DATENSCHUTZKONFORME WEBSITES IM SPANNUNGSFELD VON DSGVO, COOKIE-URTEIL UND EPVO:

Nicht mit Kanonen **auf Spatzen schießen**

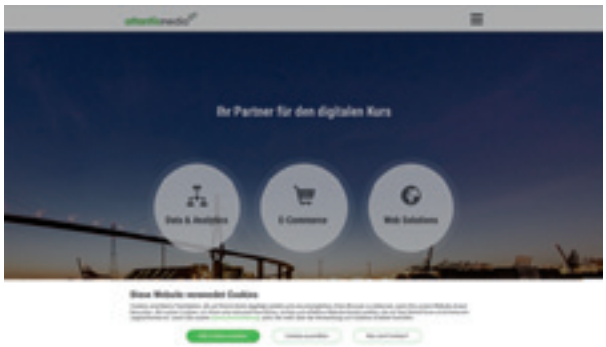
Foto: istock@#Urbanv-Photographer

Personenbezogene Daten im Internet zu schützen, ist eine Herausforderung, für die eine verbindliche Rechtsgrundlage bisher fehlt. Das aktuelle Durcheinander aus ePrivacy-Richtlinie, Cookie-Richtlinie, Telemediengesetz, Datenschutzgrundverordnung, Cookie-Urteil und ePrivacy-Verordnung ruft vielerorts Verunsicherung hervor. Zu groß sind die Interpretationsspielräume für Unternehmen, zu unterschiedlich die sich daraus ergebenden Vorschriften im Umgang mit personenbezogenen Informationen. Unabhängig von der momentanen Situation sollten Unternehmen ihre Corporate Website so aufsetzen, daß sie datenschutzrechtlich auf der sicheren Seite sind … | VON RADEK PALUSZAK

Der juristische Hintergrund der aktuellen Datenschutzdiskussionen ist sehr komplex. Darum lohnt es sich, die verschiedenen Vorgaben zunächst zueinander in Bezug zu setzen. Die ePrivacy-Richtlinie 2002/58/EG (2002) regelt die Verarbeitung personenbezogener Daten und den Schutz der Privatsphäre in der elektronischen Kommunikation. Die Cookie-Richtlinie 2009/136/EG (2009) ergänzt die ePrivacy-Richtlinie: Anbieter müssen Nutzer aufklären, um Cookies auf ihrem Endgerät speichern zu dürfen. In Deutschland hat der Gesetzgeber die Cookie-Richtlinie durch Anpassungen im Telemediengesetz (TMG) umgesetzt: Unternehmen müssen die Nutzer über das Setzen von Cookies nicht nur informieren, sondern auch eine Möglichkeit zum Widerspruch bieten (Opt-out). Die Datenschutzgrundverordnung (DSGVO, 2018) stellt wiederum einen Basisschutz bei der Verarbeitung personenbezogener Daten sicher. »

Gehören Cookies bald der Vergangenheit an?

Ursprünglich sollte die ePrivacy-Verordnung (ePVO) gemeinsam mit der DSGVO in Kraft treten – was nicht gelungen ist, weil sich EU-Parlament, EU-Kommission und EU-Rat bis heute nicht auf einen gemeinsamen Entwurf einigen konnten. Wie bereits die ePrivacy-Richtlinie, soll auch die ePVO personenbezogene Daten in der elektronischen Kommunikation schützen. Dabei stehen Cookies im Zentrum. Um Cookies setzen und Nutzerprofile erstellen zu dürfen, soll der Betroffene aktiv zustimmen müssen (Opt-in) – sofern das Cookie nicht zwingend notwendig ist, um den entsprechenden Service bereitzustellen. Damit konkretisiert die ePVO die teils schwammigen beziehungsweise fehlenden Formulierungen der aktuellen Gesetzgebung im speziellen Bereich der Cookies und der Datenerfassung. Diese Auffassung hat der Europäische Gerichtshof (EuGH) im Oktober 2019 gestärkt. Das vieldiskutierte Cookie-Urteil verbietet Cookie Consent Banner: Sie informieren Nutzer lediglich darüber, daß der Website-Betreiber Cookies setzt. Auch das Zustimmungsfeld bereits mit einem Haken vorauszufüllen, den der Besucher dann entfernen muß, ist nicht mehr erlaubt.



„Sobald Nutzer eine Website besuchen, sollte ein gut sichtbares Banner erscheinen, das sich idealerweise in das Corporate Design der Seite harmonisch einfügt und das Nutzer als organischen Bestandteil der Seite wahrnehmen."

Besucher verständlich aufklären

Um nicht gegen geltendes Recht zu verstoßen und damit empfindliche Bußgelder zu riskieren, sollten Unternehmen besser gestern als morgen aktiv werden. Eine Maßnahme, die sich recht einfach umsetzen läßt, ist die rechtskonforme Gestaltung des Cookie-Banners. Sobald Nutzer eine Website besuchen, sollte ein gut sichtbares Banner erscheinen, das sich idealerweise in das Corporate Design der Seite harmonisch einfügt und das Nutzer als organischen Bestandteil der Seite wahrnehmen. Erfahrungsgemäß erhöht das die Bereitschaft, dem Setzen von Cookies zuzustimmen. Der Text des Banners sollte zum einen verständlich erklären, warum das Unternehmen Cookies setzen möchte. Zum anderen muß der Besucher die Möglichkeit erhalten, seine Einstellungen individuell anzupassen. Daneben ist die Datenschutzerklärung direkt im Cookie Banner zu verlinken. Dort sollten User das Banner nachträglich noch einmal aufrufen können, um die ursprüngliche Konfiguration zu ändern.

Aller guten Cookies sind drei

Natürlich wollen Unternehmen, daß Nutzer möglichst viele Cookies erlauben (Opt-in). Darum darf es durchaus einfacher sein, den „Akzeptieren"-Button im Banner zu klicken, als die Cookie-Einstellungen zu konfigurieren. Doch Vorsicht: Nutzern eine umfangreiche Liste mit allen eingesetzten Tracking- und Analyse-Tools zu präsentieren oder sie aufzufordern, ihre Cookie-Einstellungen im Browser anzupassen, wirkt sehr abschreckend. Besser ist es, wenige Auswahlmöglichkeiten zu geben und diese kurz zu erklären: Wesentliche Cookies stellen die Funktionalität der Website sicher und lassen sich darum nicht deaktivieren. Funktionelle Cookies dienen dazu, die Website-Nutzung zu analysieren und so ihre Performance sowie Funktionalität kontinuierlich zu verbessern. Marketing-Cookies wiederum sind notwendig, um Benutzerprofile zu erstellen und – auf dieser Basis – personalisierte Werbeinhalte anzuzeigen. Im Hinblick auf das Cookie-Banner sind viele Unternehmen verunsichert.

Mehr als ein Banner mit übersichtlichen Auswahlmöglichkeiten braucht es üblicherweise nicht. Und manchmal nicht einmal das. Weil die Rechtslage so undurchsichtig ist, wollen manche Unternehmen ein unnötig umfangreiches und damit kostspieliges Banner ausspielen, obwohl sie gar keine oder nur wesentliche Cookies setzen. Für beide braucht es kein Banner. Beispiele sind unter anderem technisch erforderliche Session-Cookies zur Speicherung der Spracheinstellung oder Warenkorb-Cookies. Ohne sie wäre es nicht möglich, die gewünschten Artikel im Warenkorb anzuzeigen – eine unverzichtbare Grundfunktion jedes Onlineshops.

Datenkraken die Stirn bieten

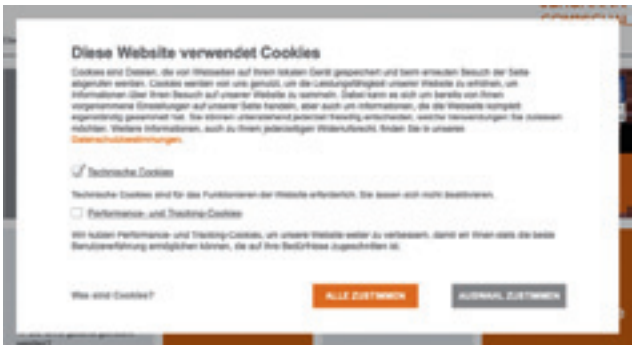
Ebenso wichtig wie Cookie-Banner, aber ungleich komplexer, ist es, Inhalte von Drittanbietern in eine Website zu integrieren und dabei einen rechtskonformen Umgang mit personenbezogenen Daten sicherzustellen. Um Website-Inhalte auf Social-Media-Plattformen liken und teilen zu können, übertragen die Buttons bei jedem Seitenaufruf sensible Nutzerdaten über das Surfverhalten an den Betreiber des jeweiligen Social Netzworks – unabhängig davon, ob der User Mitglied des Netzwerks beziehungsweise eingeloggt ist. Die über Embedded Cookies erhobenen Nutzerdaten fließen in der Regel an US-amerikanische Server – wo sie nicht mehr dem europäischen Datenschutz unterliegen.

Was viele nicht wissen: Website-Betreiber können diese Datensammlung unterbinden. Unternehmen, die zum Beispiel das quelloffene Content-Manage-

ment-System (CMS) TYPO3 einsetzen, müssen Tracking-Mechanismen aktiv hinzufügen. Seit Version 9 werden in der Standard-Installation keine Cookies mehr gesetzt. Aber auch Unternehmen mit einem anderen CMS sind der Sammelwut von Datenkraken nicht schutzlos ausgeliefert.

Die Privatsphäre der Nutzer schützen

Es gibt nämlich Tools, welche die Privatsphäre von Website-Besuchern schützen. Sobald Like- und Share-Buttons in eine Website integriert sind, erfassen üblicherweise Social Plug-ins die IP-Adresse des Nutzers, um seine weiteren Aktivitäten zu protokollieren – auch dann, wenn er die Buttons nicht klickt. Entsprechende Tools hingegen stellen den Kontakt zwischen Social Network und Besucher erst beim Klicken des Buttons her. Damit hinterlassen Nutzer keine ungewollte digitale Spur, und soziale Netzwerke können keine kompletten Surf-Profile erstellen. Andere Tools erlauben, Videos datenschutzkonform in eine Website einzubinden. Auch wenn ein Video direkt in das jeweilige Social Network eingebettet ist, erfolgt der Datentransfer im Hintergrund über den Server des Website-Betreibers. Der Video-Dienst erhält damit nur dessen Daten, nicht aber die des Besuchers.



Manchmal sind zwei Klicks besser als einer

Ein Dienst, der diese Tools noch nicht unterstützt, ist Google Maps. Um dennoch zu verhindern, daß Google Nutzerdaten erfaßt, kommen Website-Betreiber um eine Zwei-Klick-Lösung nicht herum. Der Nutzer muß zwei Klicks tätigen, um ein Web-Angebot zu nutzen – was etwas weniger komfortabel ist. Um sich den Standort eines Unternehmens bei Google Maps anzeigen zu lassen oder eine Wegbeschreibung abzurufen, erscheint bei einer Zwei-Klick-Lösung zunächst ein kleines Banner. Es weist den Besucher darauf hin, daß er den Datenschutzbestimmungen des Anbieters, in diesem Fall Google, zustimmen muß, um die interaktive Karte zu nutzen. Erst im Anschluß erfolgt der Datentransfer.

Radek Paluszak ist Head of Web Solutions bei atlantis media, einem Hamburger IT-Dienstleister im Bereich Digitalisierung (Bilder: Atlantismedia)

Nicht über's Ziel hinausschießen

Wofür sich ein Unternehmen entscheidet, ist eine höchst individuelle Angelegenheit. Aufgrund der Komplexität ist die professionelle Beratung durch einen auf Datenschutz spezialisierten Anwalt unerläßlich – ebenso wie eine Bedarfsanalyse, die ein erfahrener IT-Dienstleister durchführt. Im Mittelpunkt stehen dabei drei Fragen: Welche Dritt-Technologie setzt ein Unternehmen ein? Woher stammen diese Lösungen? Und garantieren sie nachweislich einen hierzulande als rechtskonform geltenden Umgang mit personenbezogenen Daten?

Weiterhin wichtig sind die Fragen: Braucht es Google Analytics? Und welche Daten zu erheben, ist generell sinnvoll? Erfahrungsgemäß ist das Tracking der größte Knackpunkt. Einige Nutzer sind inzwischen für das Thema Datenschutz sensibilisiert und darum zu keinem Opt-in bereit.

Andere sind genervt und stimmen dem Setzen von Cookies zu, ohne sich über die Auswirkungen bewußt zu sein. Ein seriöser IT-Dienstleister weist Unternehmen auf die rechtliche Uneindeutigkeit und das damit verbundene Risiko hin. Er sollte für das Thema Datenschutz sensibilisieren, ohne Ängste zu schüren. In der Praxis müssen Unternehmen bei ihrer Corporate Website die richtige Balance zwischen Datenschutz und Usability finden. Und dabei gilt: Nicht mit Kanonen auf Spatzen schießen.

Noch Fragen?
www.atlantismedia.de

IMPRESSUM

Computern im Handwerk/ handwerke.de
gegründet 1984, dient als unabhängiges Fachmagazin für moderne Kommunikation den Betrieben der **Bauhaupt- und Nebengewerbe** im „portionierten" Wissens- und Technologie-Transfer.

Herausgeber: Horst Neureuther

© Copyright: CV München
CV Computern-Verlags GmbH
Goethestraße 41, 80336 München

Telefon 0 89/54 46 56-0
Telefax 0 89/54 46 56-50
Postfach 15 06 05, 80044 München
E-Mail: info@cv-verlag.de
redaktion@cv-verlag.de
www.handwerke.de

Geschäftsleitung:
Dipl.-Vw. H. Tschinkel-Neureuther

Anzeigenleitung:
Dipl.-Vw. Heide Tschinkel-Neureuther
e-mail: anzeigen@cv-verlag.de

Redaktion und redaktionelle Mitarbeiter in dieser Ausgabe:
Heike Blödorn, Helene-Monika Filiz, Daniel Knep, Prof. em. Dr. Klaus Kruczynski, Margrit Lingner, Horst Neureuther (verantw.), Radek Paluszak, Stéphane Paté, Myrko Rudolph, Gundo Sanders, Stefan Wehrhahn

Anzeigenvertretung:
Medienmarketing SANDERS
Tel. 0 72 03/50 27 270
Mail: gsanders@mm-sanders.de

Layout:
AD&D Werbeagentur GmbH,
Silvia Romann, Dietmar Kraus

Druck:
Walstead NP Druck GmbH, St. Pölten

Druckauflage: 52.500
Tatsächliche Verbreitung: 51.285 (II/20)

Auflage und Verbreitung kontrolliert.

36. Jahrgang
Erscheinungsweise: 10 x jährlich

Abo-Preis:
29,– € p.a. plus Porto inkl. MwSt.

Einzelpreis: 2,90 €
Ein Abonnement verlängert sich automatisch um ein Jahr, wenn es nicht spätestens 3 Monate vor Ablauf des Bezugszeitraumes gekündigt wird.

ISSN 0931-4679
Mitglied der Informationsgemeinschaft zur Feststellung der Verbreitung von Werbeträgern e.V. (IVW) Berlin

Zur Zeit gilt die Anzeigenpreisliste Nr. 37 vom 01.11.2019.

Titelkopf: © Fotolia.de/yellowj