

Datenschutz und E-Commerce

Wer im Internet surft, hinterlässt Spuren. Webserver speichern Angaben über Rechneradresse (IP), Datum, Zeit, durchgeführte Aktion usw. in Log-Files. Auch auf dem Computer des Nutzers platzierte Cookies generieren nützliche Informationen. Diese Daten werden oft zu Statistikzwecken ausgewertet. Alleine lassen die Angaben noch nicht ohne weiteres auf die Identität des Nutzers schliessen und sind daher datenschutzrechtlich wenig problematisch. Sobald der Anbieter jedoch weitere personenbezogene Daten über den Nutzer erhält – beispielsweise durch Angaben in Bestell- oder Anmeldefeldern – sind Verknüpfungen möglich, die zu umfangreichen Persönlichkeitsprofilen führen. Da die Daten elektronisch vorliegen, sind Verknüpfungen und Auswertungen durch Datenverarbeitungssysteme einfach.

Neue Technologien und Methoden ermöglichen es, kontinuierlich eine grosse Menge an Personendaten zu sammeln, zu ordnen und so auszuwerten, dass Ge-

Mathias Kummer

wohnheitsmuster (z.B. Kaufverhalten), künftige Trends und Kundenprofile erstellt werden können. Die Auswertungsmethoden des Data Mining erzeugen sogar persönliche Informationen, die zuvor noch gar nicht explizit vorhanden waren [1].

Solche Profile sind für Unternehmungen, die E-Commerce betreiben, von grossem Wert. Dem Besucher einer Website können Informationen angezeigt werden, die speziell auf seine Bedürfnisse und Interessen abgestimmt sind (so genannte Personalisierung im E-Commerce) [2]. Individuell massgeschneiderte Kaufempfehlungen, Rabatte und Werbung binden den Kunden an das Unternehmen. Durch gezielte Direktmarketingmassnahmen werden Neukunden

gewonnen. Das Konsumverhalten wird gezielt beeinflusst und gesteuert.

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 Privatsphäre 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 Bestimmungen. Weitere Massnahmen sind 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 Internetauftritts in so genannten Datenschutzaudits.

Vertrauensfördernde Massnahmen für den elektronischen Geschäftsverkehr

Einhaltung der datenschutzrechtlichen Grundsätze im Datenschutzgesetz

Den wirtschaftlichen Interessen des Anbieters steht der Schutz der Persönlichkeit der betroffenen Person gegenüber. Dieser wird durch das Bundesgesetz über den Datenschutz¹⁾ (DSG) gewährleistet. Für Online-Anbieter gilt: Nicht alles, was machbar ist, ist auch erlaubt.

Die Einhaltung der Datenbearbeitungsgrundsätze des schweizerischen Datenschutzgesetzes ist die erste, zwingende Voraussetzung der Vertrauensbildung. Personendaten dürfen nur dann bearbeitet werden, wenn diese rechtmässig beschafft wurden, die Bearbeitung zweck- und verhältnismässig ist und nicht gegen Treu und Glauben verstösst. Die Daten müssen durch angemessene technische und organisatorische Massnahmen gegen unbefugtes Bearbeiten geschützt werden.

Wer Personendaten bearbeitet, hat sich über deren Richtigkeit zu vergewissern. Private Personen, die regelmässig besonders schützenswerte Personendaten oder Persönlichkeitsprofile bearbeiten oder Personendaten an Dritte bekannt geben, müssen Sammlungen vor ihrer Eröffnung beim Eidgenössischen Datenschutzbeauftragten (EDSB)²⁾ registrieren. Die Rechte der Betroffenen (umfangreiches Auskunftsrecht, Recht auf Berichtigung, Sperrung bzw. Löschung der Personendaten) sind zu wahren. Besonders schützenswerte Personendaten oder Persönlichkeitsprofile dürfen nicht ohne Rechtfertigungsgrund (insbesondere nicht ohne Einwilligung) Dritten bekannt gegeben werden. Speziell reglementiert wird zudem die Bekanntgabe von Personendaten ins Ausland. Sie ist grundsätzlich nur dann erlaubt, wenn im Empfängerstaat ein gleichwertiger Datenschutz wie in der Schweiz herrscht. Zur Bekanntgabe der Daten in einen Staat mit weniger weit reichendem Datenschutz

braucht es auf alle Fälle die Einwilligung der betroffenen Person. 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, Gesetz) vor.

Treu und Glauben

Der Grundsatz von Treu und Glauben verlangt die transparente und lautere Beschaffung und Bearbeitung der Daten. Der Kunde ist über den Zweck der Bearbeitung zu orientieren.

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. 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 das Vermeiden unnötiger Daten.

Zweckgebundenheit

Personendaten dürfen nur zu dem Zweck bearbeitet werden, der bei der Beschaffung angegeben wurde, aus den Umständen ersichtlich oder gesetzlich vorgesehen ist. 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.

Es sollte daher vor dem Anlegen der Datensammlung überlegt werden, zu welchem Zweck die Personendaten verwendet werden sollen, und die betroffenen Personen sollten dementsprechend orientiert werden. Eine Verwendung der Personendaten, die vom ursprünglichen, kommunizierten Zweck abweicht – z.B. die Weitergabe an Dritte – benötigt ein erneutes (aufwändiges) Einholen der Einwilligung der betroffenen Person.

Transparenz bei der Datenbearbeitung

Eine transparente Datenbearbeitungspolitik ist ein weiteres wesentliches Element für die Vertrauensbildung gegenüber den Benutzern einer Website. Transparenz erreicht man durch Information. Den Kunden sollte aufgezeigt werden, welche Personendaten zu welchen Zwecken beschafft und bearbeitet werden. Dazu eignet sich eine Datenbearbeitungserklärung, die zum Bestandteil der Allgemeinen Geschäftsbedingungen (AGB) erklärt wird.

Durch diese Information wird die Einwilligung zur zweckgebundenen Beschaffung und Bearbeitung der Personendaten eingeholt.

Gemäss dem EDSB sollte die Datenbearbeitungserklärung mindestens über folgende Punkte informieren³⁾:

- Welchen Rechtsbestimmungen untersteht die Datenbearbeitungspraxis des Anbieters?
- Welche Personendaten werden gesammelt und zu welchem Zweck?
- Welche Daten werden an Dritte weitergegeben und zu welchem Zweck?
- Welche Wahlmöglichkeiten zur Bearbeitung seiner Daten stehen dem Benutzer zu?
- Welche Rechte (insbesondere Auskunfts- und Berichtigungsrecht) hat der Benutzer?
- Welche Stelle beantwortet Fragen über die Bearbeitung von Personendaten?
- 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 usw.), ein Link auf die Datenbearbeitungserklärung zu setzen.

Eine Musterdatenbearbeitungserklärung kann unter der Adresse <http://www.weblaw.ch/kompetenzzentrum/content/datenschutz.pdf> bezogen werden.

Wahlmöglichkeiten

Dem Nutzer sollte ein Wahlrecht hinsichtlich der Begrenzung der Nutzung und Weitergabe seiner Personendaten gegeben werden (z.B. bezüglich der möglichen Weitergabe zu Werbezwecken). Der Kunde soll nicht vor das Problem gestellt werden, dass er entweder bestellt und die Bearbeitung seiner Personendaten für Werbezwecke erlaubt oder auf die Bestellung verzichten muss.

Einsatz von Sicherheitstechnologien

Das Datenschutzgesetz 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 auf Grund des Zwecks und des Umfangs der Datenbearbeitung sowie nach Prüfung möglicher Risiken für die betroffenen Personen und auf Grund des gegenwärtigen Standes der Technik über die einzusetzenden Mittel zu entscheiden.

Je sensibler Personendaten sind, desto besser sind sie zu schützen. Für den elektronischen Geschäftsverkehr sind kryptografische Verfahren (Verschlüsselung, Hashing, digitale Signatur) 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.

Gütesiegel und Datenschutzaudits

Anbieter von Datenschutzaudits prüfen den Online-Auftritt von Website-Betreibern auf die Einhaltung der datenschutzrechtlichen Bearbeitungsgrundsätze. Entspricht der Auftritt dem geltenden Recht, so erhält der Website-Betreiber ein Gütesiegel und die Berechtigung, dieses gegen eine jährliche Gebühr und zeitlich limitiert auf seiner Site zu publizieren. Der Website-Betreiber soll mit seiner datenschutzgerechten Datenbearbeitungspolitik Werbung machen können.

In der Schweiz existieren im Moment noch keine etablierten Auditverfahren. Solange sich kein Standard durchsetzen kann, sind Gütesiegel noch nicht das erhoffte Marketinginstrument (eine Vorrolle spielt beispielsweise das Landeszentrum für Datenschutz Schleswig-Holstein in Deutschland⁴⁾). Die Kosten zur Erlangen solcher Siegel sind für KMU hoch, die Bekanntheit der Gütesiegel im Publikum ist jedoch eher klein. Zudem verzichten grosse Unternehmungen – die es sich finanziell leisten könnten – auf ein Gütesiegel, weil sie das Vertrauen ihrer Online-Kunden bereits gewonnen haben.

Die anstehende Revision des Datenschutzgesetzes sieht die Förderung der Selbstregulierung durch Zertifizierung vor. Um den Datenschutz und die Datensicherheit zu verbessern, können die Hersteller von Datenbearbeitungssystemen oder -programmen, aber auch private Personen oder Bundesbehörden, die Personendaten bearbeiten, ihre Systeme, Verfahren und ihre Organisation einer Bewertung durch anerkannte unabhängige Zertifizierungsstellen unterziehen.

Der Bundesrat erlässt Vorschriften über die Anerkennung von Zertifizierungsverfahren und die Einführung eines Datenschutz-Qualitätszeichens. Er berücksichtigt dabei das internationale Recht und die international anerkannten technischen Normen (Art. 11 Abs. 1 und 2 DSGVO-Revision).

Die Neulancierung der Idee stellt insbesondere für den E-Commerce eine grosse Chance dar. Wird diese Gesetzesbestimmung nicht noch vom Parlament gestrichen, und gelingt es danach dem Bundesrat, griffige Vorschriften über die Anerkennung von Zertifizierungsverfahren und die Einführung eines Datenschutz-Qualitätszeichens unter Berücksichtigung der international anerkannten Normen zu erlassen, so wird sich in Zukunft ein Standard mit Publikumswirkung bilden.

Das Gesetz sieht auch direkte Vorteile für zertifizierte Unternehmen vor. Diese würden nach Artikel 11a DSGVO-Revision für Datensammlungen von der allgemeinen Meldepflicht entbunden.

Internationale Bemühungen

Es bestehen auch internationale Bemühungen, die Bearbeitung von Personendaten im elektronischen Geschäftsverkehr transparenter zu gestalten. Resolutionen, Übereinkommen und Richtlinien von internationalen Organisationen tragen zur Harmonisierung der nationalen Datenschutzvorschriften bei⁵⁾. Auch die EU versucht in mehreren Richtlinien⁶⁾, eine Vereinheitlichung der Datenschutzgesetzgebung in den Mitgliedsstaaten zu erreichen.

Einen guten Überblick bietet die Datenschutzseite der EU, die unter der Adresse http://europa.eu.int/comm/internal_market/privacy/index_de.htm eingesehen werden kann.

Datenschutzerklärungsgenerator der OECD

Die OECD stellt interessierten Website-Betreibern einen Datenschutzerklärungsgenerator⁹⁾ zur Verfügung: In einem passwortgeschützten Bereich kann ein 11 Seiten umfassendes Formular in englischer Sprache ausgefüllt werden, in welchem alle Aspekte der datenschutzrechtlichen Bearbeitung von Personendaten befragt werden. Die generierten «privacy policies» können heruntergeladen werden.

Die OECD sieht den Datenschutzgenerator jedoch in erster Linie als Lerntool. Er soll dem Nutzer hilfreichen Input bei der Erstellung von Datenschutzerklärungen liefern bzw. aufzeigen, welche

Aspekte es bei der Datenbearbeitung zu beachten gilt. Die OECD übernimmt denn auch nicht die Gewähr, dass eine auf den Generator abgestützte Erklärung den nationalen Datenschutzbestimmungen und den OECD Privacy Guidelines entspricht.

P3P

Im Mai 2002 hat das World Wide Web Consortium (W3C) die Platform for Privacy Preferences (P3P) 1.0⁸⁾ als Recommendation (Empfehlung) im Bereich Datenschutz veröffentlicht. P3P soll den Schutz der Privatsphäre und die Sicherheit im Web verbessern. Bei P3P handelt es sich um ein automatisiertes Protokoll, das dem Internetbenutzer erlaubt, die von Internetseiten-Betreibern verarbeiteten personenbezogenen Daten besser zu kontrollieren.

Im Kern ist P3P eine standardisierte Liste von Multiple-Choice-Fragen, welche alle relevanten Aspekte einer Datenschutzerklärung im Web abdecken soll. Die Antworten ergeben zusammen eine computerlesbare Fassung der Datenschutz-Grundsätze einer Website. Für den Nutzer soll ersichtlich sein, welche Daten von einer Website zu welchem Zweck genutzt werden.

P3P-fähige Browser (z.B. Internet Explorer 6.0, Mozilla, privacy bird von AT&T) können die herausgefilterten Informationen interpretieren und automatisch mit den Präferenzen des Nutzers vergleichen. Die Kontrollmöglichkeiten des Nutzers werden verbessert, weil P3P die Datenschutzerklärung auffindbar und für den Nutzer verständlich macht.

Gemäss dem Dashboard⁹⁾ von Ernst & Young vom Oktober 2002 haben 18% der

500 meist besuchten Websites und 28% der Top-100-Websites (gemessen nach amerikanischen Nutzern) P3P implementiert. Zahlen aus Europa liegen nicht vor.

Eine Vorreiterrolle für P3P in Deutschland nimmt das Unabhängige Landeszentrum für Datenschutz von Schleswig-Holstein ein. Die Projektseite des Landeszentrums¹⁰⁾ enthält ausführliche Informationen zu P3P sowie Tipps und Tools für Internetnutzer und erklärt, wie Webanbieter eine P3P-Datenschutzerklärung implementieren können. Zudem unterhält sie eine umfassende Linkliste zu P3P.

Schlussfolgerung

Das Problem des fehlenden Vertrauens der Kundschaft in den E-Commerce ist erkannt. Datenschützer auf der ganzen Welt arbeiten an der Sensibilisierung von Website-Betreibern. Die Betreiber in der Schweiz sollten die ihnen zur Verfügung stehenden Möglichkeiten nutzen. Zentral ist eine transparente Datenbearbeitungspolitik, die Information und Aufklärung des Kunden, welche Personendaten zu welchem Zweck gesammelt werden, und die Gewährleistung der Datensicherheit. Mit dem Einhalten der gesetzlichen Datenbearbeitungsgrundsätze, dem Einsatz von angemessenen technischen und organisatorischen Massnahmen zum Schutz von Personendaten und der Publikation und Befolgung einer detaillierten Datenbearbeitungserklärung ist ein grosser Schritt zur Vertrauensgewinnung gemacht.

Protection des données et commerce électronique

En naviguant sur Internet, on laisse des traces. Les serveurs Web enregistrent dans des Log-Files des indications sur l'adresse de l'ordinateur (IP), la date, l'heure, les actions effectuées etc. Et les «cookies» placés sur l'ordinateur de l'utilisateur génèrent d'utiles informations. Ces données sont souvent utilisées à des fins de statistiques. A elles seules, elles ne permettent pas encore de conclure à l'identité de l'utilisateur et ne posent donc guère de problème au niveau de la protection des données. Mais dès qu'un fournisseur de services reçoit des données personnelles sur l'utilisateur – par exemple par les indications fournies dans les cas de commande ou d'inscription – des renvois sont possibles, à l'aide desquels on peut établir des profils complets de personnalité. Les données étant disponibles sous forme électronique, les raccourcis et évaluations par systèmes de traitement des données sont facilement réalisables.

Referenzen

- [1] A. Schweizer: Data Mining – Data Warehousing. Orell Füssli Verlag, 1999. ISBN 3-280-02540-0
- [2] FHBB/IAB, Weblaw GmbH: Rechtliche Implikationen der Personalisierung. Broschüre der Fachhochschule beider Basel und der Weblaw GmbH, 2003, Bestellung: <http://www.weblaw.ch/broschuere/bestellung.asp>

Weiterführende Literatur

- [3] Perspektive Datenschutz, Praxis und Entwicklungen in Recht und Technik, Hrsg: Bruno Baeriswyl, Beat Rudin, Zürich 2002. ISBN 3-7255-4329-1
- [4] Informatikrecht in der Praxis, Recht und Praxis rund um den Einsatz von Informatik- und Kommunikationsmitteln, regelmässig aufdatierte Loseblatt-Ausgabe, Hrsg: Weblaw GmbH, 2001.

- [5] R. H. Weber: E-Commerce und Recht, Rechtliche Rahmenbedingungen elektronischer Geschäftsformen, Zürich 2001. ISBN 3-7255-4171-X

Angaben zum Autor

Lic. iur. **Mathias Kummer** ist seit 2001 Geschäftsführer der Weblaw GmbH in Bern. Er unterrichtet an mehreren Informatikschulen im Bereich Internetrecht. Herr Kummer ist Initiant und Dozent des Abendseminars *Informatikrecht für die Praxis* und Autor der gleichnamigen, vierteljährlich aktualisierten Loseblattsammlung für Praktiker. Zudem ist er Mitautor der Broschüre *Rechtliche Implikationen der Personalisierung* (2003).
Weblaw GmbH, 3008 Bern,
mathias.kummer@weblaw.ch

¹ Bundesgesetz über den Datenschutz (DSG) vom 19. Juni 1992, SR 235.1.

² www.edsb.ch

³ Umsetzungshilfe und Konkretisierungsvorschläge des Eidgenössischen Datenschutzbeauftragten http://www.edsb.ch/d/themen/e-commerce/ecom_d.pdf

⁴ <http://www.datenschutzzentrum.de>

⁵ Beispielsweise das Übereinkommen Nr. 108 des Europarats zum Schutz des Menschen bei der automatischen Verarbeitung personenbezogener Daten oder die OECD-Leitlinien für den Schutz des Persönlichkeitsbereiches und den grenzüberschreitenden Verkehr personenbezogener Daten.

⁶ Insbesondere die Allgemeine Datenschutzrichtlinie (Richtlinie 95/46) und die Datenschutzrichtlinie für elektronische Kommunikation (Richtlinie 2002/58/EC).

⁷ <http://cs3-bq.oecd.org/scripts/pwv3/pwhome.htm>

⁸ P3P: Platform for Privacy Preferences Project. <http://www.w3.org/P3P/>

⁹ [http://www.ey.com/global/download.nsf/US/P3P_Dashboard_October_2002/\\$file/E&YP3PDashboardOctober2002.pdf](http://www.ey.com/global/download.nsf/US/P3P_Dashboard_October_2002/$file/E&YP3PDashboardOctober2002.pdf)

¹⁰ <http://www.datenschutzzentrum.de/projekte/p3p/index.htm>