von Rechtsanwalt **Jan Lennart Müller**

DSGVO in der Praxis: Benötigen Sie einen Cookie-Banner?

Nicht erst seit Geltung der DSGVO haben die Cookie-Banner auf Websites enorm zugenommen. Ein Grund für das massenhafte Vorkommen ist die aktuelle Rechtsunsicherheit zu diesem Thema. Die Unsicherheit rund um das Thema Cookie-Banner ist mit der DSGVO nicht ausgeräumt worden. Die DSGVO sieht keine eindeutige Regelung zu Cookie-Bannern vor. Was bedeutet die sog. Cookie-Richtlinie und die zukünftige ePrivacy-Verordnung für Cookie-Banner in diesem Zusammenhang? Benötigen Website-Betreiber und Online-Händler ein solches Cookie-Banner (jetzt oder in Zukunft)? Hierüber soll unser heutiger Beitrag aufklären.

Was sind Cookies?

Bei Cookies handelt es sich um kleine Textdateien, die auf dem Endgerät des Seitenbesuchers abgelegt werden. Cookies dienen unter anderem dazu, durch Speicherung von Einstellungen den Bestellprozess zu vereinfachen (z.B. Merken des Inhalts eines virtuellen Warenkorbs für einen späteren Besuch auf der Website). Später können diese lokal abgelegten Textdateien dann vom selben Webserver, von dem sie abgelegt wurden, auch wieder ausgelesen werden. Darüber hinaus können Cookies z.B. auch zu statistischen Analysezwecken (Webanalyse) oder für bedarfsgerechte Werbung (Re-Targeting bzw. Re-Marketing) verwendet werden.

Welche Arten von Cookies es gibt:

Einige Cookies werden nach dem Ende einer Browser-Sitzung, also nach Schließen des Browsers, wieder gelöscht (sog. Sitzungs-Cookies). Andere Cookies verbleiben auf dem Endgerät und ermöglichen den Browser beim nächsten Besuch wiederzuerkennen (persistente Cookies).

Nach den Domains, zu der die Cookies gehören wird unterschieden nach

- Erstanbieter-Cookies (first-party cookies), die vom Webserver der besuchten Seite gesetzt werden und dieselbe Domain verwenden und
- Cookies von Drittanbietern (third-party cookies), die von einer anderen Domain als der Domain der besuchten Seite gespeichert werden. Dies liegt dann vor, wenn die Website auf eine Datei verweist, z. B. JavaScript, die sich außerhalb der Domain befindet.

Ist ein Cookie überhaupt datenschutzrechtlich relevant?

Cookies sind datenschutzrechtlich relevant, wenn diese personenbezogene Daten darstellen. Was personenbezogene Daten sind, bestimmt Art. 4 Nr. 1 DSGVO:

> *"Im Sinne dieser Verordnung bezeichnet der Ausdruck:*
> *1. "personenbezogene Daten" alle Informationen, die sich auf eine identifizierte oder identifizierbare natürliche Person (im Folgenden "betroffene Person") beziehen; als identifizierbar wird eine natürliche Person angesehen, die direkt oder indirekt, insbesondere mittels Zuordnung zu einer* **Kennung** *wie einem Namen, zu einer Kennnummer, zu Standortdaten, zu einer Online-Kennung oder zu einem oder mehreren besonderen Merkmalen identifiziert werden kann, die Ausdruck der physischen, physiologischen, genetischen, psychischen, wirtschaftlichen, kulturellen oder sozialen Identität dieser natürlichen Person sind;"*

(Hervorhebung durch den Zitierenden)

Gemäß dem zweiten Halbsatz fallen **sog. "Kennungen"** ebenfalls unter den Begriff der personenbezogenen Daten. Hierunter fallen auch Online-Kennungen (wie eben Cookies). Nach Erwägungsgrund 30 der DSGVO wird klar, dass der Gesetzgeber Cookies als personenbezogene Daten ansieht:

> *"Natürlichen Personen werden unter Umständen Online-Kennungen wie IP-Adressen und Cookie-Kennungen, die sein Gerät oder Software-Anwendungen und -Tools oder Protokolle liefern, oder sonstige Kennungen wie Funkfrequenzkennzeichnungen zugeordnet. Dies kann Spuren hinterlassen, die insbesondere in Kombination mit eindeutigen Kennungen und anderen beim Server eingehenden Informationen dazu benutzt werden können, um Profile der natürlichen Personen zu erstellen und sie zu identifizieren."*

Die Folge: Werden auf oder über eine Website personenbezogene Daten **verarbeitet**, ist dies nach dem sog. Verbotsprinzip der DSGVO **nur zulässig**, wenn einer der **Erlaubnistatbestände** die jeweilige Datenverarbeitung legitimiert.

Demnach ist die Verwendung von Cookies nur dann rechtmäßig, wenn die DSGVO dies erlaubt.

Exkurs zur zukünftigen Rechtslage (ePrivacy-Verordnung):

Die europäische ePrivacy-Verordnung ist als Ergänzungsakt und Spezialgesetz zur Datenschutz-Grundverordnung für Bereiche der internetbasierten Kommunikation konzipiert und soll so spezifische Maßstäbe und Regeln für den Umgang mit personenbezogenen Daten für bestimmte Nutzungsbereiche des Internets aufstellen. Hierbei sollen der Mailverkehr, das Instant-Messaging, der Webseiten-Zugang, die Internettelefonie, aber auch die Verwendung von Tracking- Cookies näher geregelt werden. Fraglich bleibt allerdings in diesem Zusammenhang schon, was der Gesetzgeber unter "Tracking-Cookies" konkret versteht bzw. welche Arten von Cookies hierunter fallen werden.

Nach dem derzeitigen Stand beabsichtigt die ePrivacy-Verordnung, dass der Nutzer beim Einsatz von Tracking-Cookies über Zweck und Anwendungsbereich aller eingesetzten Cookies informiert werden muss. Zudem soll der Nutzer über den Zweck und den Anwendungsbereich der eingesetzten Tracking-Cookies und über die Möglichkeiten informiert werden, den Einsatz von solchen Cookies zu begrenzen oder ganz zu blockieren. Ferner soll der Nutzer **vor** dem Einsatz von Tracking-Cookies seine Einwilligung notwendigerweise erteilen.

Der erste Entwurf der ePrivacy-Verordnung wurde durch die EU-Kommission bereits im Januar 2017 eingebracht und sollte bereits Mitte 2018 in Kraft treten. Es war bald zu erkennen, dass dieser Zeitplan zu ambitioniert war. Die Verhandlungen zwischen EU-Parlament, EU-Kommission und dem EU-Ministerrat sind zurzeit festgefahren. Es besteht insbesondere Streit, ob und inwieweit die vorherige Einwilligung des Nutzers zum Einsatz von sog. Tracking-Cookies erforderlich und ob nicht eine pauschale Einwilligung ausreichend ist. Es ist noch nicht abzusehen, wann sich EU-Parlament, EU-Kommission und EU-Ministerrat über einen gemeinsamen Verordnungstext einigen.

Tipp: Mehr zum Thema ePrivacy-Verordnung können Sie **diesem Beitrag** nachlesen.

Was ist aber mit der Widerspruchs-Lösung nach § 15 Abs. 3 TMG, gilt dieser denn gar nicht (mehr)?

Man könnte annehmen, dass einem evtl. § 15 Abs. 3 TMG aus der Zwickmühle helfen könnte, denn nach dieser Vorschrift genügt ein einfaches Opt-Out (Widerspruch). Aber gilt § 15 Abs. 3 TMG überhaupt noch? Dies wird kontrovers diskutiert.

Wie viele Bestimmungen des DSGVO ist auch der Art. 95 alles andere als klar formuliert. Dem Wortlaut des ersten Halbsatzes nach soll "natürlichen (oder juristischen) Personen in Bezug auf die Verarbeitung in Verbindung mit der Bereitstellung öffentlich zugänglicher elektronischer Kommunikationsnetze in der Union keine zusätzlichen Pflichten (auferlegt werden)". Spezielle datenschutzrechtliche Pflichten der ePrivacy-Richtlinie 2002/58/EG ("Cookie-Richtlinie") oder genauer gesagt, Pflichten, die aus der Umsetzung dieser Richtlinie erwachsen, würden damit jenen der DSGVO vorgehen (s. Kommentar Gola, Art. 95 Rdr. 4 ff).

Gilt das auch für § 15 Abs. 3 TMG, der bei Verwendung von Cookies die Möglichkeit des Widerspruchs vorsieht?

Hier fangen die Schwierigkeiten an.

Art. 5 Abs. 3 Cookie-Richtlinie, der den Einsatz von Cookies regelt, bezieht sich gerade nicht auf die Betreiber öffentlich zugänglicher elektronischer Kommunikationsdienste, sondern auf jede Person, die Informationen auf Endgeräte überträgt oder auf diesen Geräten liest (Gola, a.a.O.). Weiterhin ist der zweite wenig verständliche Halbsatz des Art. 95 DSGVO zu berücksichtigen. Demnach gilt der Vorrang der Cookie-Richtlinie oder der Vorschriften zur nationalstaatlichen Umsetzung nur, soweit die natürlichen Personen "besonderen in der Cookie-Richtlinie festgelegten Pflichten unterliegen, die dasselbe Ziel erfolgen". Zusätzliche Unsicherheit erwächst aus dem Umstand, dass Art. 5 Abs. 3 Cookie-Richtlinie gar nicht in deutsches Recht umgesetzt wurde, da wie oben ausgeführt nach Auffassung der Bundesregierung deutsches Recht bereits vor Inkrafttreten der Cookie-Richtlinie die Frage der Einwilligungspflicht bei Verwendung von Cookies abdeckt. Es besteht daher keine Klarheit darüber, ob § 15 Abs. 3 TMG als Umsetzung der Cookie-Richtlinie den Regelungen der DSGVO vorgeht (s. Gola, Art. 95, Rndr. 18).

Hinweis für die Praxis: Es ist daher sicherer, nicht auf die weiterbestehende Vorrangigkeit des § 15 Abs. 3 TMG zu vertrauen.

Tipp: Nähere Informationen zum Thema Cookie-Richtlinie und § 15 Abs. 3. TMG können Sie **hier** nachlesen.

Wie kann der Einsatz von Cookies gerechtfertigt werden?

Werden personenbezogene Daten der Website-Besucher über Cookies verarbeitet, kommen in der Regel nur die Erlaubnistatbestände des

- Art. 6 Abs.1 lit. a) DSGVO (Einwilligung der betroffenen Person) oder
- Art. 6 Abs.1 lit. f) DSGVO (Berechtigte Interessen der verantwortlichen Stelle)

in Betracht.

Kann der Einsatz von Cookies über die "berechtigten Interessen" gerechtfertigt werden?

Wenn man davon ausgeht, dass cookiebasiertes Drittanbieterwerkzeuge über berechtigte Interessen legitimiert werden können, dürfen diese gesetzt werden **ohne** dass der Nutzer vorher seine **Einwilligung** hierzu erteilen muss. Für die Frage, ob cookiebasiertes Tracking oder Targeting über berechtigte Interessen im Sinne des Art. 6 Abs.1 lit.f DSGVO legitimiert werden kann oder eine Einwilligung (Opt-In) im Sinne des Art. 6 Abs.1 lit.a DSGVO notwendig ist, hängt von einer Abwägung der Interessen des Webseitenbetreibers mit denen der Besucher und deren berechtigten Nutzererwartung ab.

Nach Erwägungsgrund 47 DSGVO, welcher Direktmarketing ausdrücklich als mögliches berechtigtes Interesse nennt und Art. 21 Abs.1 Satz 1 DSGVO, der ein Widerspruchsrecht für Werbeprofiling vorsieht, liegt die Annahme nahe, dass auch Tracking und Targeting - je nach "Eingriffsintensität" und Erwartbarkeit - auch über berechtigte Interessen legitimiert werden können.

Danach sprechen gute Argumente für eine Rechtfertigung von (Tracking- und Targeting-) Cookies über die berechtigten Interessen gemäß Art. 6 Abs. 1 lit. f DSGVO.

DSK fordert allerdings Einwilligung bei Tracking- und Targeting-Cookies

Die Datenschutzkonferenz (DSK) ist die Konferenz der unabhängigen Datenschutzbehörden des Bundes und der Länder, also ein informeller Kreis der deutschen Datenschutzaufsichtsbehörden. Die DSK veröffentlichte am 26.04.2018 eine Positionsbestimmung "Zur Anwendbarkeit des TMG für nicht-öffentliche Stellen ab dem 25. Mai 2018", welche **hier** abgerufen werden kann.

Die DSK vertritt in seinem Positionspapier die Auffassung, dass die Norm des § 15 Abs. 3 TMG nach der DSGVO keine Anwendung mehr findet, dies begründet die DSK wie folgt:

"6. Als Rechtsgrundlage für die Verarbeitung personenbezogener Daten durch Diensteanbieter von Telemedien kommt folglich nur Artikel 6 Absatz 1, insbesondere Buchstaben a), b) und f) DSGVO in Betracht. Darüber hinaus sind die allgemeinen Grundsätze aus Artikel 5 Absatz 1 DSGVO, sowie die besonderen Vorgaben z. B. aus Artikel 25 Absatz 2 DSGVO einzuhalten.7. Verarbeitungen, die unbedingt erforderlich sind, damit der Anbieter den von den betroffenen Personen angefragten Dienst zur Verfügung stellen kann, können ggf. auf Art. 6 Absatz 1 Buchstabe b) oder Buchstabe f) DSGVO gestützt werden.8. Ob und inwieweit weitere Verarbeitungstätigkeiten rechtmäßig sind, muss durch eine Interessenabwägung im Einzelfall auf Grundlage des Artikel 6 Absatz 1 Buchstabe f) DSGVO geprüft werden."

Soweit erst einmal nichts neues, ABER:

Für Furore sorgt nun Ziffer 9 des DSK-Positionspapiers: Hier teilt die DSK mit, unter welchen Voraussetzungen ein Tracking unter Geltung der DSGVO zulässig sein soll:

> *"9. Es bedarf jedenfalls einer vorherigen Einwilligung beim Einsatz von Tracking- Mechanismen, die das Verhalten von betroffenen Personen im Internet nachvollziehbar machen und bei der Erstellung von Nutzerprofilen. Das bedeutet, dass eine informierte Einwilligung i. S. d. DSGVO, in Form einer Erklärung oder sonstigen eindeutig bestätigenden Handlung vor der Datenverarbeitung eingeholt werden muss, d. h. z. B. bevor Cookies platziert werden bzw. auf dem Endgerät des Nutzers gespeicherte Informationen gesammelt werden."*

Zur Begründung dieser Rechtsansicht führt die DSK an:

Diese Auffassung steht im Einklang mit dem europäischen Rechtsverständnis zu Artikel 5 Absatz 3 der ePrivacy-Richtlinie. Im überwiegenden Teil der EU-Mitgliedsstaaten wurde die ePrivacy-Richtlinie vollständig in nationales Recht umgesetzt oder die Aufsichtsbehörden fordern schon heute ein "Opt-in" entsprechend Artikel 5 Absatz 3 der Richtlinie.
Da die Verweise in der ePrivacy-Richtlinie auf die Datenschutzrichtlinie gemäß Artikel 94 Absatz 2 DSGVO als Verweise auf die DSGVO gelten, muss eine Einwilligung i. S. d. ePrivacy- Richtlinie europaweit ab dem 25.05.2018 den Anforderungen an eine Einwilligung nach der DSGVO genügen.
Um in Zukunft einen einheitlichen Vollzug europäischen Datenschutzrechts zu gewährleisten, muss sichergestellt werden, dass auch Verantwortliche in Deutschland diese datenschutzrechtlichen Anforderungen umsetzen.
Dieses Papier wird unter Berücksichtigung der Entwicklungen auf europäischer Ebene fortgeschrieben.

Die Konsequenz aus dieser Auffassung der DSK wäre, dass Tracking-Maßnahmen wie z.B. von Google Analytics, Matomo, Retargeting, etc. nur noch dann angewendet werden könnten, wenn der betroffene Seitenbesucher hierzu eine Einwilligung erteilt.

Hierbei dürfte es für den Seitenbetreiber (allen voran Online-Händler) allerdings oftmals schwer zu erfüllen sein, für alle Trackingmaßnahmen eine informierte Einwilligung des betroffenen Seitenbesuchers einzuholen, denn: Art. 7 DSGVO stellt hohe Anforderungen an das Kriterium der Informiertheit im Rahmen einer wirksamen Einwilligung.

Zudem müsste beachtet werden, dass eine Einwilligung freiwillig erteilt werden muss. Von einer Freiwilligkeit ist dann nicht auszugehen, wenn die Einwilligung gegen das sog. Kopplungsverbot verstoßen würde.

Ferner dürften entsprechende Cookies für Tracking-Maßnahmen nicht automatisch beim Seitenbesuch geladen werden, sondern dürften erst nach Erteilung der Einwilligung des Betroffenen dynamisch nachgeladen werden. Dies würde viele Internetseitenbetreiber zudem vor erhebliche technische Probleme stellen.

Kritik an der Rechtsauffassung der DSK:

Folgende Argumentationspunkte sprechen gegen die Rechtsauffassung der DSK und gegen die Notwendigkeit der Einholung einer Einwilligung für Tracking-Maßnahmen:

- In Erwägungsgrund 47 zur DSGVO ist niedergelegt, dass das Direktmarketing mit berechtigten Interessen gerechtfertigt werden kann. Wenn aber das Direktmarketing über die berechtigten Interessen gerechtfertigt werden kann, dann muss dies erst recht für Tracking-Maßnahmen als bloße Vorstufe zur Direktwerbung gelten;
- Der aktuelle Entwurf der EU-Kommission zur E-Privacy-Verordnung sieht gerade eine Privilegierung für die Messung von Websitebesuchern vor (Art. 8 Abs. 1 lit. d E-Privacy-Verordnungsentwurf), eine Einwilligung wird hier gerade nicht zur Voraussetzung gemacht;
- Auch hatte die Artikel 29-Datenschutzgruppe in der Vergangenheit ein Tracking nach § 15 Abs. 3 TMG nicht als riskant eingestuft und keinerlei Ausführungen in Richtung Einwilligung getätigt (Stellungnahme 04/2012);

Lösungsvorschläge für die Praxis:

Wie sollte man in der Praxis mit Cookies aufgrund der unterschiedlichen juristischen Ansichten umgehen?

Wahl der Rechtsgrundlage

Zunächst muss man sich überlegen, auf welche Rechtsgrundlage man die Verwendung von Cookies stützen möchte:

- Folgt man dem Verständnis der Datenschutzbehörden und wählt damit den sichersten Weg, dürfte jede Form von cookiebasiertem Tracking und Targeting nur dann eingesetzt werden, wenn der betroffene Nutzer vorher in das Setzen eben dieser Cookies (über einen entsprechenden Cookie-Banner) **eingewilligt** hat (Art. 6 Abs. 1 lit. a DSGVO). Für alle anderen Cookies könnte der Erlaubnistatbestand der "berechtigten Interessen" herangezogen werden.
- Wählt man einen risikobasierten Ansatz wird keine Einwilligung (über einen Cookie-Banner) eingeholt, es würde dann genügen, wenn man die Verwendung auf die "berechtigten Interessen" nach Art. 6 Abs.1 lit. f DSGVO stützt. Wählt man diesen Ansatz kann zusätzlich ein Cookie-Banner verwendet werden, mit welchem auf die Verwendung von Cookies informiert wird, zudem ein Hinweis au die Widerspruchsmöglichkeiten innerhalb der Datenschutzerklärung. In diesem Fall stützt man den Einsatz

von Cookies auf die "berechtigten Interessen" nach Art. 6 Abs.1 lit. f DSGVO.

Hinweis: Unabhängig davon, für welchen Weg man sich entscheiden möchte gilt: Unabdingbar ist eine **Datenschutzerklärung** mit speziellen Klauseln zum Einsatz von Cookies!

Cookie-Banner verwenden - Ja oder nein?

Lösungsmöglichkeit 1: Cookie-Banner zum Einholen einer Einwilligung

Wenn Sie die Verwendung von Tracking- und Targeting-Cookies auf eine Einwilligung stützen möchten, müssen Sie ein Cookie-Banner mit einem entsprechenden Einwilligungstext verwenden. Der Einwilligungstext für die Cookie-Nutzung sollte so konkret wie möglich sagen, um welche Daten es geht, wozu diese genutzt werden und an wen diese Daten zu welchem Zweck gegebenenfalls weiter gegeben werden. Der Nutzer muss diesen Text mit einem Klick bestätigen können.

Zudem dürfen Tracking- und Targeting-Cookies erst dann bei Seitenbesuchern gespeichert werden, wenn diese über die Cookies aufgeklärt worden sind und sich mit ihnen einverstanden erklärt haben. Es muss also dafür gesorgt werden, dass die Cookies dynamisch nachgeladen werden, nachdem (!) der Seitenbesucher seine Einwilligung erteilt hat.

WICHTIGER HINWEIS: Wenn Sie die Dienste "Google Adsense" und "Google Ad Manager" oder "Facebook Custom Audience über das Pixel-Verfahren im erweiterten Abgleich" verwenden, müssen Sie eine Einwilligung des Seitenbetreibers einholen! Mehr Informationen erhalten Sie **für die Google Dienste hier** und für Facebook **hier**.

Risikoeinschätzung: Kein Risiko.

Die IT-Recht Kanzlei wird für diesen Fall in Kürze passende Datenschutzklauseln für diverse Tracking- und Targeting-Anbieter mit der Einwilligungslösung zur Verfügung stellen - hierzu informieren wir unsere Mandanten noch gesondert! Zudem werden wir auch eine Musterformulierung für einen Cookie-Banner mit Einwilligungs-Lösung bereitstellen.

Lösungsmöglichkeit 2: Cookie-Banner als bloßer Hinweis auf die Verwendung von Cookies

Sie informieren den Seitenbesucher beim ersten Seitenaufruf über das Verwenden von Cookies und das Widerspruchsrecht (Cookie Banner), welches näher in der Datenschutzerklärung bezeichnet ist. Des Weiteren verzichten Sie aber auf die Erteilung einer Einwilligung des Seitenbesuchers.

Risikoeinschätzung: Im Augenblick gering. Die weitere Entwicklung sollte allerdings genau beobachtet werden.

Mandanten der IT-Recht Kanzlei können in der Handlungsanleitung zur Datenschutzerklärung eine Musterformulierung für einen solchen Cookie-Banner abrufen!

Die IT-Recht Kanzlei rät derzeit diesen Mittelweg zu beschreiten, solange keine anderslautende Rechtsprechung ergeht - die weitere Entwicklung der Rechtsprechung zu diesem Thema behält die IT-Recht Kanzlei für ihre Mandanten genauestens im Auge!

Lösungsmöglichkeit 3: Keine Verwendung eines Cookie-Banners

Wenn Sie weder die Dienste "Google Adsense" und "Google Ad Manager", noch "Facebook Custom Audience über das Pixel-Verfahren im erweiterten Abgleich" verwenden, könnte auf den Einsatz eines Cookie-Banners auch komplett verzichtet werden.

Risikoeinschätzung: Mittel. Stellen Sie sich allerdings dem Grunde nach darauf ein, dass eine Cookie-Banner-Pflicht mit Geltung der ePrivacy-Verordnung bevorstehen könnte!

Wichtig: Was Sie bei der Platzierung des Cookie-Banners beachten müssen!

Achten Sie unbedingt auf die genaue Platzierung des Cookie-Banners auf der Website. Das Cookie-Banner darf keine anderen (Pflicht-)Informationen, die dem Nutzer zwingend zur Verfügung zu stellen sind, verdecken oder den Zugang zu diesen blockieren. Das Cookie-Banner darf daher z.B. nicht den Zugang zu Ihrem Impressum oder der Datenschutzerklärung der Website verdecken, da diese Pflichtangaben jederzeit verfügbar und leicht einsehbar sein müssen!

Zusammenfassung

Es wird noch lange keine Ruhe im Thema Cookie-Verwendung einkehren. Spätestens mit der zukünftigen ePrivacy-Verordnung werden Website-Betreiber sich verstärkt mit dem Thema der Cookie-Verwendung auseinander setzen müssen!

Bis dahin gilt: Auch die Verwendung von cookiebasierten Tracking- und Targeting-Maßnahmen ist in Zeiten der DSGVO äußerst umstritten. Fraglich ist bereits heute, ob derartige Maßnahmen über die sog. "berechtigten Interessen" (Art. 6 Abs.1 lit. f DSGVO) gerechtfertigt werden können oder hierzu (gemäß der Auffassung der DSK) verpflichtend eine Einwilligung (Art. 6 Abs. 1 lit. a DSGVO) des betroffenen Seitenbesuchers eingeholt werden muss. Es wird hier allerdings nicht eine deutsche Rechtsauffassung, sondern eine einheitliche europäische Auslegung der DSGVO-Grundsätze maßgeblich zugrunde zu legen sein.

Wer bis zur Geltung der ePrivacy-Verordnung den sichersten Weg gehen möchte, verwendet Tracking- und Targeting-Cookies nur nach vorheriger Einwilligung des Seitenbesuchers.

Die IT-Recht Kanzlei hält es derzeit allerdings für vertretbar, die Verwendung einer Vielzahl von Tracking- und Targeting-Cookies (nach Durchführung einer persönlichen Risikoabwägung) über den Erlaubnistatbestand der "berechtigten Interessen" zu verwenden und hierzu einen entsprechenden (bloßen) Cookie-Hinweis auf der Seite zu platzieren. Sollte sich die Rechtsprechung oder die Gesetzgebung in eine andere Richtung entwickeln, werden wir hierzu selbstverständlich informieren!

Autor:
RA Jan Lennart Müller
Rechtsanwalt