Datenschutz im Onlineshop: Was Shopbetreiber beachten müssen

istockphoto.com / Natali_Mis

Immer mehr Menschen kaufen online ein. Auch viele Augenoptiker nutzen den Onlinehandel als zusätzlichen oder gar alleinigen Vertriebskanal. Mithilfe eines eigenen Onlineshops können neue Kundenkreise erschlossen, Umsatzsteigerungen erzielt und eine engere Kundenbindung erreicht werden. Gleichzeitig stellt der Onlineshop den Shopbetreiber allerdings auch vor die Herausforderung, sich in vielen verschiedenen Bereichen Kenntnisse anzueignen, um die kommerzielle Website rechtssicher und erfolgreich betreiben zu können. Neben grundlegenden Kenntnissen zu Shopsystemen, Shopdesigns, Servern und zum Onlinemarketing sind insbesondere auch Rechtskenntnisse erforderlich. Welche Anforderungen sind beim Betrieb eines Onlineshops in datenschutzrechtlicher Hinsicht zu beachten? Der folgende Beitrag gibt einen Überblick:

Wer einen Onlineshop betreibt, ist daran gewöhnt, sich regelmäßig auch mit rechtlichen Fragestellungen, wie der Impressumspflicht und den Allgemeinen Geschäftsbedingungen, auseinanderzusetzen. Gerade im Datenschutz gibt es indes zahlreiche gesetzliche Vorgaben, die viele Shopbetreiber nicht kennen.

Ein wesentliches Verkaufsargument ist dabei der rechtskonforme Umgang mit Kundendaten: Im Rahmen eines Bestellprozesses gibt der Kunde unter anderem seinen Namen, seine Anschrift und seine Bankverbindung preis. Unter anderem die Forsa-Studie im Auftrag von Hiscox 2016 und die Studie „Trends im E-Commerce“ 2013 belegen, dass Internetnutzer beim Onlineshopping Angst vor dem Missbrauch persönlicher Daten haben. Das Einhalten datenschutzrechtlicher Bestimmungen und die Gewährleistung von Datensicherheit können somit die Entscheidung für einen bestimmten Onlineshop positiv beeinflussen.

Nur notwendige personenbezogene Daten dürfen als Pflichtangaben erhoben werden.

Aus datenschutzrechtlicher Sicht stellt sich zunächst die Frage, welche personenbezogenen Daten im Rahmen des Onlinebestellprozesses abgefragt werden dürfen. Personenbezogene Daten sind dabei alle Informationen, über die ein Personenbezug hergestellt werden kann, wie Name, Adresse, Telefonnummer, Geburtsdatum und Kontoverbindung. Insoweit ist der Grundsatz der Datenvermeidung und der Datensparsamkeit gemäß § 3a Bundesdatenschutzgesetz zu beachten. Demnach sollen nur so viele personenbezogene Daten erhoben werden, wie für die jeweilige Anwendung unbedingt notwendig sind.

Bei der Gestaltung von Eingabemasken im Internet ist somit sicherzustellen, dass allein die für den angestrebten Zweck erforderlichen Daten als Pflichtangaben abgefragt werden. Es ist jedoch zulässig, auch weitere Angaben zu erfassen, soweit eindeutig erkennbar ist, dass die Angabe freiwillig erfolgt. Dies kann beispielsweise dadurch geschehen, dass alle Pflichtfelder mit einem Sternchen gekennzeichnet werden. Das Sternchen muss dann allerdings an anderer, gut sichtbarer Stelle aufgelöst werden, so dass erkennbar ist, welche Bedeutung diesem zukommt.

So dürfte es für die Durchführung des Bestellprozesses regelmäßig nicht erforderlich sein, auch die Telefonnummer abzufragen. Ist jedoch klar erkennbar, dass es sich hierbei um eine freiwillige Angabe handelt, spricht nichts dagegen, ein entsprechendes Feld zu integrieren.

„Ohne Einwilligung in der Regel kein Newsletterversand möglich“

Das Newslettermarketing ist eine schnelle, flexible und kostengünstige Möglichkeit, um potenzielle Kunden auf sich aufmerksam zu machen. Es bietet Shopbetreibern damit viele Vorteile. Wer seinen Newsletter nicht nur an Bestandskunden schicken möchte, ist gesetzlich dazu verpflichtet, vom Empfänger vorher eine Einwilligung einzuholen. ▸

Nach einem Urteil des Bundesgerichtshofs vom 16.07.2008, Az. VIII ZR 348/06, muss der Empfänger von E-Mail-Werbung die Einwilligung durch ein sogenanntes Opt-In, also durch das aktive Anklicken eines Kästchens, erteilen.

Bei der Versendung von Newslettern reicht das einfache Opt-In auf einer Website jedoch nicht aus. Aus Beweisbarkeitsgründen wird ein sogenanntes Double-Opt-In und damit die zweimalige Zustimmung des Empfängers benötigt. Nach Eingabe der E-Mail-Adresse auf der Website des Unternehmens sollte eine Bestätigungs-E-Mail an die eingegebene Adresse versendet werden mit der Bitte, die Einwilligung per Klick auf einen Bestätigungslink endgültig zu bestätigen. Die Bestätigungs-E-Mail muss dabei stets absolut werbefrei sein. Erst nach Anklicken des Links durch den Empfänger darf eine Aufnahme in den Newsletterverteiler erfolgen. Durch dieses Verfahren soll sichergestellt werden, dass auch wirklich der Inhaber des E-Mail-Kontos die Einwilligung in den Erhalt des Newsletters erteilt.

Inhaltlich ist erforderlich, dass die Einwilligung bewusst und eindeutig erteilt wird. Der Newsletterempfänger ist daher auf den Zweck der Erhebung, Verarbeitung und Nutzung seiner Daten hinzuweisen. Es ist unbedingt empfehlenswert, die Einwilligung des Empfängers zu protokollieren, um die Abgabe der Einwilligung im Streitfall beweisen zu können.

Der Shopbetreiber muss dem Empfänger die Möglichkeit geben, seine Einwilligung jederzeit mit Wirkung für die Zukunft zu widerrufen. Die Ausübung des Widerrufsrechts sollte dem Empfänger dabei so leicht wie möglich gemacht werden. Bereits bei der Erhebung der E-Mail-Adresse sollte ein entsprechender Hinweis auf das Widerrufsrecht vorhanden sein. Darüber hinaus ist es ausreichend, wenn dem Empfänger beispielsweise am Ende eines Newsletters die Möglichkeit gegeben wird, sich durch Anklicken eines Links wieder vom Newsletter abzumelden. Es sollte allerdings darauf geachtet werden, dass der entsprechende Link leicht zu finden und gut lesbar ist.

Datenschutzerklärung – ein Muss, sobald Daten erhoben werden

Eine Datenschutzerklärung ist immer dann erforderlich, wenn bei Aufruf einer Website Daten erhoben werden. Da dies bei jedem Aufruf einer Website der Fall ist, sollte eine Datenschutzerklärung bei keinem Internetauftritt fehlen.

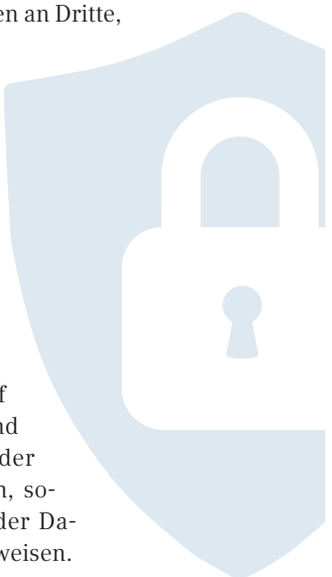
Die Information über die Inhalte hat gemäß § 13 Absatz 1 Satz 1 Telemediengesetz „zu Beginn des Nutzungsvorgangs“ zu erfolgen. Ausreichend dafür ist, dass die Information dem Nutzer direkt bei Aufruf der Website möglich ist. Die Information muss jedoch auch dann möglich sein, wenn ein Nutzer nicht über die Startseite auf die Website gelangt. Es ist daher empfehlenswert, dass die Datenschutzerklärung wie das Impressum von jeder Seite der Website aus erreicht werden können. Das Landgericht Frankfurt a.M. hat in einem Urteil vom 18.02.2014, Az. 3 10 O 86/12 entschieden, dass die Datenschutzerklärung eindeutig gekennzeichnet sein muss. Taugliche Bezeichnungen sind etwa „Datenschutz“, „Datenschutzhinweise“ oder eben „Datenschutzerklärung“. Nicht ausreichend ist es hingegen, die Informationen zum Datenschutz beispielsweise ins Impressum zu integrieren.

Die Ausgestaltung der Datenschutzerklärung ergibt sich aus den Datenerhebungs- und Datenverarbeitungsprozessen.

Die konkrete Ausgestaltung der Datenschutzerklärung hängt im Wesentlichen von den durchgeführten Datenerhebungs- und Datenverarbeitungsprozessen ab. Ein allgemeines Muster, das von jedem Shopbetreiber verwendet werden kann, gibt es daher nicht.

In der Datenschutzerklärung wird der Nutzer über Art, Umfang und Zweck der Erhebung und Verwendung personenbezogener Daten informiert. Insbesondere bei Onlineshops muss der Nutzer erfahren, welche Daten im Bestellvorgang zu welchen Zwecken gespeichert und genutzt werden. Auch über die Weitergabe von Daten an Dritte, wie Versandunternehmen, muss die Datenschutzerklärung informieren.

Hat der Shopbetreiber ein Kontaktformular auf seiner Website, sollte er in der Datenschutzerklärung auch über den Ablauf der Speicherung und der Beantwortung der Anfrage informieren, sowie auf die Dauer der Datenspeicherung hinweisen.



Datenschutz greift auch bei Webanalysetools

Webanalysetools dienen der Überprüfung des Surfverhaltens von Nutzern auf einer Website. Sie untersuchen unter anderem die Anzahl der Nutzer, die Häufigkeit einzelner Seitenaufrufe, die Verweildauer auf einzelnen Seiten sowie die verwendeten Suchbegriffe, die Benutzer von Suchmaschinen auf eine Website geführt haben. Viele Shopbetreiber benutzen Webanalysetools zur Auswertung des Nutzerverhaltens, um auf dieser Grundlage eine Optimierung der Website durchführen zu können.

Bei der Erstellung von Nutzungsprofilen greifen datenschutzrechtliche Bestimmungen. Wer Webanalysedienste auf seiner Website einbindet, haftet für die Einhaltung des deutschen Datenschutzrechts. Insbesondere bei nicht-europäischen Anbietern oder Anbietern, die sich mit ihren Produkten hauptsächlich an den US-amerikanischen Markt wenden, muss der Shopbetreiber als Verwender des Analysetools genau überprüfen, ob die Einhaltung des deutschen Datenschutzrechts sichergestellt werden kann.

Im Jahr 2009 haben die obersten Aufsichtsbehörden für den Datenschutz im

nicht-öffentlichen Bereich Kriterien für den datenschutzkonformen Umgang mit Webanalysetools beschlossen. Ein Analyseprogramm kann ohne Einwilligung durch den Nutzer angewendet werden, soweit die nachfolgenden Kriterien erfüllt werden:

- Abschluss eines Auftragsdatenverarbeitungsvertrages, soweit Daten an Dritte übermittelt werden (§ 11 Bundesdatenschutzgesetz),
- Anonymisierung der IP-Adressen,
- Widerspruchsrecht der Betroffenen,
- Datenschutzhinweis in der Datenschutzerklärung,
- Gegebenenfalls Löschung von Altdaten.

Shopbetreiber zur technischen Sicherung verpflichtet

Durch das am 25.07.2015 in Kraft getretene IT-Sicherheitsgesetz wurde auch die Regelung in § 13 Abs. 7 Telemediengesetz modifiziert. Demnach sind Betreiber von Webangeboten verpflichtet, ausreichende, dem Stand der Technik entsprechende Maßnahmen zum Schutz ihrer Kundendaten und der von ihnen genutzten IT-Systeme zu ergreifen. Shopbetreiber sollten daher ein anerkanntes Verschlüsselungsverfahren implementieren, um die sichere Übermittlung von personenbezogenen Daten gewährleisten zu können.

Social Plugins und datenschutzfreundlichere Lösungen

Social Plugins sind kleine Programme oder Programmpakete, die auf einer Website eingebunden werden, um diese mit sozialen Netzwerken wie Facebook, Twitter, Instagram oder Google Plus zu verbinden. Sofern ein Nutzer auf einer Website den entsprechenden Button anklickt, kann er in seinem jeweiligen Social Media Profil einen Artikel, eine Seite oder ein Produkt teilen, das ihm gefällt.

Viele Shopbetreiber verwenden Social Plugins, da sie über die Social Media Plattformen neue Besucher für ihre Website und damit potenzielle Kunden generieren möchten.

Social Plugins funktionieren dergestalt, dass der Browser des Nutzers bereits bei Aufruf einer Website, die ein solches Plugin enthält, eine direkte Verbindung zu den Servern des jeweiligen Social Media Anbieters herstellt. Hierbei werden Daten des Nutzers von dem fremden Server erfasst. Die jeweiligen Social Media Anbieter erhalten auf diese Weise verschiedene Informationen über den Nutzer und haben die Möglichkeit, das Surfverhalten der Nutzer zu analysieren. Je mehr Webseitenbetreiber das jeweilige Plugin auf ihrer Website integrieren, desto umfassender kann der Social Media Anbieter Nutzerprofile erstellen und diese beispielsweise auch kommerziell für Zwecke der personalisierten Werbung verwenden.

Übertragung persönlicher Daten beginnt mit Einbindung des Social Plugins.

Dem Nutzer wie auch vielen Shopbetreibern ist hierbei oftmals unbekannt, dass bereits allein durch die Einbindung des Social Plugins eine Übermittlung personenbezogener Daten an das jeweilige Soziale Netzwerk stattfindet.

Durch Urteil vom 09.03.2016 hat das Landgericht Düsseldorf (Az. 12 O 151/15 – nicht rechtskräftig) entschieden, dass das Plugin „Gefällt mir“ des sozialen Netzwerks Facebook nicht auf einer Website integriert werden darf, ohne dass die Nutzer

- zuvor über die dadurch veranlasste Datenerhebung und -verwendung aufgeklärt werden,
- in diese eingewilligt haben, und
- über die jederzeitige Widerruflichkeit der Einwilligung informiert sind.

Soweit ein Shopbetreiber nicht ganz auf die Einbindung von Social Plugins verzichten möchte, empfiehlt es sich aber, jedenfalls keine direkte Einbindung von Social Plugins in Websites vorzunehmen. Stattdessen sollte auf datenschutzfreundlichere Alternativlösungen, wie etwa die von Heise entwickelte Sharing-Lösung „Shariff“ oder auf eine einfache Verlinkung zurückgegriffen werden.

Datenschutzverstöße sind abmahnfähig und bußgeldbewährt

Wird der Nutzer einer Website nicht richtig, nicht vollständig oder nicht rechtzeitig über die datenschutzrechtlichen Belange im Zusammenhang mit dem Besuch der Website aufgeklärt, kann der Webseitenbetreiber abgemahnt werden. Darüber hinaus sind die zuständigen Behörden berechtigt, bei Verstößen gegen Vorschriften des Bundesdatenschutzgesetzes gemäß § 43 Bußgelder bis zu 300.000 Euro und bei Verstößen gegen einzelne Verhaltensnormen des Telemediengesetzes gemäß § 16 Bußgelder bis zu 50.000 Euro zu erheben. Um derartige Sanktionen zu vermeiden, sollten die geltenden datenschutzrechtlichen Regelungen eingehalten werden. ■

Tina Weigand
Rechtsanwältin (Syndikusrechtsanwältin)