

Datenschutz im Web – viel mehr als nur lästige Pflicht

7 Tipps zum korrekten Umgang mit Online-Kundendaten

Vielen Unternehmen, die online Kundendaten zu Marketing- und CRM-Zwecken erfassen und verarbeiten, fällt es schwer, sich im Dschungel der gesetzlichen Bestimmungen zu orientieren und sich im Dickicht der Vorschriften datenschutzkonform zu bewegen. Eine Verschärfung der datenschutzrechtlichen Vorschriften droht zudem seit einiger Zeit durch die Umsetzung der EU-Privacy-Richtlinie (auch Cookie-Richtlinie genannt) in deutsches Recht. In Bezug auf die Erfassung von Daten soll dann das Opt-In Verfahren die bisherige Opt-Out Regelung ersetzen. Das heißt, jeder Nutzer muss über die Datenerfassung und das Setzen von Cookies auf seiner Festplatte informiert werden und explizit oder implizit seine Einwilligung dazu erteilen.

Obwohl die Frist zur Umsetzung bereits am 26. Mai 2011 abgelaufen ist, hat die Bundesrepublik die EU-Richtlinie bislang nicht in nationales Recht umgesetzt. Der Bundesbeauftragte für Datenschutz, Peter Schaar, vertritt dennoch die Auffassung, dass die EU-Richtlinie von den deutschen Datenschutzbehörden in der bestehenden Form anwendbar sei. Ob sich diese Ansicht durchsetzen wird, kann im Moment noch niemand sagen. Als Orientierungshilfe inmitten all dieser Unwägbarkeiten gibt etracker, als einer der führenden Anbieter von Produkten und Dienstleistungen zur Optimierung von Websites und Online-Marketing Maßnahmen, Website-Betreibern 7 Tipps für die Generierung von Nutzerprofilen sowie für den richtigen Umgang mit ihnen.

Tipp 7: Sparsam mit Daten umgehen

Laut §3a BDSG dürfen personenbezogene Daten nur in dem Umfang erhoben und gespeichert werden, wie es für den jeweiligen Zweck der Geschäftsbeziehung mit dem Kunden erforderlich ist. Für die Erhebung von Daten, die für die Marktforschung wünschenswert, für den jeweiligen Zweck jedoch nicht zwingend notwendig sind, bedarf es der Einwilligung des betroffenen Nutzers. Erheben Sie daher nur Daten, die Sie für den jeweiligen Zweck auch wirklich benötigen. Verzichten Sie auf unnötige „Pflichtfelder“, auch wenn weitere Daten für Marketing und Marktforschung wünschenswert wären.

Lassen Sie auf die Daten nur diejenigen Mitarbeiter zugreifen, die die Daten auch wirklich benötigen. Nutzen Sie die Daten nur zu dem Zweck, den Sie jeweils bei der Datenerhebung angegeben haben. Für andere Zwecke benötigen Sie in jedem Fall die Einwilligung des betroffenen Nutzers.

Fazit

Datenschutz als eine lästige Pflicht anzusehen ist schon vom Grundsatz her falsch. Vielmehr liegt ein ordnungsgemäßer, transparenter und umsichtiger Umgang mit Besucherdaten auch im eigenen Interesse eines Unternehmens. Denn zum einen sorgt mangelnder Datenschutz für Probleme mit Aufsichtsbehörden und Mitbewerbern, zum anderen können Mitarbeiter oder Dritte, die nachlässig sind oder gar geschäftsschädigende Absichten hegen, dem Unternehmen enormen Schaden zufügen.

Und nicht zuletzt gilt:

Online-Business ist Vertrauenssache. Ein Anbieter, der intransparent oder gar rechtswidrig mit Kundendaten umgeht, ist nicht vertrauenswürdig. Transparenz und guter Datenschutz dagegen sind Verkaufsargumente und wichtige Bausteine für Ihren Online-Erfolg.

Tipp 1: **Der gesetzlichen Hinweispflicht nachkommen**

Auf die Erstellung von Nutzungsprofilen und über den Zweck und Umfang der Datenspeicherung muss hingewiesen werden. Stellen Sie dafür Hinweise zur Datenerhebung und -verarbeitung unter dem Stichwort „Datenschutz“ für den Nutzer sofort erkennbar und transparent auf Ihre Website. Achten Sie darauf, dass diese Hinweise verständlich formuliert und für die Kunden jederzeit abrufbar sind. Verstecken Sie die Hinweise auf keinen Fall in den AGBs oder unter falschen Überschriften.

Die Datenschutzhinweise sollten Antworten darauf geben, welche Daten in welcher Form gespeichert und verarbeitet werden und wie der Datenerhebung mit Wirkung für die Zukunft widersprochen werden kann. In den meisten EU-Ländern setzt sich mehr und mehr die Praxis des impliziten Einverständnisses zur Speicherung von pseudonymen Daten auf den Rechnern der Besucher in Form von Cookies durch. Dies bedeutet, dass dem Besucher ein so genanntes Cookie Consent-Banner eingeblendet wird. Dieses enthält die Mitteilung, dass sich Besucher durch Nutzung der Website mit dem Setzen von Cookies einverstanden erklären und verlinkt auf weitergehende Informationen. In der Regel fordern die Länder an dieser Stelle auch einen Hinweis auf Opt-out-Möglichkeiten. In einigen Ländern ist hingegen ein explizites Opt-in gefordert, etwa in Lettland, Litauen, Portugal, Zypern und – je nach Cookie – auch in Frankreich.

Tipp 2: **Ausschließlich pseudonyme Nutzerprofile erstellen**

Nutzer-Profile von Besuchern dürfen laut §15 Telemediengesetz ohne Einwilligung nur unter einem Pseudonym erstellt werden. In der Regel spricht man von einem Pseudonym, wenn hinter dem jeweiligen Datensatz fünf oder mehr Personen stecken können. Die Datenschutzbehörden haben hierzu festgestellt, dass die IP-Adresse ausdrücklich kein Pseudonym darstellt, da hierdurch Rückschlüsse auf den einzelnen Besucher einer Website gezogen werden können. Achten Sie darauf, dass IP-Adressen vor der Verarbeitung und Speicherung so gekürzt werden, dass ein Bezug zur natürlichen Person nicht mehr herzustellen ist.

Tipp 3:

Widerspruchsrecht einräumen und technisch umsetzen

Besucher müssen der Erstellung von Nutzungsprofilen widersprechen können. Der Widerspruch muss vom Website-Betreiber wirksam umgesetzt werden. Website-Besucher besitzen grundsätzlich bei allen erfassten personenbezogenen Daten das Recht, eine erteilte Einwilligung zur Nutzung dieser Daten für Zwecke der Werbung und Marktforschung zu widerrufen. Außerdem besteht ein Widerspruchsrecht zur Bildung von Nutzungsprofilen, die unter einem Pseudonym für Marktforschungs- und Analysezwecke erstellt wurden.

Diese Widerspruchsrechte müssen auch für alle Anwendungen und Dienste eingeräumt werden, die auf mobilen Endgeräten wie Smartphones oder Tablets ausgeführt werden. Möchte der Kunde von diesen Rechten Gebrauch machen und nicht länger zu den personenbezogenen bzw. pseudonymisierten Nutzungsprofilen beitragen, müssen Sie dies veranlassen und technisch umsetzen. Viele Web-Analyse Anbieter haben weitreichende Methoden, um einen aktiven Ausschluss eines einzelnen Besuchers aus der Datenerfassung sicherzustellen. Bei der Wahl eines Web-Analyse Anbieters sollten Sie auf eine solche Funktion unbedingt Wert legen.

Tipp 4:

Keine IP-Adressen verarbeiten oder gar speichern

Ohne bewusste, eindeutige Einwilligung des Betroffenen darf die vollständige IP-Adresse nicht verarbeitet werden. Eine illegale Verarbeitung ist beispielsweise bereits die IP-Geolokalisierung oder die Identifikation der Firma des Besuchers auf Basis vollständiger IP-Adressen. Allerdings ist eine Geolokalisierung auch mit verkürzter IP-Adresse – und damit datenschutzkonform – möglich. Achten Sie darauf, dass die von Ihnen gewählte Web-Analyse Software über entsprechende Konfigurationsmöglichkeiten verfügt, um diese Informationen auch auf Basis verkürzter IP-Adressen zu ermitteln. Aufwendige Programmierungen im Code sind dann nicht notwendig.

Tipp 5: **Strikte Datentrennung einhalten**

Pseudonyme und personenbezogene Daten müssen stets getrennt gespeichert und dürfen ohne Einwilligung nicht zusammengeführt werden. Speichern Sie personenbezogene und nicht personenbezogene Daten in separaten Datenbanken. Eine Löschung bzw. Anonymisierung von personenbezogenen Informationen ist dann unproblematisch und schnell umgesetzt. Generell gilt: Je stringenter Sie Ihre Daten organisieren, umso schneller und einfacher können Sie auch dem Widerspruchsrecht Ihrer Kunden entsprechen.

Tipp 6: **„Auftragsdatenvereinbarung“ mit Dienstleister abschließen**

Die Auftragsdatenverarbeitung (ADV) ist ein fester Bestandteil des Bundesdatenschutzgesetzes (BDSG): Der Vertrag mit einem Dienstleister muss den Anforderungen nach §11 BDSG entsprechen. Die ADV erfordert stets die Schriftform, eine Online-Akzeptanz ist nicht möglich. In der ADV wird die Zusammenarbeit mit dem Dienstleister geregelt. In den meisten Fällen wird das Web-Controlling nicht auf eigenen Servern betrieben, sondern es werden hierfür die Dienste Dritter in Anspruch genommen.

Wenn auf diese Weise die Daten weitergeleitet werden, ist es zwingend erforderlich, dass Sie die Kontrolle über die Daten behalten. Schließen Sie daher in jedem Fall mit dem Dienstleister einen schriftlichen Vertrag zur Verarbeitung der Daten in Ihrem Auftrag ab (Auftragsdatenverarbeitung). Wichtig zu beachten ist: Der Auftraggeber bleibt stets verantwortlich für die datenschutzkonforme Verarbeitung. Nur er wird haftbar gemacht und muss im Falle eines Verfahrens mit Bußgeldstrafen rechnen (vergl. §11 Abs. 1 BDSG).

Anforderungskatalog zum Datenschutz

Checkliste der datenschutzrechtlichen Anforderungen bei der Web-Analyse*

Anforderungen	etracker
Der gesetzlichen Hinweispflicht nachkommen Auf die Erstellung von Nutzungsprofilen und über den Zweck und Umfang der Datenspeicherung muss hingewiesen werden.	✓
Ausschließlich pseudonyme Nutzungsprofile erstellen Nutzungsprofile von Besuchern dürfen nur unter einem Pseudonym erstellt werden. Die IP-Adresse ist ausdrücklich kein Pseudonym.	✓
Widerspruchsrecht einräumen und technisch umsetzen Besucher müssen der Erstellung von Nutzungsprofilen widersprechen können. Der Widerspruch muss vom Seitenbetreiber wirksam umgesetzt werden.	✓
Keine IP-Adressen verarbeiten oder gar speichern Ohne bewusste, eindeutige Einwilligung des Betroffenen darf die vollständige IP-Adresse nicht verarbeitet werden. Eine illegale Verarbeitung ist beispielsweise bereits die IP-Geolokalisierung.	✓
Strikte Datentrennung einhalten Pseudonyme und personenbezogene Daten müssen stets getrennt gespeichert werden und dürfen nicht zusammengeführt werden.	✓
„Auftragsdatenverarbeitung“ mit Dienstleister abschließen Web-Analyse Dienstleister müssen ihren Kunden eine Vereinbarung zur Auftragsdatenverarbeitung anbieten aus der hervorgeht, dass der Auftragsdatenverarbeiter pseudonyme Nutzungsprofile erstellt.	✓

* Gemäß dem Beschluss der obersten Aufsichtsbehörden für den Datenschutz im nicht-öffentlichen Bereich vom 26./27. November 2009 in Stralsund.

etracker ist damit



etracker[®]
more than analytics.