Rechtliche Implikationen der Personalisierung

von

Mathias Kummer, Petra Schubert und Uwe Leimstoll

www.weblaw.ch

Rechtliche Implikationen der Personalisierung

Datenschutz im E-Commerce

Mathias Kummer, Petra Schubert, Uwe Leimstoll

Inhalt

Ein Gemeinschaftsprojekt von

www.weblaw.ch

Fachhochschule beider Basel Nordwestschweiz FHBB | Departement Wirtschaft

Mit finanzieller Unterstützung von

soft[net]

1 Einführung in das Thema

Aktuelle Untersuchungen kommen häufig zum Ergebnis, dass der Internet-Auftritt vieler Unternehmen nicht den rechtlichen Anforderungen entspricht, die aus juristischer Sicht an öffentlich zugängliche Websites zu stellen sind. Dies mag aus der Diskrepanz zwischen einer marketingorientierten und einer juristisch geleiteten Sichtweise resultieren. Aus der Sicht des Marketing sollen dem Besucher einer Website nämlich nur die wichtigsten Informationen angeboten werden, um die Site übersichtlich und leicht bedienbar zu halten. Aus der Sicht des Juristen hingegen erfordert die Publikation von Inhalten im Internet eine Reihe begleitender Informationen über das Unternehmen, die Produkte und vor allem über den Umgang mit Kundendaten. Die vorliegende Broschüre beschreibt, welche Massnahmen wirklich wichtig sein können, um eine Website den rechtlichen Anforderungen entsprechend zu gestalten, ohne sie zu überladen.

Die persönlichen Daten der Kunden stehen in den folgenden Ausführungen im Vordergrund. Sie spielen für die Personalisierung von Informationsangeboten eine besondere Rolle. Die Broschüre liefert zunächst einen kurzen Überblick über die rechtlichen Grundlagen des E-Commerce und geht dann detailliert auf die datenschutzrechtlichen Aspekte des E-Commerce ein. Neben der Erläuterung häufig auftretender Fragen schildert die Analyse eines konkreten Fallbeispiels, welche Massnahmen den Umgang mit personenbezogenen Daten auf eine rechtlich solide Basis stellen.

Zunächst stellt sich die Frage, was das Besondere an personalisierten Angeboten im Internet und an der Behandlung der dazu benötigten persönlichen Daten ist. Personalisierung im E-Commerce bedeutet, dass dem Besucher einer Website Informationen angezeigt werden, die speziell auf seine Bedürfnisse und Interessen abgestimmt sind. Dies bringt sowohl für Online-Anbieter als auch für Online-Käufer viele Vorteile mit sich. Aufgrund der gesammelten und durch besondere Verfahren ausgewerteten Personendaten lassen sich individuelle Kaufempfehlungen erstellen. Die Bindung des Kunden an einen Anbieter nimmt dadurch zu und es entwickeln sich langfristige Kundenbeziehungen. Gleichzeitig können Werbekosten gesenkt und neue Kunden gewonnen werden. Auch das sogenannte Cross-Selling erfährt mit Hilfe der hinzugezogenen Kundendaten eine neue Qualität.

Um die Bedürfnisse und Interessen des Kunden aufzuspüren, ist die Speicherung und Verknüpfung von persönlichen Daten des Kunden nötig. Eine Vielzahl von Auswertungsmethoden insbesondere des Web Mining erlaubt es, Datenprofile zu generieren. Diese Datenprofile enthalten mitunter wesentlich mehr Informationen über den Kunden, als diesem bewusst ist. Die Tabelle auf der folgenden Seite gibt einen Überblick über verschiedene Profiltypen.

Den wirtschaftlichen Interessen des Anbieters und den Vorteilen für den Kunden steht also der Schutz der Persönlichkeit der betroffenen Person gegenüber. Dieser wird durch das Bundesgesetz über den Datenschutz (DSG) gewährleistet. Für Online-Anbieter gilt:

Nicht alles was machbar ist, ist auch erlaubt.

Profiltyp	Eigenschaft
Explizite Profile	
Identifikationsprofil (obligatorisches Kundenprofil)	Benutzername, Vorname, Name, Rechnungs- und Lieferadresse, Zahlungsinformationen, persönliche (Browser-) Einstellungen
Präferenzprofil	Selbstauswahl von angebotenen Präferenzkategorien (bei Büchern z.B. Science Fiction, Computer, Business), Hobbys, Interessen, Geschmack (die Kategorien entsprechen den Metadaten des Produktkatalogs)
Sozio-demographisches Profil	Selbstkategorisierung des Kunden in vordefinierte Kategorien (Alter, Geschlecht, Einkommen, Herkunft, Tätigkeit)
Ratings	Bewertungen von Produkten, Webseiten und Reviews anderer Kunden anhand vorgefertigter Skalen (z.B. Musikgeschmack: 1 für „sehr gut“ bis 5 für „sehr schlecht“)
Beziehungen (Community Profil)	Angabe von besonderen Beziehungen zu anderen Kunden (z.B. Soulsister, Affinitätsgruppen)
Reviews/Meinungen	Freitexteingaben von Meinungen und Erfahrungen, typische Community-Beiträge, Multimedia-Beiträge wie Bilder, Fotos, Videos, MP3-Dateien.
Implizite Profile	
Transaktionsprofil (TA-Profil)	Speicherung der durchgeführten Transaktionen (z.B. Käufe, Zahlungen, Inanspruchnahme von Dienstleistungen); gekaufte Produkte/Dienstleistungen werden ebenfalls den Vorgabekategorien (Metadaten) zugeordnet.
Interaktionsprofil	Summe der aufgezeichneten Zugriffe auf vordefinierte Kategorien (Metadaten), die ein vermeintliches Interesse widerspiegeln können (Politik, Computer, Weltgeschehen, Börse, etc.)
Externe Daten	Informationen aus anderen Quellen (z.B. Wetterbericht, regionale Nachrichten, Bonitätsinformationen)

Diese Tabelle gibt einen Überblick über verschiedene Profiltypen. In der Fallstudie (Kap. 4, S. 21) werden diese Profiltypen wieder aufgegriffen.

2 Rechtliche Grundlagen des E-Commerce

Obwohl es sich beim Internet um ein stetig an Bedeutung gewinnendes Medium ohne staatliche Grenzen handelt, stellt es keinen rechtsfreien Raum dar. Das Internet ist grundsätzlich den Schranken der jeweiligen nationalen Rechtsordnung unterworfen.

Das Schweizerische Recht kennt bis anhin nur sehr wenige Gesetzesbestimmungen, die ausdrücklich internetspezifische Sachverhalte regeln. Vielmehr werden bestehende Gesetze auch auf solche Sachverhalte angewendet. Unternehmungen, die E-Commerce betreiben, haben viele unterschiedliche Rechtsgebiete und Erlasse zu beachten. Die folgende, nicht abschliessende Übersicht zeigt betroffene Rechtsgebiete und die anwendbaren Erlasse.

Bereiche	**Erlasse**
Regeln zum Vertragsabschluss im Internet; Geltung von Online-AGB (Vertragsrecht)	OR
Anbieterkennzeichnung, Produktbeschreibung und Preisbekanntgabe (Lauterkeitsrecht, Vertragsrecht)	OR; UWG, PBV
Lieferbedingungen, Rückgabe, Widerruf, Gewährleistung, Haftung (Vertragsrecht)	OR
Konsumentenschutz im nationalen und internationalen Umfeld (Konsumentenrecht)	GestG; IPRG
Zulässigkeit der Verlinkung, Nutzung von fremden Inhalten (Immaterialgüterrecht)	URG; UWG; StGB
Verwendung von Domain Namen (Namensrecht, Markenrecht, Firmenrecht, Lauterkeitsrecht)	MSchG, ZGB, UWG, AEFV, etc.
Einhaltung der lauterkeitsrechtlichen Bestimmungen (u.a. keine Verwechslungsgefahr schaffen, keine Herabsetzung, vergleichende Werbung, etc.)	UWG
Kartellrechtlich bedeutsames Verhalten (Absprachen, Missbrauch der marktbeherrschenden Stellung, etc.)	KG
Straf- und zivilrechtliche Verantwortlichkeit für Inhalte	OR, StGB
Rechtsverhältnisse beim Einbezug von Kreditkarten	OR
Datenschutz im E-Commerce (Datenschutzrecht)	DSG, VDSG
Erläuterungen: **OR**: Obligationenrecht; **UWG**: Bundesgesetz gegen den unlauteren Wettbewerb; **PBV**: Preisbekanntgabeverordnung; **GestG**: Gerichtsstandsgesetz; **IPRG**: Bundesgesetz über das Internationale Privatrecht; **URG**: Urheberrechtsgesetz; **StGB**: Strafgesetzbuch; **MSchG**: Markenschutzgesetz; **AEFV**: Verordnung über die Adressierungselemente im Fernmeldebereich **KG**: Kartellgesetz; **DSG**: Datenschutzgesetz; **VDSG**: Verordnung zum Datenschutzgesetz	

Ausblick: Im Jahr 2001 hat der Bundesrat zwei Gesetzesentwürfe, die einschneidende Änderungen für den E-Commerce in der Schweiz vorsehen, in die Vernehmlassung geschickt. Es handelt sich um das **Bundesgesetz über Zertifizierungsdienste im Bereich der elektronischen Signatur (ZertES)** und um das **Bundesgesetz über den elektronischen Geschäftsverkehr**.

Durch das Inkrafttreten des weniger umstrittenen ZertES könnten schon in absehbarer Zeit rechtsgültige Unterschriften in elektronischer Form geleistet werden.

Der Gesetzesentwurf über den elektronischen Geschäftsverkehr zielt im Wesentlichen auf eine **Besserstellung des Konsumenten beim Online-Einkauf**. So soll beispielsweise die Einführung eines **7-tägigen Widerrufsrechts** auf im Fernabsatz geschlossene Verträge mit einem Transaktionswert von über 100 Franken Schutz vor unüberlegten Vertragsabschlüssen bieten. Nicht unter diese Regelung sollen u.a. Verträge mit Banken und Versicherungen fallen. Der Entwurf sieht zudem ausführliche **Impressumspflichten** für E-Shop-Betreiber vor.

Gefordert sind u.a. klare und vollständige Angaben über die Identität des Anbieters, seinen Sitz oder Wohnsitz, seine Adresse, E-Mail, eine Produktbeschreibung, genaue Preisangaben mit zusätzlich anfallenden Kosten, Zahlungsbedingungen, Lieferfristen, etc. Zudem wird der Anbieter verpflichtet, auf die einzelnen technischen Schritte, die zu einem Online-Vertragsschluss führen, hinzuweisen.

Gemäss Entwurf ist die Nichteinhaltung der Informationspflichten unlauter und kann zivil- und strafrechtliche Folgen haben.

Die Botschaft des Bundesrates, Vernehmlassungen und weitere Informationen zu den Gesetzesentwürfen finden sich auf der Website des Bundesamtes für Justiz.

www.bj.admin.ch/themen/e-commerce/intro-d.htm

2.1 Datenschutz im Speziellen

Wer im Internet surft, hinterlässt Spuren. Webserver speichern Angaben über Rechneradresse, Datum, Zeit, Aktion, etc. in sogenannten Logfiles. Auch auf dem Computer des Nutzers platzierte Cookies generieren nützliche Informationen. Sobald der Anbieter weitere, personenbezogene Daten über den Nutzer erhält – z.B. durch Angaben in Bestell- oder Anmeldefeldern – sind Verknüpfungen möglich, die zu umfangreichen **Persönlichkeitsprofilen** der Nutzer führen. Da die Daten elektronisch vorliegen, sind Verknüpfungen und Auswertungen durch Datenverarbeitungssysteme einfach.

Neue Technologien und Methoden ermöglichen es, kontinuierlich eine grosse Masse an Personendaten zu sammeln, zu ordnen und so auszuwerten, dass Gewohnheitsmuster, Kaufverhalten, zukünftige Trends und Kundenprofile erstellt werden können. Die Auswertungsmethoden des **Data Mining** erzeugen Informationen über Personen, die zuvor noch gar nicht explizit vorhanden waren.

Solche Profile können für Unternehmungen von grossem Wert sein. Individuell massgeschneiderte Kaufempfehlungen, Rabatte und Werbung binden Kunden an

das Unternehmen. Durch gezielte Direktmarketingmassnahmen werden Neukunden gewonnen. Das Konsumverhalten kann gezielt beeinflusst und gesteuert werden.

Das wirtschaftliche Wachstumspotenzial des elektronischen Geschäftsverkehrs wird als gross eingeschätzt. Es hängt jedoch direkt vom Vertrauen der Kunden ab. Dieses Vertrauen wird mit dem **Schutz der Privatheit** und mit der **Sicherheit des Datenverkehrs** gestärkt. Die aufgezeigten technischen Möglichkeiten gefährden bei rücksichtslosem Einsatz die Persönlichkeit und damit das Vertrauen der Kunden in den E-Commerce.

Es gibt eine Vielzahl vertrauensfördernder Massnahmen für den elektronischen Geschäftsverkehr. Die wichtigste Massnahme ist die **Einhaltung der einschlägigen datenschutzrechtlichen Grundsätze (DSG, VDSG)**. Auf das schweizerische Datenschutzgesetz wird im folgenden Abschnitt eingegangen. Zu weiteren vertrauensfördernden Massnahmen zählen: eine transparente Datenbearbeitung durch eine umfassende Datenbearbeitungserklärung, Wahlmöglichkeiten für die Begrenzung der Nutzung und Weitergabe von Personendaten, der Einsatz neuer technischer Möglichkeiten zum Schutz von Personendaten, das Einhalten von privaten Verhaltensregeln (Netiquette, Vorschriften von Verbänden) und die Überprüfung des eigenen Internetauftrittes in sogenannten Datenschutzaudits, verbunden mit der Platzierung eines Qualitätszeichens (Gütesiegel).

2.2 Die Datenschutzgesetzgebung

Menschen sollen selber über die Preisgabe und Verwendung ihrer persönlichen Daten bestimmen und frei über die Aufnahme und Gestaltung ihrer Informationsbeziehungen entscheiden können. Das besagt das im Datenschutzgesetz verwirklichte **Grundrecht der informationellen Selbstbestimmung (Art. 13 Abs. 2 BV)** .

Das **Bundesgesetz über den Datenschutz** vom 19. Juni 1992 (DSG) regelt die Handhabung von Personendaten, die von Privatpersonen und Bundesbehörden beschafft und bearbeitet werden. Kantonale Behörden unterstehen hingegen der kantonalen Datenschutzgesetzgebung.

Das Gesetz bezweckt den Schutz der Persönlichkeit und der Grundrechte von Personen, über die Daten gesammelt und bearbeitet werden (DSG 1). Geschützt werden sowohl natürliche wie auch juristische Personen.

Das Sammeln und Bearbeiten von Personendaten ist grundsätzlich erlaubt. Verhindert werden soll die missbräuchliche Handhabung der personenbezogenen Daten. Wann ein Missbrauch und damit eine Persönlichkeitsverletzung **durch Privatpersonen** vorliegt, wird in Art. 12 DSG umschrieben.

Eine Persönlichkeitsverletzung begeht, wer

1. Personendaten entgegen den datenschutzrechtlichen Grundsätzen (Rechtmässigkeit, Bearbeitung nach Treu und Glauben, Verhältnismässigkeit, Zweckmässigkeit, etc.) beschafft und bearbeitet,
2. Daten einer Person **gegen deren ausdrücklichen Willen bearbeitet** oder
3. **besonders schützenswerte Personendaten** (z.B. religiöse Ansichten, medizinischer Befund, etc.) **oder Persönlichkeitsprofile** (Zusammenstellung von Daten, die eine Beurteilung wesentlicher Aspekte der Persönlichkeit einer natürlichen Person erlaubt, z.B. Kundenprofile) **Dritten bekannt gibt**.

Hat der Bearbeitende keinen Rechtfertigungsgrund für die Persönlichkeitsverletzung, so ist diese widerrechtlich und kann zivilrechtliche Folgen mit sich bringen. Die Rechtsansprüche des Betroffenen sind in Art. 15 DSG und Art. 28 ff. DSG festgehalten. Die in ihrer Persönlichkeit verletzte Person kann u.a. einen Anspruch auf Schadenersatz, auf Berichtigung, Vernichtung und das Recht auf Sperrung der Bekanntgabe an Dritte geltend machen.

Der häufigste Rechtfertigungsgrund ist die rechtsgültige **Einwilligung des Betroffenen** in die Persönlichkeitsverletzung (vgl. auch Kap. 3, Fragestellung 2, S. 16). Bei der Personalisierung von E-Commerce-Applikationen kommt der Einwilligung eine zentrale Bedeutung zu. Die Einwilligung kann durch eine wahrheitsgetreue und umfassende Aufklärung eingeholt werden.

Als weitere Rechtfertigungsgründe sieht das DSG in Art. 13 **ein überwiegendes privates oder öffentliches Interesse** vor. Zudem ist die Verletzung der Persönlichkeit nicht widerrechtlich, wenn sie das Gesetz vorsieht. Die Beschaffung und Bearbeitung von Personendaten in unmittelbarem Zusammenhang mit dem Abschluss, der Abwicklung oder Erfüllung eines Vertrages, die Sammlung und Bearbeitung von Informationen zur Konkurrenz im Wettbewerb, die Prüfung der Kreditwürdigkeit, die Beschaffung und Auswertung von Personendaten **zu nicht personenbezogenen Zwecken** (Forschung, Planung, Statistik) und das Sammeln von Daten über eine Person des öffentlichen Lebens sind die im Datenschutzgesetz beispielhaft aufgezählten Rechtfertigungsgründe.

Wichtig: In der Regel liegt keine Persönlichkeitsverletzung vor, wenn die betroffene Person die Daten allgemein zugänglich gemacht und eine Bearbeitung nicht ausdrücklich untersagt hat (Art. 12 Abs. 3 DSG).

2.3 Die Grundsätze im Datenschutz

Der Verstoss gegen die Datenschutzgrundsätze ohne Rechtfertigungsgrund stellt eine widerrechtliche Persönlichkeitsverletzung dar (Art. 12 Abs. 2 lit. a DSG). Die Grundsätze sind in Art. 4 – Art. 7 DSG wiedergegeben.

Rechtmässigkeit

Personendaten dürfen nur rechtmässig beschafft werden (Art. 4 Abs. 1 DSG). Ein Verstoss gegen geltendes Recht stellt insbesondere das unbefugte Beschaffen von Personendaten nach Art. 179novies StGB dar: Wer unbefugt besonders schützenswerte Personendaten oder Persönlichkeitsprofile, die nicht frei zugänglich sind, aus

einer Datensammlung beschafft, wird auf Antrag mit Gefängnis oder mit Busse bestraft.

Treu und Glauben

Der Grundsatz verlangt eine transparente und lautere Beschaffung und Bearbeitung der Personendaten (Art. 4 Abs. 2 DSG). Geschützt werden soll die Freiwilligkeit der Zurverfügungstellung von Daten. Das bedingt, dass Daten nicht unter Vorspiegelung falscher Tatsachen beschafft und nicht ungefragt für einen anderen Zweck eingesetzt werden. Ebenfalls einen Verstoss gegen den Grundsatz von Treu und Glauben stellt die völlig intransparente oder verschleierte Zweckangabe dar. Zudem dürfen die Daten nicht in einer Art und Weise verwendet werden, die für den Betroffenen völlig unerwartet ist.

Bedeutung für personalisierte E-Commerce-Lösungen: Die Beschaffung und Bearbeitung der Daten hat transparent und lauter zu erfolgen. Der Kunde ist über den Zweck der Bearbeitung zu orientieren. Das Profiling ermöglicht Verknüpfungen von Personendaten, durch die man völlig neue persönliche Informationen gewinnen kann. Wird der Betroffene nicht darüber aufgeklärt, so verstösst der Bearbeitende gegen das Prinzip von Treu und Glauben. Allgemeine Aussagen wie „Sammlung von Daten zur administrativen Verarbeitung“ sind (zu) wenig aussagekräftig und abzulehnen.

Verhältnismässigkeit

Nach dem Grundsatz der Verhältnismässigkeit dürfen nur die Personendaten gesammelt und bearbeitet werden, die **geeignet** und **erforderlich** sind, um den (legalen) Zweck der Bearbeitung zu erfüllen. Zudem muss der Eingriff in die Persönlichkeit im Verhältnis zum Zweck schonend erfolgen (Art. 4 Abs. 2 DSG).

Für die Abwicklung von elektronischen Geschäftstransaktionen sind oftmals viel weniger Daten notwendig als die in einer Eingabemaske gesammelten Angaben. Auf die Abfrage von besonders sensiblen Personendaten ist – wenn möglich – zu verzichten. Sammlungen auf Vorrat sind zu unterlassen. Ziel ist die **Vermeidung unnötiger Daten**.

Bedeutung für personalisierte E-Commerce-Lösungen: Jede Beschaffung und Bearbeitung von Personendaten muss unter dem Gesichtspunkt der Verhältnismässigkeit geprüft werden. Personalisierte Lösungen werden eingesetzt, um dem Kunden ein massgeschneidertes Angebot zu liefern. Die Datensammlung rechtfertigt sich im Sinne einer **optimalen Kundenbetreuung**. Die Erstellung von Persönlichkeitsprofilen kann jedoch einen schwerwiegenden Eingriff in die Persönlichkeit der betroffenen Person darstellen. Der Unternehmer muss abwägen, welche Daten zu einer optimalen Kundenbetreuung wirklich notwendig sind und welche Daten dafür nicht gesammelt und bearbeitet werden müssen.

Zweckgebundenheit

Personendaten dürfen nur zu dem Zweck bearbeitet werden, der bei der Beschaffung angegeben wurde, aus den Umständen ersichtlich oder gesetzlich vorgesehen ist (Art. 4 Abs. 3 DSG).

Verlangt wird eine **klare Zweckumschreibung.** Eine nachträgliche Zweckänderung darf nur mit Zustimmung des Betroffenen vorgenommen werden. In zeitlicher Hinsicht verlangt das Prinzip der Zweckgebundenheit, dass nicht mehr benötigte Daten gelöscht werden. Zudem verstossen auf Vorrat angelegte Datensammlungen ohne Zweckbestimmung gegen das Prinzip der Zweckgebundenheit.

Bedeutung für personalisierte E-Commerce-Lösungen: Ob eine Datenbearbeitung zweckgebunden erfolgt, ist wie bei der Prüfung der Verhältnismässigkeit im Einzelfall zu beurteilen. Dem Nutzer eines E-Shops sollte im Allgemeinen bekannt sein, dass er Datenspuren hinterlässt und dass diese Spuren zur optimalen Kundenbetreuung ausgewertet werden. Jedoch ist der Umfang der bearbeiteten Daten meist viel grösser, als der Kunde das erwarten muss.

Obwohl der Zweck der Bearbeitung im Einzelfall aus den Umständen ersichtlich ist, empfiehlt es sich auf jeden Fall, umfassend über den Zweck der Bearbeitung zu informieren.

Überlegen Sie vor dem Anlegen der Datensammlung, zu welchem Zweck Sie die Personendaten verwenden möchten und orientieren Sie den Kunden darüber. Eine Verwendung der Personendaten, die vom ursprünglichen Zweck abweicht, z.B. die Weitergabe an Dritte, benötigt eine erneute Einholung der Einwilligung der betroffenen Person.

Überprüfung der Richtigkeit der Daten

Wer Personendaten bearbeitet, hat sich über deren Richtigkeit zu vergewissern. Betroffene Personen können zudem die Berichtigung unrichtiger Daten verlangen (Art. 5 DSG). Die Richtigkeit der gesammelten Daten ist für den Erfolg der Personalisierung von entscheidender Bedeutung.

Bekanntgabe ins Ausland (Art. 6 DSG)

Personendaten dürfen nicht ins Ausland bekannt gegeben werden, wenn dadurch die Persönlichkeit der betroffenen Personen schwerwiegend gefährdet würde, namentlich weil ein Datenschutz fehlt, der dem schweizerischen gleichwertig ist (Prinzip der Gleichwertigkeit in Art. 6 Abs. 1 DSG). Wer Datensammlungen ins Ausland übermitteln will, muss dies zudem gemäss Art. 6 Abs. 2 DSG dem Eidgenössischen Datenschutzbeauftragten (EDSB) melden. Nicht gemeldet werden muss die Bekanntgabe, wenn dafür eine gesetzliche Pflicht besteht oder wenn die betroffene Person Kenntnis von der Bekanntgabe ins Ausland hat.

Das Prinzip der Gleichwertigkeit kommt für die Bekanntgabe von Personendaten in vielen Staaten einem generellen Verbot gleich. In solchen Fällen ist die Bekanntgabe jeweils nur mit der Einwilligung der betroffenen Person möglich (vgl. auch Kap. 3, Fragestellung 3, S. 17).

Die Veröffentlichung der Mitarbeiterangaben im eigenen Internetauftritt stellt ebenfalls eine Bekanntgabe ins Ausland dar. Dazu braucht es die umfassende Einwilligung der Mitarbeitenden.

Weitere Informationen zur Bekanntgabe von Personendaten ins Ausland:

Themenseite des EDSB
www.edsb.ch/d/themen/ausland/index.htm

Unverbindliche Liste der Staaten, die über eine gleichwertige Datenschutzgesetzgebung verfügen
www.edsb.ch/d/themen/ausland/liste_d.pdf

Meldeformular des EDSB
www.edsb.ch/d/themen/ausland/anmaus-d.doc

Datensicherheit

Personendaten müssen durch angemessene technische und organisatorische Massnahmen gegen unbefugtes Bearbeiten geschützt werden (Art. 7 DSG). Ziel ist es, die Vertraulichkeit, die Integrität und die Verfügbarkeit der Daten zu schützen. Gerade die unverschlüsselte Übermittlung von Personendaten per E-Mail gibt keine Gewähr für die Vertraulichkeit und Integrität der Daten (vgl. auch Kap. 3, Fragestellung 3, S. 17).

Weiterführende Informationen zur Datensicherheit:

Themenseite des EDSB
www.edsb.ch/d/themen/sicherheit/index.htm

Leitfaden des EDSB zu den technischen und organisatorischen Massnahmen des Datenschutzes
www.edsb.ch/d/doku/leitfaeden/tom/tom.pdf

2.4 Weitere datenschutzrechtliche Pflichten

Das DSG enthält weitere Pflichten des Bearbeitenden, deren Nichtbeachtung strafrechtlich sanktioniert werden. Es handelt sich um die Auskunftspflicht, die Meldepflicht und um Mitwirkungspflichten gegenüber dem EDSB.

Auskunftspflicht

Gemäss Art. 8 DSG kann jede Person vom Inhaber einer Datensammlung Auskunft darüber verlangen, ob und welche Daten über sie bearbeitet werden. Der Bearbeitende muss über das Vorhandensein, den Inhalt, den Zweck der Bearbeitung, die Rechtsgrundlage, die Kategorie der bearbeiteten Personendaten, die Beteiligten an der Datensammlung und den Kreis der Datenempfänger im Falle der Weitergabe von Daten Auskunft geben. Dem Auskunftsberechtigten kommt das Recht zu, seine Angaben **berichtigen, löschen** oder **für die Weitergabe an Dritte sperren** zu lassen. Die Auskunft ist grundsätzlich **schriftlich**, in Form eines Ausdrucks oder einer Fotokopie, sowie **kostenlos** zu erteilen. Die auskunftsberechtigte Person hat sich über ihre Identität auszuweisen. In gewissen Fällen kann die Auskunft eingeschränkt oder verweigert werden (Art. 9 DSG). Dies muss dem Gesuchssteller in einem begründeten Entscheid mitgeteilt werden.

Bedeutung für personalisierte E-Commerce-Lösungen: Der Inhaber der Personendatensammlung muss organisatorische und verfahrensmässige Voraussetzungen schaffen, damit die betroffene Person Einsicht in ihre Personendaten nehmen kann. Die Datenbank ist so aufzubauen, dass auf Wunsch alle über die betroffene Person

gespeicherten Daten ohne grossen Aufwand gelöscht, berichtigt oder für die Weitergabe an Dritte gesperrt werden können.

Meldepflicht

Der EDSB führt ein Register der gemeldeten Datensammlungen, in das jede Person einsehen kann (Art. 11 DSG). **Von natürlichen Personen und Unternehmungen nicht angemeldet werden müssen Datensammlungen, die von Gesetzes wegen zu führen sind, Datensammlungen, von denen Betroffene Kenntnis haben und Sammlungen gewöhnlicher Personendaten, die nicht weitergegeben werden.**

Bedeutung für personalisierte E-Commerce-Lösungen: Datensammlungen, die Persönlichkeitsprofile beinhalten, müssen grundsätzlich dem EDSB gemeldet werden. Der Meldepflicht kann man entgehen, indem man die betroffenen Personen ausführlich über die Datenbearbeitung informiert.

2.5 Revision der Datenschutzgesetzgebung

Zu den wesentlichen Neuerungen der laufenden Revision gehören

- eine erhöhte Transparenz bei der Erhebung von besonders sensiblen Daten und Persönlichkeitsprofilen durch aktive Information der Betroffenen,
- eine Neuregelung der grenzüberschreitenden Datenübermittlung,
- die Förderung der Selbstregulierung durch Zertifizierung,
- die Einschränkung und der gleichzeitige Ausbau der Meldepflicht von Datensammlungen sowie
- eine Verschärfung des Rechts der betroffenen Person, die Bearbeitung von Personendaten zu untersagen.

Erhöhte, aktive Informationspflicht

Für E-Shop-Betreiber ist die **erhöhte, aktive Informationspflicht gegenüber den Besuchern und Kunden** von grosser Bedeutung. Die betroffene Person muss **aktiv** mindestens über die Identität des Inhabers der Datensammlung, über den Zweck der Datenbearbeitung und über die Kategorien der allfälligen Datenempfänger informiert werden. Erfordert es der Grundsatz von Treu und Glauben, muss der Inhaber der Datensammlung indessen noch weitere Informationen liefern. Dieser Informationspflicht kann in den AGB und in einer Datenbearbeitungserklärung nachgekommen werden.

Um dem Prinzip der Transparenz das nötige Gewicht zu verleihen, sieht Art. 34 Abs. 1 des Entwurfes eine **strafrechtliche Verantwortung** bei der Missachtung der Informationspflicht vor.

Die Beschaffung und Bearbeitung von gewöhnlichen Personendaten (z.B. Name, Adresse) soll im Vergleich zu heute ebenfalls transparenter geschehen, jedoch den Datenbearbeitenden nicht so weit reichende Pflichten auferlegen, wie bei der Bearbeitung von besonders schützenswerten Personendaten und Persönlichkeitsprofilen.

Der Entwurf beschränkt sich für gewöhnliche Personendaten auf den Grundsatz, dass die Beschaffung und insbesondere der Zweck der Bearbeitung erkennbar sein müssen.

Einschränkung und Ausbau der Meldepflicht von Datensammlungen

In Zukunft kann sich u.a. derjenige von der Meldepflicht befreien lassen, der sich erfolgreich einem Zertifizierungsverfahren unterzieht oder einen unabhängigen Datenschutzverantwortlichen ernennt, der die betriebsinterne Einhaltung der Datenschutzvorschriften überwacht und Verzeichnisse der Datensammlungen führt.

Beibehalten wird die Verpflichtung von Privatpersonen, die regelmässig besonders schützenswerte Personendaten oder Persönlichkeitsprofile bearbeiten oder regelmässig Personendaten an Dritte bekannt geben, ihre Datensammlungen beim Datenschutzbeauftragten anzumelden (Art. 11 DSG). **Entgegen den heutigen Bestimmungen soll dies auch dann gelten, wenn die betroffenen Personen über die Bearbeitung der besonders schützenswerten Personendaten, die Erstellung von Persönlichkeitsprofilen oder über die Bekanntgabe an Dritte informiert sind (Art. 11a Abs. 3 E-DSG). In diesem Punkt wird die Meldepflicht also stark ausgebaut.**

Mit dem Inkrafttreten der Revision kann in der zweiten Hälfte 2004 gerechnet werden. Für weiterführende Informationen:

www.bj.admin.ch/themen/datenschutz/bot-rev-d.pdf

2.6 Regelung in der Europäischen Union

In der EU wird der Datenschutz in mehreren Rechtsquellen geregelt.

Die **Allgemeine Datenschutzrichtlinie** (Richtlinie 95/46/EG des Europäischen Parlaments und des Rates vom 24. Oktober 1995 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten und zum freien Datenverkehr) hat einen wirksamen Datenschutz und parallel dazu die Erleichterung des Austausches personenbezogener Daten in der gesamten EU zum Ziel. Im Bereich der elektronischen Kommunikation gilt diese Richtlinie insbesondere für alle Fragen des Schutzes der Grundrechte und Grundfreiheiten. Die **Richtlinie 97/66/EG** des Europäischen Parlaments und des Rates vom 15. Dezember 1997 über die Verarbeitung personenbezogener Daten und den Schutz der Privatsphäre im Bereich der Telekommunikation befasst sich mit dem spezifischen Datenschutz im Fernmelderecht. Die Richtlinie wird auf den 31. Oktober 2003 aufgehoben. Bis zu diesem Zeitpunkt sind die Mitgliedstaaten verpflichtet, die **neue Datenschutzrichtlinie für elektronische Kommunikation** (Richtlinie 2002/58/EC des Europäischen Parlaments und des Rates vom 12. Juli 2002 über die Verarbeitung personenbezogener Daten und den Schutz der Privatsphäre in der elektronischen Kommunikation) in das jeweilige Landesrecht umzusetzen. Die neue Richtlinie berücksichtigt dabei die Entwicklungen der Märkte und Technologien für elektronische Kommunikationsdienste.

Die Richtlinie 2002/58/EC setzt Vorgaben bei der Betriebssicherheit (Art. 4), der Vertraulichkeit der Kommunikation (Art. 5), Verkehrsdaten und deren Verarbeitung

(Art. 6), der Rufnummernunterdrückung (Art. 8) und bei unerbetenen Nachrichten (Art. 13).

2.7 Internationale Instrumente, Softlaw und private Regulierungen

Um negative Auswüchse des Internets erfolgsversprechend bekämpfen zu können, braucht es internationale Regelungen, die von den einzelnen Staaten getragen und durchgesetzt werden. Das Übereinkommen des Europarates zum Schutz des Menschen bei der automatisierten Verarbeitung personenbezogener Daten vom 28. Januar 1981 (Konvention 108/81) ist in der Schweiz seit Februar 1998 in Kraft. Dieses Übereinkommen verpflichtet die Vertragsstaaten für jedermann sicherzustellen, dass sein Recht auf Achtung des Persönlichkeitsbereichs bei der automatischen Verarbeitung personenbezogener Daten geschützt wird.

Auch die OECD hat sich dieser Thematik angenommen. Die Leitlinie zur Sicherheit von Informationssystemen und die Leitlinie für den Schutz des Persönlichkeitsbereichs und den grenzüberschreitenden Verkehr personenbezogener Daten vom 23. September 1980 stellen jedoch nur Empfehlungen des OECD-Rates dar. Völkerrechtlich sind diese demnach unverbindlich. Dasselbe gilt für die UN-Richtlinie vom 14. Dezember 1990.

Internationale Bemühungen, die Bearbeitung von Personendaten im elektronischen Geschäftsverkehr transparenter zu gestalten sind auch der Datenschutzerklärungsgenerator der OECD und die „Platform for Privacy Preferences (P3P) 1.0“ des World Wide Web Consortium (W3C).

Quellen und weiterführende Informationen:

OECD-Leitlinie für den Schutz des Persönlichkeitsbereichs
http://europa.eu.int/comm/internal_market/privacy/instruments/ocdeguideline_en.htm

OECD-Leitlinie zur Sicherheit von Informationssystemen
www.oecd.org/pdf/M00034000/M00034292.pdf

UN-Richtlinie vom 14. Dezember 1990
http://europa.eu.int/comm/internal_market/privacy/instruments/un_en.htm

Datenschutzgenerator
http://cs3-hq.oecd.org/scripts/pwv3/pwhome.htm

„Platform for Privacy Preferences (P3P) 1.0“
www.w3.org/P3P/

3 Fragestellungen aus rechtlicher Sicht analysiert

Fragestellung 1: Welche Personendaten dürfen bearbeitet (insbesondere beschafft, gespeichert und ausgewertet) werden?

Grundsätzlich dürfen alle Personendaten, egal ob einfache Daten wie Adressangaben oder besonders schützenswerte Daten oder Persönlichkeitsprofile gesammelt und bearbeitet werden. Um eine missbräuchliche Handhabung zu verhindern, müssen jedoch gewisse Prinzipien und Vorschriften beachtet werden:

Personendaten dürfen nur dann bearbeitet werden, *wenn diese rechtmässig beschafft wurden, die Bearbeitung zweck- und verhältnismässig ist und nicht gegen Treu und Glauben verstösst (vgl. Kap. 2.3, S. 8 ff.). Die Daten müssen durch angemessene technische und organisatorische Massnahmen gegen unbefugtes Bearbeiten geschützt werden (vgl. Kap. 3, Fragestellung 3, S. 17). Besonders schützenswerte Personendaten oder Persönlichkeitsprofile dürfen nicht ohne Einwilligung Dritten bekannt gegeben werden.* Speziell reglementiert wird zudem die *Bekanntgabe von Personendaten ins Ausland (vgl. Kap. 2.3, S. 10 und Kap. 3, Fragestellung 5, S. 20).* Nicht zuletzt zeichnet sich das im Datenschutzgesetz verwirklichte Grundrecht der informationellen Selbstbestimmung dadurch aus, dass der Betroffene *die Datenbearbeitung gänzlich verbieten darf*, es sei denn, es liege ein Rechtfertigungsgrund (überwiegendes privates oder öffentliches Interesse) vor.

Fragestellung 2: Der Hauptrechtfertigungsgrund einer Persönlichkeitsverletzung ist die Einwilligung der betroffenen Person. Auf welche Art und Weise ist die Einwilligung einzuholen?

Im DSG fehlt es an einer klaren Definition der Einwilligung. Auch über das Formerfordernis spricht sich das Gesetz nicht aus. Eine schriftliche Einwilligung in die Datenbearbeitung ist nicht notwendig. Diese kann auch stillschweigend, z.B. durch Eingabe der Personendaten in dafür vorgesehene Datenfelder, erfolgen. **Voraussetzung ist jedoch, dass die betroffene Person vorgängig wahrheitsgemäss und transparent über den Verwendungszweck (z.B. Personalisierung, Weitergabe an Dritte) der Personendaten aufgeklärt wird.**

Für personalisierte Lösungen bedeutet dies, dass über die Beschaffung, den Zweck und die Folgen der Datenbearbeitung aufgeklärt werden muss. Der Kunde ist in den AGB und in der Datenschutzerklärung darauf hinzuweisen, dass ihm Kaufempfehlungen gemacht werden, die auf seinen Daten basieren. Der Kunde ist darüber zu informieren, dass Kauf- und Gewohnheitsmuster sowie Kundenprofile erstellt werden. Auch auf die Gewinnung völlig neuer Informationen über die betroffene Person ist hinzuweisen. Zudem ist die Auswertungsmethode (z.B. Auswertung durch Data Mining) anzugeben.

Fehlen wichtige Angaben oder wird der Verwendungszweck zu unbestimmt beschrieben, kann keine rechtsgültige Einwilligung in die Datenbearbeitung angenommen werden.

Fragestellung 3: Wozu dient eine Datenbearbeitungserklärung und welche Angaben sollte sie enthalten?

Eine transparente Datenbearbeitungspolitik ist ein wesentliches Element für die Vertrauensbildung gegenüber den Benutzern einer Website. Transparenz erreicht man durch Information. Zeigen Sie Ihren Kunden auf, welche Personendaten zu welchen Zwecken beschafft und bearbeitet werden. Erstellen Sie dazu eine Datenbearbeitungserklärung und erklären Sie diese zum Bestandteil Ihrer AGB.

Durch diese Information kann zudem die Einwilligung zur zweckgebundenen Beschaffung und Bearbeitung der Personendaten eingeholt werden. Gemäss dem EDSB sollte die Datenbearbeitungserklärung mindestens über folgende Punkte informieren:

1. Welchen Rechtsbestimmungen untersteht die Datenbearbeitungspraxis des Anbieters?
2. Welche Personendaten werden gesammelt und zu welchen Zwecken?
3. Welche Daten werden an Dritte weitergegeben und für welche Zwecke?
4. Welche Wahlmöglichkeiten zur Bearbeitung seiner Daten stehen dem Benutzer zu?
5. Welche Rechte (insbesondere Auskunfts- und Berichtigungsrecht) hat der Benutzer?
6. Welche Stelle beantwortet Fragen über die Bearbeitung von Personendaten?
7. Welche Sicherheitsmassnahmen werden zum Schutz von Personendaten angewendet?

Die Datenbearbeitungserklärung ist auf der Website so zu platzieren, dass sie für den Benutzer leicht auffindbar ist. Demnach ist überall dort, wo Personendaten gesammelt werden (Bestellformular, Anmeldetalon, etc.), ein Link auf die Datenbearbeitungserklärung zu setzen.

Quellen und weiterführende Informationen:

Musterdatenbearbeitungserklärung
www.weblaw.ch/kompetenzzentrum/content/datenschutz.pdf

Umsetzungshilfe und Konkretisierungsvorschläge des Eidgenössischen Datenschutzbeauftragten
www.edsb.ch/d/themen/e-commerce/ecom_d.pdf

Fragestellung 4: Wie muss ich Personendaten sichern?

Das Gesetz verlangt den Einsatz **angemessener technischer und organisatorischer** Massnahmen um die **Vertraulichkeit**, **Integrität** und **Verfügbarkeit** der Personendaten zu sichern. Welche Massnahmen angemessen sind, überlässt der Gesetzgeber bewusst dem Anwender. Dieser hat aufgrund des Zwecks und des Umfanges der Datenbearbeitung sowie nach Prüfung möglicher Risiken für die betroffenen Personen und aufgrund des gegenwärtigen Standes der Technik über die einzusetzenden Mittel zu entscheiden.

Gemäss Art. 9 Abs. 1 VDSG hat der Inhaber einer Datensammlung unter Berücksichtigung des Verhältnismässigkeitsprinzips die technischen und organisatorischen Massnahmen anzuwenden, die geeignet sind, namentlich acht Kontrollzielen gerecht zu werden:

1. Zugangskontrolle: unbefugten Personen ist der Zugang zu den Einrichtungen, in denen Personendaten bearbeitet werden, zu verwehren;
2. Personendatenträgerkontrolle: unbefugten Personen ist das Lesen, Kopieren, Verändern oder Entfernen von Datenträgern zu verunmöglichen;
3. Transportkontrolle: bei der Bekanntgabe von Personendaten sowie beim Transport von Datenträgern ist zu verhindern, dass die Daten unbefugt gelesen, kopiert, verändert oder gelöscht werden können;
4. Bekanntgabekontrolle: Datenempfänger, denen Personendaten mittels Einrichtungen zur Datenübertragung bekannt gegeben werden, müssen identifiziert werden können;
5. Speicherkontrolle: unbefugte Eingabe in den Speicher sowie unbefugte Einsichtnahme, Veränderung oder Löschung gespeicherter Personendaten sind zu verhindern;
6. Benutzerkontrolle: die Benutzung von automatisierten Datenverarbeitungssystemen mittels Einrichtungen zur Datenübertragung durch unbefugte Personen ist zu verhindern;
7. Zugriffskontrolle: der Zugriff der berechtigten Personen ist auf diejenigen Personendaten zu beschränken, die sie für die Erfüllung ihrer Aufgabe benötigen;
8. Eingabekontrolle: in automatisierten Systemen muss nachträglich überprüft werden können, welche Personendaten zu welcher Zeit und von welcher Person eingegeben wurden.

Je sensibler Personendaten sind, desto besser sind sie zu schützen. Persönlichkeitsprofile stellen hochsensible Daten dar und müssen daher bestmöglichst gegen interne und externe Datensicherheitsrisiken (Viren- und Hackerangriffe) geschützt werden. Es ist ein ganzheitliches Sicherheitskonzept unter Berücksichtigung der vom Gesetzgeber vorgegebenen Kontrollziele zu erstellen. Für den elektronischen Geschäftsverkehr sind kryptographische Verfahren und, sofern möglich, Authentifizierungsverfahren anzuwenden. Der Schutz des eigenen Systems und der Personendatenbanken durch Einsatz von Firewalls, bedacht gewählten Passwörtern und physischen Zutrittsbarrieren ist eine notwendige Selbstverständlichkeit. Die Massnahmen sind periodisch zu überprüfen.

Fragestellung 5: Inwieweit dürfen Personendaten an Dritte bekannt gegeben werden (z.B. an Tochterunternehmen, unabhängige Vertriebsgesellschaften, Partnerunternehmen, ins Ausland, auf Internetportalen)?

Besonders schützenswerte Personendaten oder Persönlichkeitsprofile dürfen Dritten nicht ohne Rechtfertigungsgrund (insbesondere Einwilligung) bekannt gegeben werden (Art. 12 Abs. 2 lit. c DSG). Die Weitergabe von einfachen Personendaten ist hingegen grundsätzlich erlaubt. Es müssen jedoch die Datenschutzgrundsätze (vgl. Kap. 2.3, S. 8 ff.) beachtet werden.

Zu berücksichtigen sind vor allem das Prinzip der Zweckgebundenheit sowie das grundsätzliche Verbot der Weitergabe von besonders schützenswerten Personendaten oder Persönlichkeitsprofilen. Demnach dürfen Kundenprofile nicht ohne Einwilligung der betroffenen Person an Dritte weitergegeben werden.

Bei der Datenübermittlung ins Ausland ist die Meldepflicht und das Prinzip der Gleichwertigkeit von Art. 6 DSG zu beachten. Die Bekanntgabe von Personendaten ins Ausland ist grundsätzlich nur dann erlaubt, wenn im Empfängerstaat ein gleichwertiger Datenschutz wie in der Schweiz herrscht. Zur Bekanntgabe der Daten in einem Staat mit weniger weit reichendem Datenschutz als in der Schweiz braucht es auf alle Fälle die Einwilligung der betroffenen Person. Auch die Veröffentlichung von Personendaten im Internet (z.B. Mitarbeiterportrait) kommt einer Bekanntmachung an Dritte **im In- und Ausland** gleich. Daher braucht es auch hier die Zustimmung der betroffenen Person.

Die anstehende Revision des DSG legt neue Kriterien für eine rechtmässige grenzüberschreitende Datenübermittlung fest. So wird z.B. der Abschluss eines Datentransfer-Vertrags, der einen angemessenen Schutz im Ausland gewährleistet, gesetzlich als hinreichende Garantie angesehen (Art. 6 Abs. 2 lit. a E-DSG).

4 Fallstudie Tecnofil AG

Am Beispiel eines realen Unternehmens beschreibt dieses Kapitel, welche rechtlichen Besonderheiten bei der Gestaltung einer personalisierten Website zu beachten sind. Der konkrete Fall veranschaulicht viele der bisher beschriebenen Grundlagen im Anwendungszusammenhang. Viele der Aspekte unseres Fallbeispiels lassen sich auf Websites anderer Branchen übertragen.

Die Tecnofil AG in Suhr (AG) zählt zu den führenden Schweizer Herstellern von Industrie- und Komfortfiltern im B2B-Bereich. Rund 25 Mitarbeiter produzieren und vertreiben eine Produktpalette von 3'500 verschiedenen Luft- und Wasserfiltern. Die Vielzahl der Artikel resultiert aus den unterschiedlichen Einsatzgebieten, Filterklassen und Abmessungen. Die meisten Filter sind standardisiert, Tecnofil bietet aber auch individuelle Anfertigungen an.

Um ihren Kunden einen zusätzlichen Nutzen zu bieten, möchte die Tecnofil AG ihre Services um eine neue Website ergänzen. Mit diesem Angebot kann man nebst B2B neu auch B2C-Kunden ansprechen. Die Website soll Interessenten und Kunden nicht nur umfassende und aktuelle Informationen rund um das Thema Filter zur Verfügung stellen, sondern auch eine komfortable Online-Bestellmöglichkeit bieten. Personalisierungsfunktionen spielen auf dieser Website eine wichtige Rolle, um Komfort und Nutzen für den Kunden zu gewährleisten.

In den folgenden Ausführungen wird jeweils zunächst eine Fragestellung geschildert, die anschliessend aus juristischer Sicht analysiert und beantwortet wird. Der erste Teil der Analyse behandelt den Bereich, der allen Website-Besuchern zur Verfügung steht (dem „anonymen“ Benutzer). Der zweite Teil befasst sich mit dem geschlossenen Bereich der Website für registrierte, am System angemeldete Benutzer.

4.1 Informationen und Services für den anonymen Besucher (ohne Login)

Auf den allgemeinen Webseiten präsentiert die Tecnofil AG ihr Leistungsspektrum. Diese Seiten sind für jeden Besucher zugänglich. Die Tecnofil AG möchte wissen, welche dieser Seiten wie häufig besucht werden, in welcher Reihenfolge durch die Seiten navigiert wird und wie häufig auf vordefinierte Kategorien zugegriffen wird (Interaktionsprofil). Ist diese Art der „anonymen“ Logfile- und Clickstream-Analyse zulässig?

Der Jurist: Entscheidend ist die Frage, ob Rückschlüsse auf die Identität der Besucher möglich sind. Erst dann handelt es sich bei diesen Informationen um vom DSG geschützte Personendaten. Logfiles geben nebst Datum, Zeit, Aktion und Zugriffsobjekt auch den für den Zugriff verwendeten Rechner an. Diese Angaben alleine lassen noch nicht ohne weiteres auf die Identität des Nutzers schliessen und sind daher datenschutzrechtlich wenig problematisch. Unter Umständen kann jedoch eine Verknüpfung mit weiteren Informationen (z.B. Benutzercodes) zur Identifizierung führen. Durch einen „Clickstream“ legen Browser und Betriebssystem ebenfalls zusätzliche Informationen offen.

Ein anonyme Analyse ist unter den Gesichtspunkten der Datenschutzgesetzgebung zulässig. Sind Querbezüge zur Identität durch weitere Informationen möglich, so ist

das dem Besucher trotz unpersönlicher Auswertung in der Datenschutzerklärung anzuzeigen.

Es wäre prinzipiell möglich, eine IP-Adresse auf einen bestimmten Kunden zurückzuführen (in dem Moment, wo sich dieser einloggt). Würde sich die Rechtslage ändern, wenn die Tecnofil AG beginnen würde, ein Verzeichnis über ihre registrierten User und deren IP-Adressen anzulegen?

Der Jurist: Ja. Dieses Verzeichnis ermöglicht die Verknüpfung der Logfiles-Daten mit den vorhandenen Userdaten. Für eine personenbezogene Auswertung muss die Einwilligung der betroffenen Person vorliegen. Diese ist über die Beschaffung, den Zweck und die Folgen der Datenbearbeitung aufzuklären.

Die Besucher der Website sollen die Möglichkeit haben, ihre Meinung kundzutun und ihre Erfahrungen mit Dienstleistungen und Produkten zu schildern. Dabei können sie freiwillige Angaben zu ihrer Person machen (z.B. „Beitrag von Hans Muster aus Sursee"). Diese Meinungsäusserungen sollen anschliessend allen interessierten Besuchern zur Verfügung stehen. Aus rechtlicher Sicht interessiert hier besonders die Frage, wer für falsche Äusserungen haftet oder für Fehlentscheidungen, die aufgrund dieser Äusserungen getroffen werden (z.B. bei Tipps zum idealen Wechselzeitpunkt eines Filters)?

Der Jurist: In Frage kommt eine zivilrechtliche und strafrechtliche Verantwortlichkeit. Zudem ist zu klären, wer haftbar ist: der Autor oder der Website-Betreiber.

Zivilrechtlich: Auch für freiwillig gemachte Empfehlungen, wie Tipps zum idealen Wechselzeitpunkt des Filters, kann man potenziell haftbar gemacht werden.

Der Rat und die Empfehlungen haben den Ansprüchen zu genügen, welche der Leser vernünftigerweise stellen darf. Ist ein schützenswertes Vertrauen des Lesers in die Auskunft entstanden, so haftet der Empfehlende für eine angemessene Sorgfalt bei seinen Äusserungen (Vertrauenshaftung). Entscheidend sind die Umstände des Einzelfalles.

Im vorliegenden Fall handelt es sich um ein Forum, in dem Meinungen und Erfahrungen von Anwendern ausgetauscht werden. Der Äussernde muss sich dabei nicht zu erkennen geben. Die Ansprüche, die der Leser an solche Aussagen vernünftigerweise haben kann, sind nicht hoch. Ein schützenswertes Vertrauen in Aussagen, die in anonymen Foren gemacht werden, ist eher nicht anzunehmen. Die Tecnofil AG stellt das Forum zur Verfügung, das die Nutzer zur Äusserung ihrer Meinung benutzen können. Tecnofil hat soweit zumutbar dafür zu sorgen, dass unrichtige Aussagen nicht über ihre Plattform verbreitet werden.

Strafrechtliche Verantwortlichkeit: Bei der in diesem Fall eher untypischen aber vorstellbaren strafbaren Veröffentlichung (rassistische Informationen, ehrverletzende Aussagen, etc.) in „Medien", wozu auch das Internet (inklusive Foren) zählt, ist zunächst nur der Autor belangbar. Wenn dieser nicht ermittelt oder in der Schweiz vor Gericht gestellt werden kann, dann kann der Redaktor und in letzter Linie „die für die Veröffentlichung verantwortliche Person" (Art. 27 StGB) belangt werden. Da die Äusserungen im anonymen Bereich erfolgen, ist es durchaus möglich, dass die strafrechtliche Verantwortlichkeit auf die verantwortliche Person der Tecnofil AG zurück-

fällt. Im Hinblick auf das Gesagte muss der Tecnofil AG geraten werden, die Inhalte nicht ohne vorgängige Prüfung freizuschalten.

Exkurs 1: Die Frage nach der Strafbarkeit von Access- und Hosting-Providern für strafrechtlich relevante Inhalte auf Internetseiten ist in der Schweiz sehr umstritten. Provider gelten dann strafrechtlich als Gehilfen, wenn sie von den rechtswidrigen Inhalten wissen oder darauf aufmerksam gemacht wurden und die Inhalte nicht sperren oder entfernen.

Exkurs 2: Für Diskussionsforen sollten jeweils „Benimmregeln" erstellt werden: Schreiben Sie nie etwas, was Sie dem Adressaten nicht auch vor anderen Leuten direkt mitteilen würden. Täuschen Sie nicht Fachwissen vor. Missbrauchen Sie das Forum nicht als Werbeplattform für Ihre Zwecke oder zum Vorteil eines andern. Behalten Sie sich vor, bei Verstössen die betreffenden Beiträge zu löschen.

Auf der Website sollen auch Daten Dritter (externe Daten), also Daten von Content-Anbietern angeboten werden. Dazu zählen z.B. Informationen zu Umweltschutz und Normen. Was ist bei dieser Art des „Re-Publishing" zu beachten?

Der Jurist: Veröffentlicht die Tecnofil AG Informationen auf der Website, die sie von Dritten erhalten hat, sind die Grundsätze für die Haftung für richtige Auskunft oder Rat zu berücksichtigen: Die Tecnofil AG hat aufgrund ihrer Verkehrssicherungspflicht und ihrer Fachkunde soweit als zumutbar dafür zu sorgen, dass die Informationen, die sie Dritten auf ihrer Website zugänglich macht, korrekt sind.

Praktisch ist das Anbringen eines Warnschildes (Disclaimer), in dem mitgeteilt wird, dass sich die Informationen und Meinungen nicht mit den Ansichten von Tecnofil decken müssen, dass die Beiträge vollumfänglich in der Verantwortung der Verfasser liegen und dass keine Gewähr hinsichtlich Vollständigkeit und Richtigkeit der Beiträge übernommen werden kann. Die juristische Verbindlichkeit von Disclaimern (Enthaftungsklauseln) ist jedoch umstritten.

Es empfiehlt sich bei den zur Verfügung gestellten Informationen (z.B. zu Umweltnormen) jeweils die Quelle sowie das Datum der Online-Schaltung anzugeben. Bei der Übernahme fremder Texte sind jeweils auch die Urheberrechte zu prüfen.

4.2 Informationen und Services für den registrierten Besucher (nach einem erfolgten Login)

Für die B2B-Kunden der Tecnofil AG wird die Eingabe der Kundendaten ins System von den internen Mitarbeitern übernommen. Das Kundenprofil steht anschliessend auch im E-Shop zur Verfügung. Die Zahlung erfolgt über Rechnungsstellung auf dem Postweg.

Mit dem neuen E-Shop will die Tecnofil *Neukunden* (neu auch B2C) die Möglichkeit bieten, sich selbst als Kunden zu registrieren. Meldet sich ein Besucher auf der Website an, werden in einem *Identifikationsprofil* persönliche Daten von ihm erfasst und gespeichert. Dazu zählen z.B. Name, Liefer-/Rechnungsadresse und Zahlungsinformationen (neu auch Kreditkarteninformationen). Der Kunde kann freiwillig Präferenzen zu Produktkategorien, zur Zahlungsweise, Lieferart, etc. eingeben (*Präferenzprofil*). Die eingestellten Präferenzen werden benutzt, um dem Kunden Empfehlungen zu den gewählten Produktkategorien zu geben und den Bestellprozess zu erleichtern.

Welche Massnahmen sind zu treffen, damit Speicherung und Nutzung dieser persönlichen Daten rechtlich unproblematisch sind?

Der Jurist: Die Beschaffung der Identifikations- und Präferenzdaten sind im geschilderten Fall datenschutzrechtlich unproblematisch. Die betroffenen Personen geben die Daten bewusst selber und freiwillig ein. Bei den Präferenzdaten haben die Personen sogar die Wahl, ob sie Angaben machen möchten oder nicht. Wichtig ist, dass dem Neukunden angezeigt wird, zu welchem Zweck die Personendaten gesammelt werden. Der Neukunde ist demnach in der Datenschutzerklärung dahingehend aufzuklären, dass die eingestellten Präferenzen benutzt werden, um ihm Empfehlungen zu den gewählten Produktkategorien zu machen und den Bestellprozess zu erleichtern. Die Personendaten dürfen danach auch nur zu diesen Zwecken genutzt werden (Prinzip der Zweckgebundenheit).

Datensicherheit: Das Gesetz verlangt den Einsatz angemessener technischer und organisatorischer Massnahmen gegen unbefugtes Bearbeiten. Je sensibler Personendaten sind, desto besser sind sie zu schützen. Die gesammelten Identifikations- und Präferenzangaben, vor allem auch die Kreditkarteninformationen, stellen sensible Daten dar. Die Daten sind in sicheren Datenbanken gegen unbefugte interne und externe Zugriffe (Viren und Hackerangriffe) zu schützen. Die Übertragung der Informationen hat verschlüsselt zu erfolgen. Der Schutz des eigenen Systems und der Personendatenbanken durch Einsatz von Firewalls, bedacht gewählten Passwörtern und physischen Zutrittsbarrieren ist ein Muss (vgl. auch Kap. 3, Fragestellung 3, S. 17).

Der angemeldete Besucher hat die Möglichkeit, Website, Produkte und Dienstleistungen von Tecnofil zu beschreiben und zu bewerten. Dazu kann er seine Meinungen und Erfahrungen in einem Freitextfeld formulieren (sog. Rezension). Die Rezensionen stehen anschliessend allen Besuchern der Website offen. Ist die Veröffentlichung dieser Rezensionen mit dem Namen des Autors auf der Website zulässig? Wer haftet für die Äusserungen?

Der Jurist: Für die Haftung für falsche Äusserungen kann auf das in Abschnitt 4.1 Gesagte verwiesen werden. Es stellt sich auch hier wiederum die Frage, wie viel Vertrauen man in solche Rezensionen vernünftigerweise haben kann. Die Gefahr einer Haftung der sich äussernden Person ist nicht auszuschliessen, sie ist jedoch eher klein. Bei Empfehlungen von Fachpersonen (Filterhersteller, Tecnofil AG), die sich auch als solche zu erkennen geben, ist eine Vertrauenshaftung eher anzunehmen.

Der Kunde ist zu informieren, dass seine Rezension auf der Website publiziert wird. Wenn dabei der Name des Autors angegeben werden soll, dann ist dies dem Verfasser auch im Vornherein anzuzeigen und damit seine Einwilligung einzuholen. Aufgrund der vielfältigen Möglichkeiten des Internets (Suchmaschinen) ist es einfach, Informationen über eine Person zu sammeln und diese danach zu Persönlichkeitsprofilen zu verknüpfen. Zu diesen Informationen gehören auch personalisierte Beiträge in Diskussionsforen.

Neben den bereits erwähnten *expliziten* Profilen (Identifikationsprofil, Präferenzprofil), die der Benutzer der Website bewusst zur Kenntnis gibt und sogar selbst eingibt, werden auch *implizite* Profile aufgezeichnet (Interaktionsprofil, Transaktionsprofil). Über deren Aufzeichnung ist sich der Benutzer oft nicht unmittelbar bewusst. Die In-

teraktionsprofile beinhalten Informationen über Zugriffe auf Webseiten und damit auch indirekt über das Interesse an bestimmten Produktkategorien (Metadaten) und können dazu benutzt werden, die Interessen des Benutzers abzuleiten. Dies gilt auch für die Daten aus bereits getätigten Transaktionen (Käufen). Was ist bei der Aufzeichnung derartiger impliziter Profile zu beachten?

Der Jurist: Die Beschaffung solcher Daten darf nicht gegen die datenschutzrechtlichen Grundsätze verstossen. Das heisst vor allem, dass dies nicht im Geheimen geschehen darf. Verlangt wird Transparenz. Die betroffene Person ist über die Art der Beschaffung, den Zweck und die Folgen der Datenbearbeitung aufzuklären.

Die Aufzeichnung dieser impliziten Daten führt zu einer Zusammenstellung von Daten, die eine Beurteilung wesentlicher Aspekte der Persönlichkeit einer natürlichen Person erlauben. Die Weitergabe solcher Persönlichkeitsprofile an Dritte ohne Einwilligung der betroffenen Person stellt eine Persönlichkeitsverletzung dar.

Die Tecnofil möchte ihre impliziten Profile für die Personalisierung ihrer Website und somit zum Nutzen des Kunden einsetzen. Die Daten aus dem *Transaktionsprofil* werden dazu wie folgt verwendet:

1. Der registrierte Nutzer kann seine in der Vergangenheit getätigten Bestellungen einsehen (Bestellhistorie).
2. Dem registrierten Benutzer werden auf der Basis anonymisierter Verkaufsdaten anderer Kunden Produktvorschläge unterbreitet.
3. Allen Benutzern, also auch den anonymen, stehen anonymisierte Auswertungen (z.B. über Produktgruppen, Regionen) über getätigte Käufe zur Verfügung.

Der Jurist: Die Möglichkeit der Einsichtnahme in die Bestellhistorie ist sinnvoll. Es sind angemessene Massnahmen zur Sicherstellung der Vertraulichkeit und Integrität der Bestellhistorie zu treffen.

Die Publikation von anonymisierten Auswertungen über getätigte Käufe ist an sich unproblematisch. In Einzelfällen, z.B. wenn es nur einen oder sehr wenige und bekannte Käufer in der Region gibt, sind jedoch Rückschlüsse auf die Käufer möglich. Dasselbe gilt für Produktvorschläge, die auf anonymisierten Verkaufsdaten anderer Kunden beruhen.

Tecnofil wertet das *Interaktionsprofil* (Clickstream) der Benutzer aus und zeigt Links auf häufig angesehene Produkte bereits auf der ersten Seite nach dem Login an („ihre bevorzugten Produkte“). Kunden, die bestimmte Produkte mehrfach ansehen aber nicht kaufen, werden in einem Mailing nach den Gründen gefragt („Helfen Sie uns, das richtige Angebot für Sie zu finden“).

Der Jurist: Der Benutzer ist über dieses Vorgehen in der Datenschutzerklärung zu informieren.

Die Versendung eines Mailings (Briefpost, E-Mail) an den Kunden ist auch ohne vorgängige Orientierung grundsätzlich erlaubt, da schon eine Kundenbeziehung besteht. Der Kunde kann jedoch verlangen, dass ihm solche E-Mails nicht mehr zugestellt werden. Hält sich die Tecnofil AG nicht daran, so verstösst sie gegen die Persönlichkeitsrechte des Kunden. Bei (unverschlüsselten) E-Mail-Sendungen ist zudem zu be-

achten, dass die Vertraulichkeit nicht gewährleistet werden kann. Das ist dem Kunden ebenfalls mitzuteilen.

Für neue Kunden, die bisher noch keine Tecnofil-Filter einsetzen, gibt es einen *„Filterübersetzer“*. Dieser besteht aus einer Tabelle, in der baugleiche Filter anderer Hersteller in Tecnofil-Filter übersetzt werden. Die Tabelle unterstützt Kunden dabei, von ihren bisher eingesetzten Filtern auf Tecnofil-Filter umzusteigen.

Der Jurist: Dieser Übersetzer ist sicherlich ein hilfreiches Instrument.

Probleme stellen sich bei Fehlbestellungen, die aufgrund des (ungeeigneten) Vorschlages des Filterübersetzers gemacht wurden. Die Software oder die eingelesenen Daten können fehlerbehaftet sein und zu falschen Resultaten führen. Demnach ist darauf hinzuweisen, dass keine Gewähr für die Richtigkeit des Resultates übernommen werden kann. Der Kunde soll sich im Zweifelsfall telefonisch oder persönlich beraten lassen.

Bei Vergleichen mit Konkurrenzprodukten ist jeweils auch zu prüfen, ob die Gegenüberstellung nicht unlauter ist. Unlauter handelt insbesondere, wer sich, seine Waren, Werke, Leistungen oder deren Preise in unrichtiger, irreführender, unnötig herabsetzender oder anlehnender Weise mit anderen, ihren Waren, Werken, Leistungen oder deren Preisen vergleicht (Art. 3 lit. e UWG).

Falls der Filterübersetzer auch die jeweiligen Preise vergleichen würde, müssten die tatsächlichen und aktuellen Preise beigezogen werden.

Zum Ende dieses Fallbeispiels weisen wir darauf hin, dass die hier durchgeführte Analyse nicht eins zu eins auf andere Anwendungen übertragen werden kann. Im Einzelfall ist eine individuelle juristische Analyse nötig, um die Gesetzeskonformität einer Website sicherzustellen.

5 Bibliographie

Wichtige Referenzen, weiterführende Literatur

Robert G. Briner, Verträge und Haftung im Internet, Was der Praktiker im globalen Umfeld wissen muss, Zürich 2002.

Leonardo Cereghetti, Disclaimer und Haftungsfreizeichnungen im E-Commerce, SIC 2002, S. 1 ff.

Perspektive Datenschutz, Praxis und Entwicklungen in Recht und Technik, Hrsg.: Bruno Baeriswyl, Beat Rudin, Zürich 2002.

Informatikrecht in der Praxis, Recht und Praxis rund um den Einsatz von Informatik- und Kommunikationsmitteln, regelmässig aufdatierte Loseblatt-Ausgabe, Hrsg.: Weblaw GmbH, 2001.

Alex Schweizer, Data Mining Data Warehousing, Datenschutzrechtliche Orientierungshilfen für Privatunternehmen, Zürich 1999.

Rolf H. Weber, E-Commerce und Recht, Rechtliche Rahmenbedingungen elektronischer Geschäftsformen, Zürich 2001.

Online-Quellen (weitere Quellenangaben finden sich im Text)

Systematische Sammlung des Bundesrechts
www.admin.ch/ch/d/sr/sr.html

Eidgenössischer Datenschutzbeauftragter
www.edsb.ch

Leitfaden für die Bearbeitung von Personendaten im privaten Bereich (EDSB)
www.edsb.ch/d/doku/leitfaeden/sammlungen/inhaber.pdf

Datenschutz und E-Commerce: Themenübersicht des EDSB
www.edsb.ch/d/themen/e-commerce/index.htm

Datenschutzseite der EU
http://europa.eu.int/comm/internal_market/privacy/index_de.htm

E-Commerce: Themenseite des Bundesamts für Justiz
www.bj.admin.ch/themen/e-commerce/intro-d.htm

Datenschutz im E-Commerce: Checkliste auf softnet-recht.ch
www.softnet-recht.ch/download/Checkliste_Datenschutz%20in%20E-Commerce1.pdf

Jusletter – Juristische Online Zeitschrift
www.jusletter.ch

Weblaw, Werkzeuge für die Recherche nach juristischen Informationen im Internet (juristische Datenbank, Lawsearch)
www.weblaw.ch

6 Impressum, Bezugsquellen, Wer hilft weiter?

Diese Broschüre entstand aus der Zusammenarbeit zwischen der Weblaw GmbH, Bern und der Fachhochschule beider Basel (FHBB). Die Studie wird herausgegeben vom Institut für angewandte Betriebsökonomie (IAB) an der Fachhochschule beider Basel (FHBB), Peter-Merian-Strasse 86, Postfach, CH-4002 Basel.

Die Broschüre liefert einen Überblick über rechtliche Rahmenbedingungen im E-Commerce. Die Inhalte basieren auf den zum Zeitpunkt der Drucklegung gültigen Gesetzen. Der Überblick versteht sich nicht als abschliessend. Er dient ausschliesslich zu Informationszwecken und darf nicht als verbindliche Rechtsauskunft aufgefasst werden. Die Broschüre ersetzt in keiner Weise eine juristische Beratung.

Redaktionsschluss: 13. Juni 2003

Die Broschüre kann online bei Weblaw oder bei der FHBB bestellt werden:

www.weblaw.ch/broschuere/bestellung.asp

www.e-business.fhbb.ch/broschuere-personalisierung

Kontakt

Weblaw GmbH
CyberSquare
Laupenstrasse 1
CH-3008 Bern
Telefon 031 398 80 47
Telefax 031 398 80 97
mathias.kummer@weblaw.ch

Fachhochschule beider Basel (FHBB)
Institut für angewandte Betriebsökonomie (IAB)
Peter Merian-Strasse 86, Postfach
CH-4002 Basel
Telefon 061 279 17 65
Telefax 061 279 17 98
uwe.leimstoll@fhbb.ch

Ihre Fragen zur juristischen Analyse richten Sie bitte an die Weblaw GmbH. Bei Fragen zu den Themen E-Commerce, Personalisierung und zum beschriebenen Fallbeispiel hilft die FHBB weiter.

Die Autoren danken der Tecnofil AG, Suhr (AG) und der Simultan AG, Altishofen (LU) für die offene Kooperation in diesem Projekt. Die Tecnofil AG ist im Internet unter www.tecnofil.ch zu erreichen, die Simultan AG unter www.simultan.ch.