte beispielsweise durch Implementierung eines übersichtlichen Benutzer Interfaces und Integration mehrerer Tools funktionieren. Des Weiteren müssen Internet-Nutzer vermehrt auf Risiken bei der Übertragung von per-

sönlichen Daten aufmerksam gemacht werden. Dies sollte die Nutzer aber keinesfalls verängstigen, sondern lediglich bewusst machen, dass die eigene Sorgfalt bei der Übermittlung von persönlichen Daten derzeit nicht von einem PET übernommen werden kann [Cranor L. F., 2003, S. 83].

IV. Anhang

Befragung von StudentInnen bezüglich Datenschutz im Internet

Mein Name ist Sandra Wickenhauser und ich bin Diplomandin am Institut für Informationswirtschaft. Im Rahmen meiner Diplomarbeit zu dem Thema „Elektronischer Datenschutz“ möchte ich Dich, um die Konsumentenseite diesbezüglich zu untersuchen, befragen. Um in meiner Diplomarbeit einen empirisch gehaltvollen Teil liefern zu können, ist mir jeder ausgefüllte Fragebogen sehr wichtig und wertvoll. Darum bitte ich Dich um eine ehrliche Beantwortung der Fragen und möchte Dich des Weiteren darauf hinweisen, dass es keine „richtigen“ oder „falschen“ Antworten gibt.

Ich gewährleiste Dir, dass die Daten anonymisiert erhoben werden. Solltest Du Fragen bzw. Anregungen haben, kannst Du mich jederzeit per E-Mail kontaktieren.

Das Ausfüllen des Fragebogens dauert ca. 5 Minuten.

Allgemeine Fragen zum Kaufverhalten im Internet

Frage 1: Hast Du schon einmal über das Internet etwas gekauft bzw. ersteigert?

Bitte wähle nur eine der folgenden Antworten aus:

- ☐ Ja
- ☐ Nein

[Bitte beantworte diese Frage nur, falls Deine Antwort 'Nein' war bei der Frage 'Frage 1']

Frage 2: Warum hast Du noch nie etwas über das Internet etwas gekauft bzw. ersteigert? (Mehrfachantworten möglich)

Bitte wähle alle Punkte aus, die zutreffen:

- ☐ Hat sich noch nicht ergeben, bin aber durchaus daran interessiert
- ☐ Ich kaufe lieber auf die traditionelle Art ein, d.h. ich sehe mir lieber die Ware selbst an
- ☐ Ich habe Bedenken aufgrund der Sicherheit meiner Daten
- ☐ Ich lasse mich lieber von einem/r VerkäuferIn persönlich beraten
- ☐ Ich habe kein Vertrauen in Internetshops
- ☐ Ich hätte Bedenken aufgrund der Eigenschaften der Ware (z.B.: Qualität, Funktionalität, Größe bei Kleidung, etc.)
- ☐ Ich hätte Angst, dass mir wesentliche Faktoren (z.B.: Umtauschmöglichkeiten, Lieferzeit) unklar sind
- ☐ Ich habe kein Vertrauen in elektronische Auktionshäuser
- ☐ Ich wollte schon öfters online einkaufen, habe aber dann den Kaufprozess vorzeitig abgebrochen, weil mir etwas unklar war
- ☐ Ich befürchte, dass meine Daten an Dritte weitergegeben werden
- ☐ Die Zahlungsmethoden sind mir zu unsicher

Sonstiges: _____

[Bitte beantworte diese Frage nur, falls Deine Antwort 'Ja' war bei der Frage 'Frage 1']
Frage 3: Wie oft kaufst Du durchschnittlich im Internet ein?
Bitte wähle nur eine der folgenden Antworten aus:

- ☐ weniger als alle 3 Monate
- ☐ mind. 1mal in 3 Monaten
- ☐ mind. 1mal pro Monat

Analyse der letzten Kaufsituation

Denke nun bitte an Deinen letzten, im Internet getätigten Einkauf. Beantworte bitte die folgenden Fragen hinsichtlich dieses letzten Kaufs im Internet.

[Bitte beantworte diese Frage nur, falls Deine Antwort 'Ja' war bei der Frage 'Frage 1']
Frage 4: Ordne bitte Deinen Einkauf in eines der nachfolgenden Preissegmente ein:
Bitte wähle nur eine der folgenden Antworten aus:

- ☐ niedriges Preissegment (<50€)
- ☐ mittleres Preissegment (55-150€)
- ☐ höheres Preissegment (155-300€)
- ☐ hohes Preissegment (>300€)

[Bitte beantworte diese Frage nur, falls Deine Antwort 'Ja' war bei der Frage 'Frage 1']
Frage 5: Was war der Grund für Deinen Einkauf? (Mehrfachantworten möglich)
Bitte wähle alle Punkte aus, die zutreffen:

- ☐ Bequemlichkeit
- ☐ Guter Preis
- ☐ Empfehlung des Shops durch Freunde/Bekannte
- ☐ Ich wollte bei einer Online-Auktion teilnehmen (Unterhaltungswert der Auktion)
- ☐ Der Shop wurde in den Medien empfohlen
- ☐ Neugier
- ☐ Ausschließliche Verfügbarkeit
- ☐ Man hat mehr Ruhe als im Geschäft
- ☐ Zeitersparnis
- ☐ Größere Auswahl als im herkömmlichen Geschäft
- ☐ Direkter Preisvergleich möglich

Sonstiges: _____

[Bitte beantworte diese Frage nur, falls Deine Antwort 'Ja' war bei der Frage 'Frage 1']
Frage 6: Hattest Du Bedenken auf Grund der Übermittlung Deiner Daten (z.B.: Name, Adresse, etc.)?

Bitte wähle nur eine der folgenden Antworten aus:

- ☐ Ja
- ☐ Nein

[Bitte beantworte diese Frage nur, falls Deine Antwort 'Ja' war bei der Frage 'Frage 1' *und* falls Deine Antwort 'Ja' war bei der Frage 'Frage 6']

Frage 7: Warum hattest du Bedenken? (Mehrfachantworten möglich)

Bitte wähle alle Punkte aus, die zutreffen:

- ☐ Ich wusste nicht was der Shopbetreiber mit meinen Daten macht (z.B.: Nicht autorisierte Weitergabe oder Verkauf der Daten an Dritte, etc.)
- ☐ Habe ich immer, wenn ich Daten über das Internet übermitteln muss
- ☐ Ich habe Angst davor, dass jemand meine Daten abfängt (Hacker)
- ☐ Ich befürchte, dass ich Spammails erhalte
- ☐ Ich befürchte, dass ich nicht erwünschte Werbung an meine Postadresse erhalte
- ☐ Habe ich immer beim ersten Einkauf bei einem neuen Shop
- ☐ Habe ich generell immer wenn ich online einkaufe
- ☐ Ich befürchte, dass ich unaufgefordert Newsletter erhalte

Sonstiges: ☐

[Bitte beantworte diese Frage nur, falls Deine Antwort 'Ja' war bei der Frage 'Frage 1']

Frage 8: Wie hast Du bezahlt? (Mehrfachantworten möglich)

Bitte wähle alle Punkte aus, die zutreffen:

- ☐ Nachnahme
- ☐ Zahlschein
- ☐ Vorkasse
- ☐ Kreditkarte
- ☐ Paypal
- ☐ Paysafe
- ☐ Moneybookers
- ☐ Online-Überweisung

Sonstiges: ☐

[Bitte beantworte diese Frage nur, falls Deine Antwort 'Ja' war bei der Frage 'Frage1']

Frage 9: Aus welchem Grund hast Du die Zahlungsart gewählt?

Bitte wähle alle Punkte aus, die zutreffen:

- ☐ Wurde vom Shopbetreiber vorgegeben
- ☐ Aufgrund der Sicherheit der Zahlungsart
- ☐ War für mich persönlich am Bequemsten
- ☐ War die einzige Möglichkeit für mich

☐ Einfach so

Sonstiges:

[Bitte beantworte diese Frage nur, falls Deine Antwort 'Ja' war bei der Frage 'Frage 1']

Frage 10: Hattest Du etwaige schlechte Erfahrungen beim Kauf über das Internet?

Bitte wähle nur eine der folgenden Antworten aus:

☐ Ja

☐ Nein

[Bitte beantworte diese Frage nur, falls Deine Antwort 'Ja' war bei der Frage 'Frage1' *und* falls Deine Antwort 'Ja' war bei der Frage 'Frage 10']

Frage 11: Was ist passiert? (Mehrfachantworten möglich)

Bitte wähle alle Punkte aus, die zutreffen:

☐ Lieferung nicht erhalten

☐ Habe falsche Ware erhalten

☐ Probleme mit der Zahlungsart

☐ Ware war mangelhaft

☐ Lieferung später erhalten als vereinbart war

☐ Ich erhielt plötzlich Spammails

☐ Mir wurde unaufgefordert Werbung zugesandt

☐ Ich erhielt unaufgefordert einen Newsletter

Sonstiges:

[Bitte beantworte diese Frage nur, falls Deine Antwort 'Ja' war bei der Frage 'Frage 1']

Frage 12: Hast Du Dir beim Einkauf die Datenschutzklausel des Anbieters durchgelesen?

Bitte wähle nur eine der folgenden Antworten aus:

☐ Ja

☐ Nein

[Bitte beantworte diese Frage nur, falls Deine Antwort 'Ja' war bei der Frage 'Frage1' *und* falls Deine Antwort 'Nein' war bei der Frage 'Frage 12']

Frage 13: Wenn Nein, war es weil Du die Datenschutzklausel nicht gefunden hast?

Bitte wähle nur eine der folgenden Antworten aus:

☐ Ja

☐ Nein

[Bitte beantworte diese Frage nur, falls Deine Antwort 'Ja' war bei der Frage 'Frage 1' *und* falls Deine Antwort 'Ja' war bei der Frage 'Frage 12']

Frage 14: Wenn Ja, war es für Dich verständlich was mit Deinen Daten passiert?

Bitte wähle nur eine der folgenden Antworten aus:

☐ Ja

☐ Nein

[Bitte beantworte diese Frage nur, falls Deine Antwort 'Ja' war bei der Frage 'Frage 1']
Frage 15: Wurde beim Einkauf auf die Datenschutzklausel des Shopbetreibers hingewiesen?
Bitte wähle nur eine der folgenden Antworten aus:

- ☐ Ja
- ☐ Nein

[Bitte beantworte diese Frage nur, falls Deine Antwort 'Ja' war bei der Frage 'Frage 1']
Frage 16: Ist es für Dich wichtig, dass ein Internetshop eine Datenschutzklausel hat?
Bitte wähle nur eine der folgenden Antworten aus:

- ☐ Ja
- ☐ Nein

Explizite Fragen zu Datenschutz

Achtung: Beantworte bitte die nachfolgenden Fragen, egal ob Du schon einmal online eingekauft hast oder nicht

Unter einer Datenschutzklausel versteht man eine Erklärung des Webseitenbetreibers wie mit den übermittelten Daten umgegangen wird. D.h. der/die BetreiberIn erklärt explizit welche Daten erhoben, gespeichert und eventuell an Dritte weitergegeben werden.

Frage 17: Denkst Du, dass die Art wie die Datenschutzklausel geschrieben ist, einen Einfluss auf die Entscheidung hat, ob du in einem Internetshop bzw. Auktionshaus kaufst oder nicht?
Bitte wähle nur eine der folgenden Antworten aus:

- ☐ Nein
- ☐ Ja
- ☐ weiß nicht

Frage 18: Denkst Du, dass sog. Datenschutzzertifikate einen Einfluss auf Dein Einkaufsverhalten haben bzw. hätten?
Bitte wähle nur eine der folgenden Antworten aus:

- ☐ Ja
- ☐ Nein
- ☐ Was ist das?

Einflussfaktoren auf den Kaufprozess

Achtung: Beantworte bitte die nachfolgenden Fragen, egal ob Du schon einmal online eingekauft hast oder nicht

Unter Datenschutzzertifikaten versteht man eine Art "Gütesiegel" welche Unternehmen auszeichnen, dass sie bestimmte, vom Zertifikat vorgeschriebene, Auflagen einhalten. Dabei spielt vor allem eine gesetzeskonforme Verarbeitung persönlicher Daten eine zentrale Rolle.

Frage 19: Welche der nachfolgenden Faktoren haben bzw. hätten Deiner Meinung nach einen Einfluss darauf, ob Du in einem Internetshop einkaufst? Bewerte bitte die folgenden Aussagen anhand deiner Zustimmung.

Bitte wähle die zutreffende Antwort aus:

	stimme 100%ig überein	stimme großteils überein	stimme weniger überein	stimme gar nicht überein
Ich kenne die Marke bzw. den Hersteller	☐	☐	☐	☐
Empfehlung durch Freunde oder Bekannte	☐	☐	☐	☐
Eine verständliche Datenschutzerklärung	☐	☐	☐	☐
Die Homepage wirkt seriös	☐	☐	☐	☐
Der Shop wurde in Medien beworben bzw. empfohlen	☐	☐	☐	☐
Der Shop besitzt ein Datenschutzzertifikat	☐	☐	☐	☐
Flexible Umtauschmöglichkeiten	☐	☐	☐	☐
Ich finde mich leicht auf der Homepage zurecht	☐	☐	☐	☐
Ich kenne den Shop	☐	☐	☐	☐
Billiger Preis	☐	☐	☐	☐
Keine Lieferkosten	☐	☐	☐	☐
Ich kann mir die Zahlungsart selbst aussuchen	☐	☐	☐	☐
Schnelle Lieferung	☐	☐	☐	☐

Allgemeine Fragen zur Person

Frage 20: Wie alt bist Du?

Bitte gib hier Dein Alter in Jahren ein.

Bitte schreibe Deine Antwort hier:

Frage 21: Geschlecht?

Bitte wähle nur eine der folgenden Antworten aus:

- ☐ Männlich
- ☐ Weiblich

Frage 22: Bist Du berufstätig? Bitte wähle nur eine der folgenden Antworten aus:

- ☐ nein
- ☐ ja

Frage 23: Wie hoch ist Dein monatliches Nettoeinkommen? (Wie viel Geld steht Dir monatlich zur Verfügung abzüglich Miete, Versicherungen, etc.)

Bitte wähle nur eine der folgenden Antworten aus:

- ☐ weniger als 100€
- ☐ 100-300€

- ☐ 350-500€
- ☐ 550-700€
- ☐ 750-900€
- ☐ mehr als 900€

Frage 24: Wie oft benutzt Du das Internet?
Bitte wähle nur eine der folgenden Antworten aus:

- ☐ Täglich
- ☐ Wöchentlich
- ☐ Alle 2-3 Wochen
- ☐ 1mal pro Monat
- ☐ weniger als 1mal pro Monat

Frage 25: Wozu benutzt Du das Internet nach eigenem Ermessen am Meisten?
Bitte wähle nur eine der folgenden Antworten aus:

- ☐ für private Zwecke
- ☐ für die Universität
- ☐ in der Arbeit
- ☐ Sonstiges

Absenden der Umfrage.
Vielen Dank für die Beantwortung des Fragebogens..

6. Literaturverzeichnis

[ACTA, 2007] Allensbacher Berichte 2007 / Nr. 17, November 2007.
Abgerufen am 30. Dezember 2007 vom Institut für Demoskopie Allensbach: http://www.ifd-allensbach.de/pdf/prd_0717.pdf

[Ashley, P., Hada, S., Karjoth, G., Powers, C., & Schunter, M., 2003] Enterprise Privacy Authorization Language (EPAL 1.2), 10. November 2003.
Abgerufen am 07. Juli 2008 von World Wide Web Consortium: http://www.w3.org/Submission/2003/SUBM-EPAL-20031110/

[Ashley, P., Hada, S., Karjoth, G., Powers, C., & Schunter, M., 2002]. The Enterprise Privacy Authorization Language (EPAL) - How to Enforce Privacy throughout an Enterprise, 2002. Abgerufen am 07. Juli 2008 von World Wide Web Consortium: http://www.w3.org/2003/p3p-ws/pp/ibm3.html

[Bauer, H. H., 2006]. Konsumentenvertrauen. Konzepte und Anwendungen für ein nachhaltiges Kundenbindungsmanagement, 2006. München: Vahlen.

[Bornemann, D., Hennig-Thurau, T., & Hansen, U., 2006]. Das Konstrukt der Beziehungsqualität im Zeitalter des Internets. Ein Vergleich von Internethandel und stationärem Einzelhandel. In H. H. Bauer, Konsumentenvertrauen - Konzepte und Anwendungen für ein nachhaltiges Kundenbindungsmanagement (S. 325-340), 2006. München: Vahlen.

[CompactPrivacyPolicy, 2007]. Compact Privacy Policy. Abgerufen am 11. August 2008 von Compact Policy Cross-Reference, 12. Februar 2007: http://www.compactprivacypolicy.org/compact_token_reference.htm

[Cranor, L. F., 2003]. The Role of Privacy Enhancing Technologies, 2003. In P. J. Bruening, Considering Consumer Privacy: A Resource for Policymakers and Practitioners (S. 80-83). Washington: Center for Democracy and Technology.

[Cranor, L., Langheinrich, M., & Marchiori, M., 2002]. W3C Working Draft - A P3P Preference Exchange Language 1.0 (APPEL1.0), 15. April 2002. Abgerufen am 30. Juni 2008 von P3P: The Platform for Privacy Preferences: http://www.w3.org/TR/P3P-preferences/

[Datenschutzkommission, kein Datum]. Datenschutzgesetz 2000 - DSG 2000. Abgerufen am 29. Oktober 2007 von Österreichische Datenschutzkommission: http://www.dsk.gv.at/dsg2000d.htm

[Dohr, W., kein Datum]. Datenschutz in Österreich. Abgerufen am 04. Dezember 2007 von Zentrum Polis:

http://www.politik-lernen.at/_data/pdf/DatenschutzWalterDohr.pdf
[EDPS, kein Datum]. Der europäische Datenschutzbeauftragte. Abgerufen am 29. April 2008 von EDPS - European Data Protection Supervisor:
http://www.edps.eu.int
[Europ. Parlament, 13. April 2006]. Das Portal der Europäischen Union. Abgerufen am 17. Juni 2008 von Amtsblatt der Europäischen Union:
http://europa.eu.int/eur-lex/lex/LexUriServ/site/de/oj/2006/l_105/l_10520060413de00540063.pdf
[Fischer-Hübner, S., 2001]. IT-Security and Privacy. Design and Use of Privacy-Enhancing Security Mechanisms. Berlin: Springer.
[Gitter, R., & Schnabel, C., 2007]. Die Richtlinie zur Vorratsspeicherung und ihre Umsetzung in das nationale Recht, Juli 2007. Multimedia und Recht, S. 411-417.
[Götz, K., 2006]. Vertrauen in Organisationen. München und Mering: Rainer Hampp Verlag.
[Graf, W., 2004]. Datenschutzrecht im Überblick. Wien: Facultas WUV.
[Jahnel, D., 2007]. Aktuelle Fragen des Datenschutzrechts. Wien: Facultas.WUV.
[Janisch, S., & Mader, P., 2006]. E-Business. Wien: LexisNexis Verlag ARD Orac.
[Jensen, C., Sarkar, C., Jensen, C., & Potts, C., 2007]. Tracking website data-collection and privacy practices with the iwatch web crawler. SOUPS '07: Proceedings of the 3rd symposium on Usable privacy and security, (S. 29-40).
[Kenning, P., & Blut, M., 2006]. Vertrauen: Ein Konzept des Marketingmanagements?! In H. H. Bauer, Konsumentenvertrauen. Konzepte und Anwendungen für ein nachhaltiges Kundenbindungsmanagement (S. 3-16). München: Vahlen.
[Kobsa, 2007]. Privacy-enhanced personalization. Commun. ACM 50, 8; August 2007, 24-33.
[Kommission, 2007]. Mitteilung der Kommission an das Europäische Parlament und an den Rat, (07. März 2007. Abgerufen am 04. Dezember 2007 von Europäische Kommission:
http://ec.europa.eu/justice_home/fsj/privacy/docs/lawreport/com_2007_87_f_de.pdf
[Möller, J., 2003]. Datenschutz mit P3P, 07. Oktober 2003. Abgerufen am 14. Jänner 2008 von Unabhängiges Landeszentrum für Datenschutz Schleswig-Holstein: https://www.datenschutzzentrum.de/faq/p3p.htm

[Möller, J., 2004]. Enterprise Privacy Authorization Language (EPAL), 01. März 2004. Abgerufen am 07. Juli 2008 von Unabhängiges Landeszentrum für Datenschutz Schleswig-Holstein:
https://www.datenschutzzentrum.de/faq/epal.htm
[Neuberger, O., 2006]. Vertrauen vertrauen? Misstrauen als Sozialkapital. In K. Götz, Vertrauen in Organisationen. München und Mering: Rainer Hampp Verlag.
[Osterloh, M., & Weibel, A., 2006]. Investition Vertrauen. Prozesse der Vertrauensentwicklung in Organisationen. Wiesbaden: Gabler. ISBN 9783834990679
[P3PToolbox, kein Datum]. What is P3P and how does it work? Abgerufen am 20. September 2007 von P3P Toolbox:
http://p3ptoolbox.org/guide/section2.shtml#l
[Pommerening, K., 2004]. Datenschutz und Datensicherheit: Grundbegriffe, 05. Mai 2004. Abgerufen am 29. April 2008 von Grundprobleme von Datenschutz und Datensicherheit:
http://www.staff.uni-mainz.de/pommeren/DSVorlesung/Grundprobleme/Begriffe.html
[Trček, D., 2006]. Managing Information Systems Security and Privacy. Berlin: Springer. ISBN 9783540281030
[Ulber, P., 2004]. P3P - Ein Überblick, 16. Dezember 2004. Abgerufen am 19. Jänner 2008 von Der Große Bruder:
https://www.dergrossebruder.org/miniwahr/20041216163000.html
[W3C-Initiative, 2002]. More information on using P3P, 08. Mai 2002. Abgerufen am 07. April 2008 von P3P: The Platform for Privacy Preferences:
http://www.w3.org/P3P/details.html
[W3C-WorkingGroup, 2006] W3C Working Group Note - P3P Specification 1.1, 13. November 2006. Abgerufen am 25. Juni 2008 von P3P: The Platform for Privacy Preferences:
http://www.w3.org/TR/P3P11
[Weiber, R., & Egner-Duppich, C., 2006]. Vertrauen bei Online-Käufen: Ein transaktionsbezogener Ansatz aus informationsökonomischer Sicht. In H. Bauer, Konsumentenvertrauen. Konzepte und Anwendungen für ein nachhaltiges Kundenbindungsmanagement. München: Vahlen.