Datenschutz im Online-Shop: Wissen und Tipps Teil 1

Gerade eine moderne Shopsoftware gibt Shopbetreibern viele Mittel, um wichtige Daten über Besucher, Interessenten und Käufer zu erlangen. So schön diese neue Datenwelt für den Marketing-Mann auch ist, ein Shopbetreiber muss heute auch über Datenschutz und Sicherheit informiert sein, um seine rechtlichen Anforderungen zu erfüllen.

Und von diesen Anforderungen gibt es viele. Um hier etwas mehr Licht ins Dunkel zu bringen, informiert die etracker GmbH im shopbetreiber-blog.de und gibt Tipps zum korrekten Umgang mit Online-Kundendaten. Wir starten heute mit dem ersten Teil, der zweite Teil folgt in dann in ein paar Tagen hier im Blog.

Einleitung: Webcontrolling und Datenschutz

Die Erfassung und Verwendung von Online-Kundendaten zu Marketing- und CRM-Zwecken ist ein datenschutzrechtlich sensibles Feld. Die etracker GmbH – ein in Europa führender Anbieter von Web-Controlling Lösungen und Services zur genauen Analyse des Besucherverhaltens auf Webseiten – hat sich intensiv mit diesem Thema auseinandergesetzt.

In enger Zusammenarbeit mit dem Datenschutzbeauftragten der Stadt Hamburg hat etracker hierzu einen Leitfaden entwickelt. Dieser bietet Internet-Händlern und Web-Marketing-Managern eine Hilfestellung zum datenschutzkonformen Umgang mit Kundendaten, um mögliche rechtliche Konsequenzen von vornherein auszuschließen.

Doch warum ist der Datenschutz insbesondere für Online-Shop-Betreiber von großer Bedeutung?

Der Hintergrund: „Datenverarbeitung im Auftrag“

Unabhängig davon, ob ein Unternehmen die Daten seiner Kunden auf unternehmenseigenen Servern verarbeitet oder ob es diese Prozesse an einen externen Outsourcing-Anbieter weitergibt, es zeichnet stets für den rechtlich einwandfreien Umgang mit diesen Informationen verantwortlich. Denn wer Daten zur Verarbeitung oder Archivierung an einen Dritten weitergibt, der veranlasst nach deutschem Recht eine „Datenverarbeitung im Auftrag“.

Die rechtliche Konsequenz der Datenverarbeitung im Auftrag: Der Auftragnehmer – zum Beispiel ein Betreiber von CRM- oder Tracking-Software – ist rechtlich dazu verpflichtet, die Weisungen des Auftraggebers einzuhalten. Der Auftraggeber – beispielsweise ein Online-Shop, der seine Kundenansprache optimieren will – bleibt nach Paragraph 11 des Bundesdatenschutzgesetzes für die ordnungsgemäße Datenverarbeitung verantwortlich.

Der Auftraggeber muss sicherstellen, dass sein datenverarbeitender Dienstleister alle Daten gemäß dem strengen deutschen Datenschutzgesetz verarbeitet und speichert. Und dies gilt sowohl für ausgelagerte ASP-Lösungen als auch für Software-Systeme, die im eigenen Haus betrieben werden.

Deshalb möchten wir Ihnen sechs Tipps zum Datenschutz an die Hand geben, von denen wir Ihnen heute die ersten drei vorstellen:

Tipp 1: Persönliche Daten schützen

Das Datenschutzrecht unterscheidet zwei Typen von Daten: personen- und nicht personenbezogene Daten. Zu den nicht personenbezogenen Informationen werden all jene gerechnet, die anonym erfasst, verarbeitet und gespeichert werden und die nicht wieder einer Person zugeordnet werden

können. Daten, die konkrete Rückschlüsse auf eine Person zulassen, werden unter dem Begriff personenbezogene oder auch persönliche Daten zusammengefasst. Zu dieser Kategorie gehören beispielsweise Angaben wie Name, Adresse, Telefonnummer oder Kontodaten eines Kunden. Was besonders für die Erhebung von Online-Nutzerprofilen wichtig ist: Nach deutscher Rechtsprechung zählen auch IP-Adressen zu den personenbezogenen und somit schützenswerten Daten.

Wird ein Nutzerprofil pseudonymisiert – also aus dem klar identifizierten Werner Schmidt ein beliebiger Kunde A – dann ist es wichtig, dass die Pseudonymisierung nicht rückgängig gemacht werden kann. Das bedeutet im Klartext: Im pseudonymisierten Nutzungsprofil dürfen zwar nicht personenbezogene Angaben zum Nutzerverhalten wie die Zahl der Seitenaufrufe auf einer Website, aber keine personenbezogenen Daten wie zum Beispiel die IP-Adresse des Besuchers oder gar der Name des Nutzers gespeichert werden.

Ansonsten könnte das Pseudonym im Umkehrschluss – beispielsweise über die potenziell eindeutig zuzuordnende IP-Adresse eines Kunden – aufgehoben werden und damit wieder einen Bezug zu Werner Schmidt erlauben. Das wiederum wäre aus datenschutzrechtlicher Sicht ein klarer Gesetzesverstoß und damit strafbar. Die klare Empfehlung für E-Commerce-Händler, die zum Controlling ihrer Online-Angebote Nutzerprofile erfassen: Es ist sinnvoll, IP-Adressen erst gar nicht zu speichern – insbesondere auch nicht für Verteilungsanalysen, die besagen, wie häufig eine Site von konkreten IP-Adressen aufgerufen wurde.

Tipp 2: Auf Datenverarbeitung im Ausland hinweisen

Ein weiterer, wichtiger Aspekt, den es in Sachen Datenschutz zu berücksichtigen gilt, ist die Datenverarbeitung im Ausland. Da in anderen Ländern nicht nur andere Gepflogenheiten, sondern auch andere Online-Rechtsprechungen gelten, müssen sich Kunden explizit damit einverstanden erklären, dass ihre Daten nicht auf einem deutschen Server untergebracht werden. Ein Hinweis des Website-Betreibers auf die ausgelagerte Datenverarbeitung beispielsweise in den AGBs ist in diesem Fall nicht ausreichend.

Tipp 3: Keine Rückschlüsse von Kennzahlen auf Personen

Bis vor wenigen Monaten war es nicht möglich, von einer Telefonnummer auf den Namen und die Adresse einer gesuchten Person zurückzuschließen. Ein derartiger Reverse-Look-Up war gesetzlich untersagt. Diese Bestimmung wurde inzwischen zwar für Telefonverzeichnisse gelockert, für personenbezogene Online-Daten ist sie jedoch immer noch in vollem Umfang gültig.

Das bedeutet im Klartext: Eine Versand- oder Tracking-Software darf zwar aufgrund früherer Aussendungen von Werbe-Mails registrieren, welche E-Mail-Adressen welche Produkte favorisiert haben und die Adressen anschließend auch automatisch in entsprechende Versandgruppen einteilen. Dem Werbetreibenden ist es jedoch untersagt, aus einem solchen Pool von E-Mail-Adressen und von Versand- und Tracking-Informationen einzelne Daten zu extrahieren und von gespeicherten Kennzahlen auf konkrete Personen zu schließen.

Ruft ein Online-Händler aus seiner Software ab, welche E-Mail Beiträge beispielsweise Werner Schmidt geklickt und hinterher bestellt hat, dann verstößt er damit gegen das Datenschutzgesetz, wenn hierzu keine explizite Einwilligung von Werner Schmidt vorliegt.

Über den Autor: Oliver Krapp ist Geschäftsführer der etracker GmbH aus Hamburg. Mit innovativen Technologien und einem ausgewogenen Preis-Leistungsverhältnis ist etracker heute einer der führenden Web-Controlling Anbieter im internationalen Markt. etracker analysiert in Echtzeit jedes Detail des Besucherverhaltens auf Internetpräsenzen und liefert elementare Kennzahlen zur Steigerung der Kundenbindung, Optimierung von Online-Kampagnen und Aufdeckung von Klickbetrug. Als erstem Web-Controlling Unternehmen wurde der etracker GmbH nach einem aufwändigen Prüfverfahren durch den Hamburgischen Datenschutzbeauftragten die datenschutzrechtliche Konformität

bescheinigt. Die Web-Controlling Lösung von etracker wurde bereits mehrfach ausgezeichnet, etwa mit dem „Innovation 2007“-Award – dem IT-Oscar der PCpro – und mit dem „Innovationspreis 2007 ITK“ der Initiative Mittelstand.