

Datenschutz und E-Commerce (Einführung)

Wer im Internet surft, hinterlässt Spuren. Webserver speichern Angaben über Rechneradresse, Datum, Zeit, Aktion etc. in 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, die zu umfangreichen **Persönlichkeitsprofilen** der Nutzer führen, möglich. 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 personenbezogene Informationen, 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 Wachstumspotential 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 ausführlich 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).

Transparenz bei der Datenbearbeitung

Ein wesentliches Element für die Vertrauensbildung ist eine transparente Datenbearbeitungspolitik der Websitebetreiber gegenüber den Benutzern. 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.

Wahlmöglichkeiten

Geben Sie dem Benutzer ein Wahlrecht hinsichtlich der Begrenzung der Nutzung und Weitergabe von Personendaten (z.B. Erstellung von Persönlichkeitsprofilen, 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

Stellen Sie sicher, dass Kundendaten durch angemessene technische und organisatorische Massnahmen gegen unbefugte Zugriffe geschützt werden. 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 kryptografische 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.

Gütesiegel und Datenschutzaudits

Anbieter von Datenschutzaudits prüfen den Online-Auftritt von Website-Betreibern auf die Einhaltung der datenschutzrechtlichen Bearbeitungsgrundsätze. Entsprechen die Auftritte dem geltenden Recht, so erhält der Website-Betreiber ein Gütesiegel und die Berechtigung, dieses auf seiner Site gegen eine jährliche Gebühr und zeitlich limitiert zu publizieren. Der Websitebetreiber soll mit seiner datenschutzgerechten Datenbearbeitungspolitik Werbung machen können. In der Schweiz existieren im Moment jedoch noch keine etablierten Auditverfahren.

Solange sich kein Standard durchsetzen kann, sind Gütesiegel noch nicht das erhoffte Marketing-Instrument. Die Kosten zur Erlangen solcher Siegel sind für KMU hoch, die Bekanntheit der Gütesiegel im Publikum eher klein. Grosse Unternehmungen, die sich ein Gütesiegel leisten könnten, verzichten darauf, weil sie das Vertrauen ihrer Online-Kunden bereits gewonnen haben.