

Achtung:

Datenschutz!

7 Tipps zum korrekten Umgang mit
Online-Kundendaten und Datenschutz-Anfragen.



etracker[®]
Know Now.

Inhalt.

Einleitung.....	3
Tipp 1: Gesetzlicher Hinweispflicht nachkommen. ...	4
Tipp 2: Bei der Verarbeitung von IP-Adressen vorsichtig sein.	5
Tipp 3: Widerrufs- u. Widerspruchsrecht einräumen.	6
Tipp 4: Datenschutzerklärungen von Dienstleistern prüfen.	7
Tipp 5: Sparsam mit Daten umgehen.	9
Tipp 6: Datenschutz-Anfragen richtig beantworten.	10
Tipp 7: Sicherheitsbewusstsein schärfen.	11
Fazit.	11

Die etracker GmbH aus Hamburg ist einer der führenden Anbieter von Produkten und Dienstleistungen zur Optimierung von Websites und Online-Marketing Maßnahmen.

Die etracker GmbH wurde im Jahr 2000 gegründet und ist als erstes Web-Controlling Unternehmen durch den Hamburger Datenschutzbeauftragten geprüft worden. Alle Daten werden 100 % konform zu europäischen und deutschen Datenschutzgesetzen verarbeitet.

Testen Sie alle etracker Produkte kostenlos unter www.etracker.com

Zu unseren mehr als 65.000 zufriedenen Kunden zählen:



Einleitung.

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.

Der Hamburger Web-Controlling und Online-Marktforschungs-Spezialist etracker hat deswegen einen praxisorientierten Leitfaden entwickelt, der E-Commerce-Anbietern und Web-Marketing Mitarbeitern konkrete Handlungsempfehlungen für effektives und rechtlich einwandfreies Datenschutzmanagement mit auf den Weg gibt.

Die folgenden 7 Tipps unterstützen Unternehmen nicht nur beim datenschutzkonformen Umgang mit Online-Kundendaten, sondern sorgen auch für ein adäquates Handling von Datenschutz-Anfragen von Nutzern.

Tipp 1:

Gesetzlicher Hinweispflicht nachkommen.

Unternehmen müssen ihre Kunden sowohl auf die Erhebung von personenbezogenen Daten hinweisen – dies sind Daten, über die sich ein Bezug zu einer Person bereitstellen lässt – als auch über die Art der erhobenen Daten sowie Art und Umfang ihrer Verwendung.

Auch über die Übermittlung an Dritte und die Datenverarbeitung außerhalb Deutschlands müssen Kunden aufgeklärt werden. Diese gesetzliche Verpflichtung zur Unterrichtung ergibt sich aus §13 Abs.1 Telemediengesetz.

IP-Adressen zählen zu den personenbezogenen Daten

Zu den Pflichten zählt zudem der Hinweis auf die Speicherung und Weiterverarbeitung von IP-Adressen, denn nach Teilen der deutschen Rechtsprechung zählen auch diese zu den personenbezogenen Daten. Anbieter sollten auch dann auf die Speicherung von IP-Adressen hinweisen, wenn Namen oder andere persönliche Identifikationsmerkmale nicht mit erhoben werden.

Konkrete Handlungsempfehlung:

Transparente und sichtbare Hinweise geben

Stellen Sie 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 Allgemeinen Geschäftsbedingungen oder unter falschen Überschriften.

Machen Sie Ihre Kunden auch darauf aufmerksam, wenn Sie ein Web-Analyse System einsetzen und klären Sie sie transparent über den Zweck der Erhebung und die Verwendung der Daten auf. Ein Hinweis auf die Verwendung einer Analyse-Software ist zwingend erforderlich, wenn die Web-Analyse Daten außerhalb der Europäischen Union gespeichert oder verarbeitet werden.

Tipp 2:

Bei der Verarbeitung von IP-Adressen vorsichtig sein.

Verarbeitung von IP-Adressen ist illegal

In weiten Teilen der deutschen Rechtsprechung ist es unstrittig, dass IP-Adressen zu den personenbezogenen Daten gehören und Kunden deswegen auf ihre Speicherung und Weiterverarbeitung hingewiesen werden müssen. Einzelne Datenschutzbehörden, etwa die in Nordrhein-Westfalen, gehen aber noch weiter: Ihrer Auffassung nach handelt ein Website-Betreiber bereits dann rechtswidrig, wenn er – ohne darauf hinzuweisen – IP-Adressen nutzt, um beispielsweise herauszufinden, wo ein Besucher lokalisiert ist oder welchen Provider und welche Zugangsbandbreite er nutzt. Rechtswidrig sei dies auch dann, wenn der Website-Betreiber die IP-Adressen nicht speichert.

Konkrete Handlungsempfehlung:

Seien Sie auch dann vorsichtig bei der Verarbeitung von IP-Adressen, wenn sie diese nicht oder nur verkürzt speichern. Achten Sie bei der Auswahl eines Web-Analyse Systems darauf, dass es über Konfigurationsmöglichkeiten verfügt, um die Abfrage beispielsweise von Geo- oder Provider-Informationen über die Besucher zu unterbinden.

Tipp 3:

Widerrufs- und Widerspruchsrecht einräumen.

Rechte der Kunden jederzeit berücksichtigen

Kunden 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.

Möchte der Kunde von diesen Rechten Gebrauch machen und nicht länger zu den personenbezogenen bzw. pseudonymisierten Nutzungsprofilen beitragen, muss der Website-Betreiber dies veranlassen und technisch umsetzen. Dies betrifft insbesondere auch die Löschung vorhandener personenbezogener Daten, soweit diese nicht für die Vertragsbeziehung mit dem Nutzer benötigt werden.

Aus datenschutzrechtlicher Sicht ist es daher nicht ausreichend, dem Kunden bestimmte Modifizierungen seines Browsers, etwa das Blockieren von Cookies, vorzuschlagen.

Konkrete Handlungsempfehlung:

Separate Datenbanken verwenden

Speichern Sie personenbezogene und nicht personenbezogene Daten in separaten Datenbanken. Eine Löschung bzw. Anonymisierung von personenbezogenen Informationen ist so unproblematisch und schnell umgesetzt.

Generell gilt: Je stringenter Sie Ihre Daten organisieren, umso schneller und einfacher können Sie dem Widerspruchsrecht Ihrer Kunden entsprechen.

Logfile deaktivieren

Damit Nutzungsdaten nicht gespeichert werden, sollten Sie zunächst das Logfile Ihres Webservers abschalten. Dort werden nämlich in der Regel IP-Adressen gespeichert, über die wiederum personenbezogene Nutzungsprofile generiert werden können. Oder Sie sollten das Logfile so umkonfigurieren, dass die IP-Adresse des Nutzers gar nicht aufgeführt

wird. Viele Web-Analyse Anbieter haben weitreichende Methoden, um einen aktiven Ausschluss eines einzelnen Besuchers aus der Datenerfassung sicherzustellen. Bei der Wahl eines Web-Controlling Anbieters sollten Sie auf eine solche Funktion unbedingt Wert legen.

Tipp 4:

Datenschutzerklärungen von Dienstleistern prüfen.

Viele Unternehmen übermitteln Daten an Dritte, die für sie tätig sind oder Dienste erbringen – beispielsweise an Betreiber von Web-Analyse Systemen. Werden personenbezogene Daten von Dritten verarbeitet, bedeutet dies nach deutschem Recht eine „Datenverarbeitung im Auftrag“.

Keine Datenübermittlung an Dritte ohne Zustimmung

Nach §11 Bundesdatenschutzgesetz bleibt der Auftraggeber in diesem Fall für die ordnungsgemäße Datenverarbeitung verantwortlich. Übermittelt ein Unternehmen also Daten etwa an einen Web-Analyse Anbieter und hat dafür keine ausdrückliche Zustimmung der Nutzer, haftet es für daraus entstehende Probleme und den Missbrauch durch Dritte.

Verwendet der Web-Analyse Dienstleister beispielsweise die ihm zur Verarbeitung vorliegenden Daten in personenbezogener Form für weitere Zwecke – etwa für die Bildung von personalisierten Interessensprofilen – oder gibt er personenbezogene Daten an Dritte weiter, wie dies bei kostenlosen Web-Analyse Diensten oft der Fall ist, ist nach geltendem Recht eine ausdrückliche Einwilligung des Betroffenen in Opt-In-Form vor der Datenerhebung erforderlich (§§ 12 Abs. 1 und 2, 13 Abs. 2 Telemediengesetz).

Haftung liegt beim Website-Betreiber

Für Zuwiderhandlungen ist derjenige verantwortlich, auf dessen Internetseite(n) die Daten erhoben wurden. Unternehmen können sich nicht darauf berufen, dass sie in die technischen Abläufe ihres Dienstleisters keine Einsicht hatten.

Konkrete Handlungsempfehlung:

Transparenz schaffen

Analysieren Sie Ihre Datenverwendung genau. Sehen Sie sich die Vertrags- und Datenschutzerklärungen Ihrer Dienstleister im Detail an und bestehen Sie auf Klarheit. Lassen Sie sich von Ihren Analyse-Anbietern und Dienstleistern schriftlich mitteilen, wozu sie die auf Ihrer Internetseite erhobenen Daten verwenden, wenn eine solche Information nicht klar und verständlich bereitgestellt wird. Bleiben Sie hartnäckig, wenn Dritte Ihnen keine klare und vollständige Auskunft geben wollen und verzichten Sie im Zweifelsfall auf die Beauftragung.

Erfolgt die Datenverarbeitung durch Dritte außerhalb der Europäischen Union, müssen Sie sich auf jeden Fall die Einhaltung des deutschen Rechts bei der Datenverarbeitung bestätigen lassen. Lassen Sie sich auch hier keineswegs durch ausweichende Antworten abwimmeln.

Datenschutzkonzepte vorlegen lassen

Um Auftragsdatenverarbeiter zu testen, lassen Sie sich den Inhalt der Verpflichtung zum Datengeheimnis, die diese für ihre Mitarbeiter verwenden, mitteilen und bestätigen, dass alle Mitarbeiter, die an der Auftragsdatenverarbeitung beteiligt sind, dementsprechend verpflichtet wurden. Sie sollten sich darüber hinaus vom Dienstleister auch sein Datenschutzkonzept vorlegen lassen.

Datenschutzprüfungen nur durch offizielle Behörden

Verlassen Sie sich nicht allein auf Prüfsiegel, mit denen etwa Web-Analyse Anbieter werben. Denn viele privatwirtschaftliche Prüfunternehmen untersuchen die Einhaltung der Datenschutzgesetze gar nicht. Häufig werden nur die Website und die Usability untersucht, nicht aber, ob die Anbieter interne Prozesse gemäß den deutschen rechtlichen Anforderungen etabliert haben und ihre Web-Analytics Lösung 100 % datenschutzkonform ist. Achten Sie deswegen unbedingt darauf, ob ein Web-Analyse Anbieter von einer offiziellen Behörde geprüft wurde. Nur diese garantiert maximale Sicherheit.

Tipp 5:

Sparsam mit Daten umgehen.

Nur notwendige Daten erheben

Personenbezogene Daten dürfen nur in dem Umfang erhoben und gespeichert werden, wie es für den jeweiligen Zweck der Geschäftsbeziehung mit dem Kunden erforderlich ist. Dies ergibt sich aus dem Grundsatz der Datensparsamkeit und der Zweckbindung (§3a Bundesdatenschutzgesetz). Reine Nützlichkeit reicht grundsätzlich nicht aus.

Konkret bedeutet dies, dass beispielsweise keine Namen oder Adressen für einen Newsletter erhoben werden dürfen. Hier darf ausschließlich die E-Mail-Adresse als Pflichtangabe verlangt werden.

Auch die weit verbreitete verpflichtende Abfrage von Kunden-Telefonnummern bei Online-Bestellungen für eventuelle Rückfragen ist rechtswidrig.

Konkrete Handlungsempfehlung:

Erheben Sie 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.

Zweckgemäße Datenverarbeitung einhalten

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. Beim Web-Controlling sollten Sie darauf achten, dass Sie das Speichern von IP-Adressen vermeiden. Bei seriösen Web-Analyse Betreibern werden IP-Adressen – wenn überhaupt – standardmäßig nur verkürzt gespeichert.

Tipp 6:

Datenschutz-Anfragen richtig beantworten.

Auskunftspflicht

Nutzer haben nach §34 Bundesdatenschutzgesetz ein Auskunftsrecht über die zu ihrer Person gespeicherten Daten.

Es ist deswegen sinnvoll – auch angesichts der jüngsten Skandale und der gestiegenen Sensibilität in der Bevölkerung – auf Anfragen gut vorbereitet zu sein und interne Prozesse zur Abwicklung solcher Anfragen zu etablieren.

Konkrete Handlungsempfehlung:

Datenschutzbeauftragten benennen

Legen Sie einen konkreten Ansprechpartner bei Fragen zum Thema Datenschutz fest. In Ihrem Unternehmen sollte eine zentrale Stelle, im Idealfall ein betrieblicher Datenschutzbeauftragter, über sämtliche Datenerhebungen und die weitere Verwendung der Daten informiert sein.

Für die Nutzer muss auf der Website direkt ersichtlich sein, wer der richtige Ansprechpartner für ihre Fragen ist: Binden Sie deswegen entweder einen direkten E-Mail-Link in die Datenschutzerklärung ein oder stellen Sie Ihren betrieblichen Datenschutzbeauftragten namentlich vor.

Kundenanfragen ernst nehmen

Wenn Sie eine Anfrage erhalten, sollten Sie sie genau durchlesen, eine klare und richtige Antwort geben und auf die Bedenken Ihrer Kunden eingehen – möglichst zeitnah und mit der erforderlichen Offenheit. Verweisen Sie auf Ihre Datenschutzerklärung, wenn darin alle Fragen adäquat beantwortet werden und sie gut sichtbar verfügbar ist.

Sprachlosigkeit, unfreundliche und sachlich falsche Antworten oder ein Verweis auf eine Datenschutzerklärung, die keine relevanten Inhalte besitzt, wirken unseriös, unprofessionell und schaden dem Vertrauensverhältnis massiv.

Tipp 7:

Sicherheitsbewusstsein schärfen.

Kundendaten auch intern vor Missbrauch schützen

Seien Sie risikobewusst beim Umgang mit Kundendaten. Achten Sie darauf, dass keine Dateien mit Kundendaten auf Laufwerken liegen, die für alle Mitarbeiter zugänglich sind, und lassen Sie – so banal dies klingen mag – auch keine Datenträger mit Kundendaten herumliegen.

Vermeiden Sie auf jeden Fall auch unsichere Übermittlungen, beispielsweise unverschlüsselte E-Mail-Anhänge. Bei all diesen Vergehen handelt es sich nicht um kleine Nachlässigkeiten – sie können vielmehr katastrophale Folgen haben. Das zeigen nicht zuletzt die jüngsten, publik gewordenen Datenschutz-Skandale.

Ein fehlendes Sicherheitsbewusstsein – von der Chefetage bis zu den unteren Ebenen eines Unternehmens – ist nach wie vor ein immenser Risikofaktor für einen effektiven Datenschutz.

Fazit.

Datenschutz als eine lästige Pflicht anzusehen, ist schon vom Grundsatz her falsch. Vielmehr liegt ein ordnungsgemäßer, transparenter und umsichtiger Umgang mit personenbezogenen Daten auch im eigenen Interesse eines Unternehmens.

Denn zum Einen sorgt schlechter Datenschutz für Probleme mit Aufsichtsbehörden und Mitbewerbern, zum Anderen können kriminell veranlagte oder nachlässige Mitarbeiter oder Dritte dem Unternehmen enormen Schaden zufügen.

Und nicht zuletzt gilt: Online-Business ist Vertrauenssache. Ein Anbieter, der intransparent oder gar rechtswidrig mit personenbezogenen Daten umgeht, ist nicht vertrauenswürdig. Transparenz und guter Datenschutz dagegen sind wichtige Verkaufsargumente für den Online-Erfolg.

etracker GmbH
Alsterdorfer Straße 2a
22299 Hamburg
Germany

t +49 40 55 56 59 50
f +49 40 55 56 59 59
e info@etracker.com
i www.etracker.com

