

FOX Group

FTC-Urteil gefährdet transatlantische Datenflüsse

Das US-Supreme-Court-Urteil *Trump vs. Slaughter* vom 29.06.2026 hebt die Unabhängigkeit der Federal Trade Commission (FTC) auf und macht sie nunmehr weisungsgebunden. Da das EU-US Data Privacy Framework (DPF) elementar auf einer unabhängigen US-Aufsicht basiert, ist seine Rechtsgrundlage geschwächt. Europäische Unternehmen sollten wegen möglicher Klagen beim EuGH gegen das EU-US-Abkommen sofort handeln, um empfindliche DSGVO-Bußgelder zu verhindern.

Als Sofortmaßnahme sollten alle US-Datenflüsse (Cloud, CRM, Marketing-Pixel) lückenlos inventarisiert werden. Verträge sind auf EU-Standardvertragsklauseln (SCC) umzustellen und um ein aktuelles Transfer Impact Assessment (TIA) zu ergänzen, in dem das veränderte US-Schutzniveau dokumentiert ist.

Zusätzlich sind datenschutzkonforme technische Hürden zu implementieren: z. B. eine verbindliche Datenlokalisierung auf EU-Servern, die jedoch zwingend mit einer konsequenten Ende-zu-Ende-Verschlüsselung unter rein europäischer Schlüsselgewalt gekoppelt sein sollte.

Urteil vom 29.06.2026: https://www.supremecourt.gov/opinions/25pdf/25-332_qn12.pdf

Thema 1

**FTC-Urteil
gefährdet
transatlantische
Datenflüsse**

Thema 2

**Dunkel gestaltet,
hell verpackt:
Nudging im
Cookie Banner**

Thema 3

**Robot.txt als
vermeintlicher
Schutz vor KI-
Crawler**



Dunkel gestaltet, hell verpackt: Nudging im Cookie Banner

Wer eine Website besucht, begegnet ihm fast unvermeidlich: dem Cookie-Banner. Was auf den ersten Blick wie eine neutrale Einwilligungsabfrage wirkt, ist in vielen Fällen sorgfältig choreografiert – mit dem Ziel, die Personen beim Webseitenbesuch unbemerkt in eine bestimmte Richtung zu lenken. Der Fachbegriff dafür lautet Nudging, auf Deutsch: Anstupsen. Das Prinzip dahinter beschreibt gezielt die Entscheidungsoberfläche so zu gestalten, um das Verhalten in eine gewünschte Richtung zu beeinflussen, ohne es klar zu äußern. Beim Cookie-Banner erkennt man das daran, dass der Zustimmungsknopf zu allen Cookies entweder optisch hervorgehoben, farblich betont oder an prominenter Stelle platziert ist bzw. alle drei Optionen gleichzeitig ausgewählt sind. Die Ablehnung hingegen wird versteckt, ist grau hinterlegt und nur mit mehreren Klicks möglich oder kaum zu finden. Technisch bedenkenlos wird so Nudging perfekt umgesetzt. Beabsichtigt oder unbewusst umgehen Webdesignstudios oder Marketingleute die Vorgaben der DSGVO.

Der Fantasie beim Nudging sind keine Grenzen gesetzt. Die Palette der Möglichkeiten reicht vom dezenten bis zum dreisten Eingriff in die Entscheidungsfreiheit. Beliebt sind: ein auffälliges „Alles akzeptieren“ kombiniert mit einem kaum sichtbaren „Ablehnen“-Link, vorangekreuzte Checkboxes für nicht notwendige Cookies, irreführende Formulierungen wie „Einstellungen verwalten“ anstelle von „Ablehnen“ sowie das bewusste Weglassen einer gleichwertigen Ablehnungsoption auf der ersten Ebene des Banners. Einige Anbieter gehen sogar so weit, den „Ablehnen“-Button direkt neben oder zwischen den Zustimmungsoptionen zu platzieren. Bei der Smartphone-Nutzung spekulieren sie gezielt auf den sogenannten ‚Dicke-Finger-Effekt‘, um durch versehentliches Vertippen doch noch eine Einwilligung zu erhalten. Auch der nachträgliche Widerruf wird Nutzenden bewusst schwer gemacht. Den dafür nötigen Button für die Cookie-Einstellungen nachträglich wiederzufinden, wird durch unübersichtliche Menüstrukturen verkompliziert.

Der Europäische Datenschutzausschuss (EDSA) hat in seinen Leitlinien zu Cookie-Bannern eindeutig klargestellt: Eine Einwilligung ist nur dann wirksam, wenn sie freiwillig, spezifisch, informiert und unmissverständlich erteilt wird. Designs, die eine bestimmte Entscheidung in seiner Gestaltung begünstigt, bekannt auch als „dark patterns“ verstoßen gegen den Grundsatz der wirksamen Einwilligung. Europäische Aufsichtsbehörden haben begonnen Millionenstrafen gegen namhafte Unternehmen auszusprechen (z.B. Google, Shein, American Express und TikTok). In einer aktuellen Entscheidung bezüglich der Website ORF.at bestätigte das Bundesverwaltungsgericht Österreich (Mai 2026) hier die absolute Unzulässigkeit von Cookie-Nudging.

Ein Cookie-Banner ist längst kein rein technisches Beiwerk mehr. Es dient als datenschutzrechtliches Aushängeschild. Wer seine Banner nicht kritisch hinterfragt, sollte zeitnah aktiv werden. Aufsichtsbehörden setzen mittlerweile automatisierte Software-Scanner ein, die tausende Webseiten vollautomatisch nach fehlerhaften Bannern und ungleichen Buttons durchkämmen– unabhängig davon, ob sie auffällig wurden.



Robots.txt als vermeintlicher Schutz vor KI-Crawler

Künstliche Intelligenz revolutioniert das Marketing, doch sie bedient sich auch ungefragt an den Webseiten von Unternehmen: an Texten, Grafiken und Konzepten. Um KI-Systeme wie ChatGPT, Claude oder Gemini zu trainieren durchsuchen KI-Crawler rund um die Uhr das Internet. Für Marketingabteilungen birgt dies das Risiko, dass einzigartiger Content an Exklusivität verliert und Reichweite direkt in die Chat-Fenster der KI-Anbieter wandert, ohne dass Nutzer jemals eine Website besuchen. Dies ist auch unter dem Begriff „Zero-Click“ bekannt.

Was Unternehmen dagegen tun, ist den Bot-Zugriff über die sogenannte Robots.txt-Datei zu limitieren. Diese kleine Textdatei liegt im Hauptverzeichnis von Webseiten und fungiert als digitales „Stoppschild“. Indem gezielte Kommandos hinterlegt werden, erhalten Crawler-Bots Anweisungen welche Inhalte sie lesen dürfen und welche nicht.

Der Einsatz von Robots.txt ist ein reines Gentlemen's Agreement zwischen den Webseiten-Betreibern und den KI-Entwicklern, für die es jedoch keine gesetzliche Verpflichtung gibt. Der Schutz eigener Inhalte ist im KI-Zeitalter kein technisches Detail, sondern eine strategische Marketing-Entscheidung. So ist die Wahl einer Bot-Strategie sinnvoll, um mit einer KI-Bot Blockade die eigenen Inhalte zu schützen. Dieser Schutz kann jedoch auch dazu führen, nicht mehr im Netz durch Google und Co. gefunden zu werden.

Die Webseite *Wayback Machine*, gestartet als reines Webarchiv, z. B., um archivierte Webseiten und ihre Änderungen und Anpassungen mit Datum und Inhalt betrachten zu können, musste handeln, um nicht als kostenlose Quelle zu enden. Ihr riesiges Webarchiv nutzten KI-Entwickler weltweit als historische Datenbasis zum Trainieren ihrer KI-Modelle. Um Urheberrechte zu schützen und Datenmissbrauch zu verhindern, blockiert der Webseiten-Betreiber die KI-Bots gezielt per Robots.txt. Weitere Archive und Zeitungs- und Nachrichtenanbieter folgten und nutzen zusätzlich eine Paywall.

Mit einer sauber konfigurierten Robots.txt-Datei wird die Exklusivität des Webseiten-Contents geschützt samt Kontrolle über die Markenbotschaft – ohne die SEO-Sichtbarkeit zu opfern. Es empfiehlt sich, proaktiv zu handeln, bevor wertvolle Unternehmensdaten die Konkurrenz von morgen trainieren.

Impressum

complimant AG, Edt 4, 84558 Kirchweidach

Vorstand: Franz Obermayer, Ann-Karina Wrede

Vorsitzender des Aufsichtsrates: Christian Volkmer

Telefon: +49 8683 99390-40

E-Mail: info@complimant.de / datenschutz@complimant.de

www.complimant.de

Eintragung im Handelsregister: Amtsgericht: Traunstein

Registernummer: HRB 20500 Steuernummer: 141/120/07009

Umsatzsteuer-Identifikationsnummer gemäß §27a

Umsatzsteuergesetz: DE274380239

Verantwortlich für den Inhalt nach §18 Abs. 2 MStV Franz Obermayer