

# DATENSCHUTZ- BERATER

» Ihr zuverlässiger Partner für Datenschutz und Datensicherheit

**Chefredakteur: Dr. Carlo Piltz**

**Schriftleitung: Dr. Alexander Golland, Tilman Herbrich, Philipp Quiel, Laurenz Strasse Meyer**

## Editorial

Dr. Alexander Golland

**Geschenke aus Berlin und Brüssel (nicht nur zu Weihnachten)**

Seite 337

## Stichwort des Monats

Dr. Gregor Scheja

**Virtual Voice Assistants (VVA) – ist der Einsatz von Sprachassistent ohne Einwilligungserklärung möglich?**

Seite 338

## Datenschutz im Fokus

Corinna Bernauer

**Dürfen Arbeitgeber nach dem Impfstatus von Beschäftigten fragen?  
Der DSK-Beschluss und § 28b IfSG n. F.**

Seite 342

Dr. Matthias Jantsch und Dr. Dominik Sorber

**3G-Regel am Arbeitsplatz datenschutzkonform ausgestalten – Gesetzgeber lässt Gestaltungsspielraum**

Seite 345

Felix Meurer

**Neue gesetzliche Pflichten bei Telefonwerbung**

Seite 348

Rainer Burkardt und Jürgen Recha

**Das neue chinesische Datenschutzrecht und die europäische DSGVO im Rechtsvergleich**

Seite 350

## Aktuelles aus den Aufsichtsbehörden

Dr. Carlo Piltz

**Blick über den Tellerrand: FAQ der finnischen Datenschutzbehörde zur DSGVO**

Seite 356

Andreas Schmidt

**Aufforderungs-E-Mails zur Bewertung eines Online-Shops bedürfen der Einwilligung**

Seite 358

## Rechtsprechung

Niklas Plutte

**LG Frankfurt: Haftung bei technisch fehlerhaftem Consent Banner**

Seite 360

▪ Nachrichten Seite 340 ▪ Service Seite 364

Niklas Plutte

# LG Frankfurt: Haftung bei technisch fehlerhaftem Consent Banner

LG Frankfurt, Urt. v. 19.10.2021 – 3-06 O 24/21 (nicht rkr.)

## Consent Banner als Haftungsrisiko

Wer aufgrund eines technisch defekten Consent Banners Tracking Cookies im Browserspeicher seiner Websitebesucher speichert, ohne dass diese vorher eingewilligt haben, verstößt gegen TMG und UWG. Er haftet auch dann als Täter auf Unterlassung, wenn der Fehler nicht auf einer falschen Integration des Banners in die Internetseite basieren sollte, sondern auf einer Systemumstellung des beauftragten Consent Banner Anbieters.

## Der Fall

Die Wettbewerbszentrale ging aufgrund einer Beschwerde gegen eine Fitnessstudiobetreiberin vor, die bei Aufruf ihrer Internetseite Tracking Cookies und Web Storage Dateien der populären Dienste Criteo, Facebook Pixel, Google Analytics, Hotjar und Microsoft Ads ohne Einwilligung im Browser der Besucher abspeicherte.

Auf der Internetseite war zwar ein sog. Consent Banner eingebunden, über das Einwilligungen der Besucher eingeholt werden sollten. Das Banner funktionierte aber nicht korrekt. Sämtliche Tracking Cookies sowie Web Storage Dateien wurden bereits bei erstmaligem Seitenaufruf im Browser der Website-Besucher abgespeichert. Die nachfolgende Entscheidung der Besucher im Banner hatte keine Auswirkungen. Lehnte der Besucher eine Aktivierung der oben genannten Trackingdienste ab, blieben trotzdem alle aktiv. Stimmte er deren Aktivierung zu, wurden keine weiteren Cookies bzw. Web Storage Dateien nachgeladen, da initial bereits sämtliche Daten geladen worden waren. Der Fehler wirkte sich darüber hinaus in den Cookie Einstellungen der Internetseite aus, wo angezeigt wurde, nicht notwendige Cookies seien deaktiviert, obwohl dies nicht zutraf.

Die Beklagte räumte die Fehlfunktion des Banners ein. Es habe sich um einen kurzzeitigen Fehler gehandelt, der auf einer Systemumstellung der Consent Management Plattform (CMP) basiere, bei der es sich um den Marktführer für CMP-Lösungen handele. Nach dem Vortrag der Beklagten sei im Consent Banner der ursprüngliche Standardwert, ob ein Cookie gespeichert wird, ein „Ja“ gewesen. Besucher hätten das Speichern explizit ablehnen müssen. Zu einem unbekanntem Zeitpunkt habe der CMP-Anbieter den Prozess geändert von einem „negativen Consent“ hin zu einem „positiven Consent“, ohne die Beklagte zu informieren. Zusätzlich habe der Anbieter eine technische Änderung vorgenommen, nach der es nicht mehr möglich gewe-

sen sei, Cookie-auslösende JavaScripts zu blockieren, selbst wenn der Websitebesucher das Speichern von Cookies abgelehnt habe.

## Die Gründe

Das Landgericht Frankfurt verurteilte die Websitebetreiberin antragsgemäß unter Verweis auf den konkreten Verletzungsfall, es zu unterlassen, ohne erforderliche Einwilligung der betroffenen Website-Besucher nicht notwendige Cookies und/oder vergleichbare Speicherobjekte im lokalen Browserspeicher auf deren Endgerät zu speichern bzw. speichern zu lassen (§§ 8 Abs. 1, 3, 3a UWG in Verbindung mit §§ 12 Abs. 1, 15 Abs. 3 TMG).

Gleichzeitig verbot es der Beklagten, in den Cookie Einstellungen anzuzeigen bzw. anzeigen zu lassen, nicht notwendige Cookies seien deaktiviert, sofern dies nicht zutrifft (§§ 8 Abs. 1, 3, 5 UWG).

## Klageanträge ausreichend bestimmt

Das Landgericht stufte die Klageanträge als ausreichend bestimmt ein, da die Wettbewerbszentrale auf die konkrete Verletzungsform Bezug genommen hatte. Die Verwendung unbestimmter Rechtsbegriffe in den Anträgen führe ebenfalls nicht zur Unzulässigkeit der Klage. Es bestehe ein allgemeines Verständnis des Inhalts der Begriffe der notwendigen Cookies. Die Beklagte selbst gehe angesichts ihrer im Consent Banner vorgenommenen Unterscheidung in notwendige und andere Cookies von einem solchen allgemeinen Verständnis aus. Gleiches gelte für die Begriffe der „vergleichbaren Speicherobjekte“ und der „erforderlichen Einwilligung“.

## Rechtliche Einordnung

Bei der rechtlichen Beurteilung unterscheidet man zwischen notwendigen und nicht notwendigen Cookies. Für Web Storage Dateien, die im lokalen Browserspeicher abgelegt werden, gelten die gleichen Grundsätze. Die folgende Darstellung beschränkt sich daher auf den Begriff des Cookies.

Cookies sind kleine Textdateien, die bei Aufruf einer Webseite im Browser des Besuchers gespeichert werden können. Sie ermöglichen dem Browser bei erneutem Aufruf eine Zuordnung des Besuchers, wobei sich die Einsatzzwecke in der Praxis erheblich unterscheiden können.

Zum einen werden Cookies beispielsweise eingesetzt, um

in Onlineshops einen Warenkorb bereitzustellen. Ein spezielles Cookie erlaubt dem Browser die Zuordnung, ob und welcher Artikel vom jeweiligen Besucher in den Warenkorb gelegt wurde. Besucher können im Anschluss weitersurfen, ohne dass sich der Warenkorb bei Aufruf der nächsten Webseite des Shops leert. Nach dem gleichen Prinzip können etwa auch passwortgeschützte Member Areas entwickelt werden. Innerhalb des geschützten Websitebereichs verhindert typischerweise ein Session Cookie den Logout. Beide Beispiele haben gemein, dass die Eingriffsintensität der gesetzten Cookies erkennbar gering ist. Ihr Zweck erschöpft sich in der Bereitstellung einer unverzichtbaren Funktionalität. Dies rechtfertigt die Einstufung als notwendige Cookies. Auf der anderen Seite des Spektrums können Cookies dazu benutzt werden, das Verhalten von Menschen auf Websites zu verfolgen, ggf. sogar über verschiedene Websites und Endgeräte hinweg. Aus den gewonnenen Daten lassen sich u. a. Profile des jeweiligen Nutzers erzeugen, entsprechend hoch ist die Eingriffsintensität. Solche Tracking Cookies sind im rechtlichen Sinne nicht notwendig.

Für notwendige Cookies benötigen Websitebetreiber nach der Rechtsprechung von EuGH und BGH keine Einwilligung. Sie dürfen direkt bei Seitenaufruf im Browser des Besuchers abgespeichert werden.

Setzt ein Websitebetreiber auf seiner Internetseite hingegen Werbe-, Analyse- oder Marketingdienste ein, die nicht notwendige Cookies verwenden (z. B. Google Analytics, Facebook Pixel), ist deren Speicherung nach dem Planet49-Urteil des EuGH nur zulässig, wenn der Websitebesucher zuvor eine aktive und informierte Einwilligung erteilt hat. Die nötigen Besuchereinigilligungen können faktisch nur über Consent Banner eingeholt werden (der Begriff „Cookie Banner“ stellt einen Unterfall des Consent Banners dar). Solche Banner müssen so in die Website eingebunden werden, dass sie bei erstmaligem Aufruf einer beliebigen Webseite der Internetpräsenz erscheinen und vom Besucher erfragen, ob er der Speicherung von im Einzelnen aufgeschlüsselten nicht notwendigen Cookies zustimmt (zur inhaltlichen Ausgestaltung von Cookie Bannern, insbesondere eingesetzter Buttons vgl. LG Rostock, Urte. v. 15.09.2020 – 3 O 762/19). Im Browser des Besuchers dürfen sodann nur Cookies gespeichert werden, für die eine ausdrückliche Einwilligung erteilt worden war. Zu beachten ist, dass die Rechtsprechung vorangeklickte Checkboxes nicht als ausdrückliche Einwilligung wertet.

### Defektes Banner verletzt TMG und UWG

Vor diesem Hintergrund entschied das Landgericht Frankfurt, dass sich die Beklagte eine unlautere Handlung nach § 3 Abs. 1 UWG vorwerfen lassen muss, da sie durch das Speichern nicht notwendiger Cookies ohne vorherige Einwilligung der Websitebesucher gegen § 15 Abs. 3 TMG verstoßen hatte.

Die Vorschrift des § 15 Abs. 3 TMG stelle eine Marktverhaltensregel im Sinne von § 3a UWG dar. Sie statuiere bei richtlinienkonformer Auslegung unter Berücksichtigung von Art. 5 Abs. 3 RL 2002/58/EG eine Verpflichtung des Diensteanbieters, nach der für Zwecke der Werbung, Marktforschung oder bedarfsgerechten Gestaltung von Telemedien Nutzungsprofile bei Verwendung von Pseudonymen nur erstellt werden dürfen, sofern der Nutzer dem nicht widerspricht.

### Websitebetreiber haftet als Täter

Dem Versuch der Beklagten, die wettbewerbsrechtliche Haftung auf den Anbieter des Consent Banners abzuwälzen, erteilte das Landgericht eine Absage. Der Consent Banner Anbieter habe zwar Dienstleistungen für die Beklagte erbracht. Die Beklagte hafte für die Rechtsverstöße gleichwohl als Täterin nach § 8 Abs. 1 UWG, weil allein sie Diensteanbieterin im Sinne des TMG sei. Da der Unterlassungsanspruch kein Verschulden erfordert, kam es auf die Gründe des Fehlverhaltens des Consent Banner Anbieters nicht an.

Durch die Falschanzeige in den Cookie Einstellungen der Website, wonach nicht notwendige Cookies deaktiviert seien, habe die Beklagte ihre Besucher über wesentliche Merkmale der Websitenutzung getäuscht. Durch Klicks auf die Checkboxes „Notwendig“ und „Einstellungen speichern“ im Consent Banner seien diese davon ausgegangen, dass keine optionalen Cookies gespeichert werden, was tatsächlich nicht der Fall war. Die Täuschung sei wettbewerbsrechtlich relevant, da sich Verbraucher aufgrund ihrer irrigen Annahme näher mit den Angeboten der Website beschäftigen würden, was sie bei Kenntnis der tatsächlichen Umstände womöglich nicht getan hätten.

Für die vom Consent Banner Anbieter falsch vorgenommenen Einstellungen hafte die Websitebetreiberin nach § 8 Abs. 2 UWG, da es sich um einen Beauftragten der Beklagten gehandelt habe. Aufgrund der Erfolgshaftung ohne Entlastungsmöglichkeit könne sich die Beklagte nicht darauf berufen, sie habe die Zuwiderhandlung ihres Beauftragten nicht gekannt oder verhindern können.

### Auswirkungen auf die Praxis

Wer Dienste auf seiner Internetseite einsetzt, die nicht notwendige Cookies bzw. Web Storage Dateien im Browser der Besuchern speichern, benötigt ein korrekt in die Website integriertes Consent Banner.

Die Entscheidung des Landgerichts Frankfurt verdeutlicht das Haftungsrisiko bei technisch wirkungslosen Banner-Fassaden. Ob Websitebetreiber im Innenverhältnis für technisch defekte Consent Banner verantwortlich sind, spielt im Außenverhältnis keine Rolle, da sie für Fehler beauftragter Consent Banner Anbieter einstehen müssen (§ 8 Abs. 2 UWG).

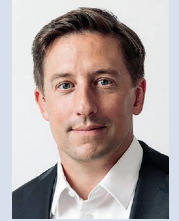
Ob Consent Banner technisch korrekt funktionieren, lässt sich bei Besuch einer Internetseite leicht überprüfen, z. B. durch Nutzung von Browsererweiterungen wie dem kostenlos erhältlichen Add-On "Ghostery".

Abmahngefahr geht bei Datenschutzverstößen spätestens seit Einführung von § 13 Abs. 4 UWG weniger von Mitbewerbern als von anspruchsbefugten Verbänden wie der Wettbewerbszentrale aus. Die Liste qualifizierter Wirtschaftsverbände nach § 8b UWG mit weiteren abmahnberechtigten Anbietern wurde jüngst vom Bundesamt für Justiz veröffentlicht.

Kommt es zu einer Abmahnung, sollte sorgsam abgewogen werden, ob die Abgabe einer strafbewehrten Unterlassungserklärung vertretbar ist. Wer sein Consent Banner selbst hosted und vollen Zugriff auf dessen Verhalten hat, mag sich dazu eher in der Lage sehen. Weitaus gängiger ist jedoch die Integration externer Consent Banner Anbieter

wie UserCentrics, Consentmanager.de oder Borlabs Cookie in die eigene Website. Käme es nach Abgabe einer strafbewehrten Unterlassungserklärung erneut zu einem Fehlverhalten des (zumindest teilweise extern kontrollierten) Banners, das dem Unterlassungsvertrag unterfällt, steht zu befürchten, dass Gerichte den Websitebetreiber für etwaige Versäumnisse seines Beauftragten haften lassen und Vertragsstrafen zusprechen. Dem Websitebetreiber blieben allenfalls Regressansprüche im Innenverhältnis mit ungewissen Erfolgsaussichten.

**Autor:** Niklas Plutte ist Rechtsanwalt und Fachanwalt für gewerblichen Rechtsschutz. Seine Kanzlei berät Unternehmen in den Bereichen IT-Recht, Gewerblicher Rechtsschutz und Medienrecht. Er ist Gründer und Geschäftsführer des Legaltechs avalex, das via Plugins automatisch aktuelle Rechtstexte für Websites & Shops anbietet.



## Kompakte Einführung



### Themenschwerpunkte

- Zivilrechtliche Regulierung von Plattformen (P2B-VO)
- Fernabsatzrecht inkl. elektronischem Streitschlichtungsverfahren
- Widerrufsrecht und Informationspflichten im eCommerce und mCommerce
- Eigenes Kapitel zu den neuen Regelungen für digitale Inhalte
- Haftung der Portalbetreiber sowie wettbewerbs- und datenschutzrechtliche Fragen
- **Topaktuell:** Enthält bereits die Neuregelungen aufgrund der Umsetzung der Richtlinie über digitale Inhalte und das sog. **'Faire Verbraucherverträge'-Gesetz**

### Von erfahrenen Spezialisten

Prof. Dr. Prof. h.c. **Jürgen Taeger** ist Of Counsel bei DLA Piper. Bis März 2020 war er Inhaber des Lehrstuhls für Bürgerliches Recht, Handels- und Wirtschaftsrecht sowie Informationsrecht an der Universität Oldenburg und Direktor des Zentrums für Recht der Informationsgesellschaft (ZRI). Er ist Vorstandsvorsitzender der Deutschen Stiftung für Recht und Informatik (DSRI).

**Sascha Kremer** ist FA für IT-Recht, Datenschutzexperte und Lehrbeauftragter an den Hochschulen Düsseldorf und Bonn-Rhein-Sieg für IT- und Datenschutzrecht.

Taeger/Kremer | **Recht im E-Commerce und Internet**

2. Auflage 2021 | Kommunikation & Recht | Einführung | 538 Seiten | Broschur | € 98,- | ISBN: 978-3-8005-1727-5

Weitere Informationen [shop.ruw.de/17275](https://shop.ruw.de/17275)

