Websites und der Datenschutz

Informationspflichten im Web

Die Webpräsenz Ihres Unternehmens ist schon lange nicht mehr nur ein Thema des Marketings oder Vertriebs. Seit Google Analytics und Facebook in die Kritik der Datenschutzaufsichtsbehörden geraten sind, haben auch Sie als Datenschutzbeauftragter eine Kontrollpflicht. Wir zeigen, welche Aspekte Sie aus Sicht des Datenschutzes berücksichtigen müssen. Diese Aspekte sind nicht nur rechtlich gefordert, sie können vielmehr auch kaufentscheidend sein.

Petabyte oder gar Exabyte von Daten und Informationen surren mittlerweile durch das Netz. Darunter sind naturgemäß auch riesige Mengen personenbezogener Daten – höchstwahrscheinlich mittendrin Ihre eigenen oder solche aus Ihrem Unternehmen.

Datenschutz auf unserer Website – warum das denn?

Dass die Erfordernisse nach dem Bundesdatenschutzgesetz auch im Rahmen der Firmenpräsenz eingehalten werden müssen, scheint jedoch die wenigsten zu interessieren.

Denn die Marketingabteilung ist ausschließlich an einem optimalen Aufbau des Webauftritts interessiert. Statistische Auswertungen à la Google Analytics aus den Aktivitäten und Seitenaufrufen von Besuchern sind willkommene Arbeitsgrundlagen, um die Präsenz weiter zu verbessern. Und so sind Sie regelmäßig mit der Frage konfrontiert: Datenschutz – warum?

Der Seitenbetreiber hat eine Informationspflicht gegenüber den Betroffenen

Nach dem BDSG ist der Betroffene bei der Datenerhebung zu informieren. Diese Informationspflicht beinhaltet

- die verantwortliche Stelle,
- die Zweckbestimmung und
- die Empfänger der Daten.

Diese Pflicht gilt grundsätzlich auch bei der Erhebung von personenbezogenen Daten im Rahmen Ihres Webauftritts.

„Wir erheben doch gar keine personenbezogenen Daten!?“

Der häufig genannte Einwand lautet: Wir erheben keine Daten. Indirekt mag dies richtig sein, jedoch werden regelmäßig die verschiedenen Zusatztools und Begleitanwendungen vergessen, die auf Basis von Cookies oder IP-Adressen arbeiten.

Nach § 3 Abs. 1 BDSG unterliegen auch anfallende Daten einer bestimmbaren natürlichen Person dem Anwendungsbereich des Datenschutzes. Das ist bei einer IP-Adresse der Fall.

Die IP-Adresse ist zumindest personenbeziehbar

Ob eine IP-Adresse zu den personenbezogenen Daten gehört, ist umstritten. Das bayerische Landesamt für Datenschutzaufsicht äußert sich dazu z.B. in seinem Tätigkeitsbericht 2009/2010 folgendermaßen: „Die IP-Adresse ist häufig nicht nur für den jeweiligen Access-Provider, der die IP-Adressen vergibt, einem bestimmten Nutzer zuordnen. Insbesondere in den Fällen, in denen sich der Nutzer auf der besuchten Webseite registriert hat, ist auch für den jeweiligen Webseitenbetreiber eine Verbindung zwischen der empfangenen IP-Adresse und der Person des Nutzers herstellbar. Wir gehen daher im Regelfall von der Personenbezogenheit der IP-Adresse aus.“

(Quelle: Bayerisches Landesamt für Datenschutzaufsicht, Tätigkeitsbericht 2009/2010, S. 29–30, *kurzlink.de/taetigkeitsbericht*)

Die IP-Adresse kommt öfter zum Einsatz, als man denkt

Prüfen Sie daher, über welche Zusatzanwendungen im Rahmen des Webauftritts die IP-Adresse Verwendung findet. In der Regel sind dies:

- Cookies, die unter Umständen die IP-Adresse speichern
- klassische Analysetools wie Google Analytics, PIWIK, eTracker o.Ä.
- Trackingtools zur Echtzeitanalyse, Live- oder Mouse-Trackinglösungen, die analysieren, wie sich die Besucher auf Ihrer Website bewegen
- Geolokalisierung zur geografischen Ortung und Rückverfolgung
- Behavioural Targeting für gezielte Werbebanner
- Social Networks à la Facebook

Allen diesen Zusatz- und Begleitanwendungen ist gemein, dass sie in der Regel auf Basis der IP-Adresse und/oder Cookies auf den Rechnern des Besuchers funktionieren.

Nutzungsprofile pseudonymisieren

Arbeiten Webseitenbetreiber mit Nutzungsprofilen, müssen sie entsprechend dem Telemediengesetz (TMG) folgende Bestimmungen beachten:

- Nach § 15 Abs. 3 TMG dürfen Nutzungsprofile nur bei Verwendung von Pseudonymen erstellt werden.
- Weiter ist nach § 15 Abs. 3 Satz 2 dem Betroffenen die Möglichkeit zum Widerspruch gegen die Erstellung von Nutzungsprofilen einzuräumen.

Ausschlaggebend dabei: Eine vollständige IP-Adresse stellt kein Pseudonym im Sinne des TMG dar!

Drängen Sie auf eine Datenschutzerklärung auf der Website

Für alle Datenerhebungen und Weitergaben von personenbezogenen Daten ist eine Erklärung auf Ihrer Website erforderlich. Obligatorisch sollte dazu

Die Besucher Ihrer Webpräsenz müssen sich darauf verlassen können, dass ihre Daten bei Ihnen sicher sind

eine spezielle Webseite mit den Einzelinformationen aufgebaut werden.

Insbesondere beim Betrieb eines eigenen Bestell-Shops sind qualifizierte Informationen oft kaufentscheidend für Interessenten. Wer seinen Kunden größtmögliche Sicherheit bietet, sollte das auch klar kommunizieren.

Spezialgebiet Online-Shop: Übermittlung vertraulicher Daten

Speziell im Online-Shop werden neben den notwendigen Namen und Kontaktdaten nicht selten auch personenbezogene Daten zu Bank- oder Kreditkartenkonten erhoben. Daher sollte für die Übermittlung vertraulicher Daten immer eine gesicherte Verbindung aufgebaut werden. Als Standard hat sich hierbei die SSL-Verschlüsselung etabliert.

Weisen Sie auf HTTPS hin

Insbesondere bei der Erhebung von vertraulichen Daten wie z.B. der Kontoverbindung bietet sich in der Erfassungsmaske ein Hinweis an, um auf den geschützten Datentransfer aufmerksam zu machen. Idealerweise findet sich dieser Hinweis als vertrauensbildende Maßnahme direkt vor dem „Weiter"- oder „Bestellen"-Button.

Gütesiegel schaffen Vertrauen

Sicherheit hat für die Shop-Nutzer oberste Priorität – nicht nur beim Online-Einkauf, sondern auch bei der Abwicklung der Bestellung. Verschiedene Anbieter werben mit der Vergabe von Gütesiegeln. Experten prüfen und analysieren dazu im Rahmen der Zertifizierung Ihren Shop anhand unterschiedlicher Prüfkriterien.

Logos und Testate finden unter den Nutzern von Online-Shops immer mehr Aufmerksamkeit. Das Qualitätssiegel „geprüfter Webshop" kann Vertrauen bei Ihren Bestellkunden wecken. Auch die Angabe eines direkten Ansprechpartners zu Fragen der Shop-Sicherheit und des Datenschutzes hinterlassen bei Ihren potenziellen Kunden einen seriösen Eindruck.

Der „Anti-Abzock"-Button

Der Bundestag hat Anfang März 2012 ein neues Gesetz verabschiedet, um Verbraucher besser vor Kostenfallen im Internet zu schützen. Daher muss zukünftig bei kostenpflichtigen Bestellungen mit einem Bestell-Button unmissverständlich klar gemacht werden, dass das Angebot einen Geschäftsabschluss zur Folge hat (mehr dazu unter *kurzlink.de/kostenfallen*).

Vom Imageschaden bis zur Haftstrafe

Grundsätzlich riskiert Ihr Unternehmen bei einem fahrlässigen Umgang mit Kundendaten im Web einen erheblichen Imageschaden. Auch empfindliche Geldbußen und sogar Gefängnisstrafen sind möglich.

Grundsätzlich gilt: Erlaubt ist nur die Verwendung und Speicherung von personenbezogenen Daten, die unbedingt notwendig ist.

Oberstes Gebot beim Webauftritt ist die Datensparsamkeit

Prüfen Sie als Datenschutzbeauftragter die Webaktivitäten Ihres Unternehmens grundsätzlich nach dem Gebot der Datensparsamkeit. Je nach Webangebot sind dazu unterschiedliche Maßstäbe anzusetzen. Dazu müssen Sie sich ausführlich mit dem Bundesdatenschutzgesetz sowie dem Telemediengesetz auseinandersetzen.

Besonders wichtig: Nehmen Sie Ihre Kunden durch ausführliche Datenschutzinformationen mit ins Boot!

Hermann Keck

Hermann Keck ist externer Datenschutzbeauftragter (*www.keck-dsb.de*).

Mehr zum Thema

Praxisratgeber „Rechtssichere Internetseiten"

Das „Electronic Commerce-Kompetenzzentrum Ruhr" hat eine durch das Bundesministerium für Wirtschaft und Technologie geförderte Broschüre herausgegeben. Der Ratgeber ist online zu finden unter *kurzlink.de/internetseiten.*

Musterdatenschutzerklärung

Abonnenten der Datenschutz PRAXIS finden einen ausführlichen Fachbeitrag zur Datenschutzerklärung sowie ein kostenloses Muster für eine Datenschutzerklärung unter *kurzlink.de/dserklaerung.*