

COMPLIANCE

Cookie-Banner – Pflicht für jede Website in der EU? Was wirklich gilt

Wann braucht eine Website einen Cookie-Banner? Wann nicht? Klare Antworten zu TKG 2021, DSGVO und der Self-Hosted-Alternative — von Strukturaflow-CEO Natascha Reiner.

AUTOR

Natascha Reiner

VERÖFFENTLICHT

26. April 2026

ONLINE LESEN

<https://wissen.strukturaflow.it.com/cookie-banner-pflicht-website-eu-2026/>

Nicht jede Website braucht einen Cookie-Banner. Wer das nicht weiß, baut entweder einen Banner, den er nicht bräuchte — oder keinen, obwohl er einen müsste.

Beides kann teuer werden. Aus unterschiedlichen Gründen.

Der Cookie-Banner ist das meistmissverstandene Element im europäischen Webrecht. Manche Betriebe betreiben aufwendige Consent-Systeme auf Websites, die schlicht keinen bräuchten. Andere ignorieren die Thematik vollständig — auf Seiten, auf denen ein Banner längst Pflicht wäre.

Dieser Artikel gibt Ihnen eine klare, ehrliche Antwort: Wann brauche ich einen Cookie-Banner? Wann nicht? Und was steht wirklich dahinter?

Was ist ein Cookie überhaupt? Ohne Fachjargon erklärt

Stellen Sie sich vor, Sie betreten ein Geschäft. Der Verkäufer gibt Ihnen beim Eingang eine Nummer — und notiert intern: „Kunde 4271 hat heute um 10:14 Uhr die Schuhabteilung besucht, war drei Minuten beim Sneaker-Regal und hat dann die Kasse passiert.“

Beim nächsten Besuch erkennt das System Sie sofort. Ihr Verhalten wird mit dem früheren Besuch verknüpft. Vielleicht werden Ihnen dann gezielt Angebote gemacht.

Genau das passiert beim Laden einer Website — nur unsichtbar und innerhalb von Millisekunden.

Ein Cookie ist eine kleine Textdatei, die ein Webserver über Ihren Browser auf Ihrem Gerät ablegt oder von dort ausliest. Er enthält Informationen: eine Kennung, eine Einstellung, einen Zeitstempel. Ihr Gerät merkt sich diese Datei und schickt sie beim nächsten Besuch automatisch mit.

Was harmlos klingt, ist der technische Unterbau für ein riesiges Ökosystem: Werbenetzwerke, die Sie über Dutzende von Websites verfolgen. Algorithmen, die Ihnen passende Anzeigen ausspielen. Analyseplattformen, die das Verhalten von tausenden Nutzern aggregieren und auswerten.

Die entscheidende Frage ist nicht: Hat meine Website Cookies? Fast jede Website hat irgendwelche. Die entscheidende Frage lautet: **Was tun diese Cookies — und wessen Dienste stecken dahinter?**

Das Gesetz dahinter: Was EU-Recht tatsächlich regelt

Die rechtliche Grundlage für Cookie-Banner in der EU stammt aus zwei Quellen, die zusammenwirken.

Die ePrivacy-Richtlinie – das Fundament

Die europäische Richtlinie 2002/58/EG, mehrfach geändert, regelt den Zugriff auf das Endgerät eines Nutzers. Der entscheidende Satz steht in Artikel 5 Absatz 3: Das Speichern von Informationen auf dem Endgerät eines Nutzers oder das Auslesen von dort gespeicherten Informationen ist **grundsätzlich nur mit dessen Einwilligung** zulässig.

Wichtig: Das Gesetz schützt das Gerät — unabhängig davon, ob die Daten personenbezogen sind oder nicht.

Für Österreich ist diese Richtlinie im Telekommunikationsgesetz 2021 (TKG 2021), § 165 Abs. 3 umgesetzt. Seit 1. November 2021 gilt: Wer nicht notwendige Informationen auf dem Endgerät eines Nutzers speichert oder ausliest, braucht eine aktive Einwilligung.

Die DSGVO – die Anforderungen an die Einwilligung

Die DSGVO kommt ins Spiel, sobald über Cookies personenbezogene Daten verarbeitet werden — also sobald ein Nutzer auch nur theoretisch identifizierbar wird. Sie definiert, was eine gültige Einwilligung ist: **freiwillig, informiert, eindeutig und aktiv**.

Das Zusammenspiel ist entscheidend: Das TKG regelt, ob ein Cookie überhaupt gesetzt werden darf. Die DSGVO regelt, wie die dazugehörige Einwilligung aussehen muss. Beide greifen in der Praxis fast immer gleichzeitig.

Was 2025 passiert ist – und warum das relevant bleibt

Jahrelang war geplant, die ePrivacy-Richtlinie durch eine unmittelbar geltende EU-Verordnung zu ersetzen — um den Flickenteppich nationaler Umsetzungsgesetze zu beenden. Am 11. Februar 2025 hat die Europäische Kommission diesen Vorschlag offiziell zurückgezogen. Begründung: keine Einigung absehbar, der Entwurf durch neue Gesetzgebung wie den Digital Markets Act bereits überholt.

Für Website-Betreiber in Österreich bedeutet das: Das TKG 2021 bleibt auf unbestimmte Zeit die maßgebliche Rechtsgrundlage. Es gibt keine neue EU-Vereinheitlichung. Und die Zuständigkeiten bleiben komplex: Bei TKG-Verstößen sind Fernmeldebehörden zuständig, bei DSGVO-Verstößen die Datenschutzbehörde (DSB).

Wann brauche ich keinen Cookie-Banner?

Das ist der Teil, den die meisten nicht kennen — und der einen echten Unterschied machen kann.

Das Gesetz kennt eine zentrale Ausnahme: Cookies, die **technisch unbedingt erforderlich** sind, damit ein vom Nutzer ausdrücklich gewünschter Dienst erbracht werden kann, dürfen ohne Einwilligung gesetzt werden.

Anerkannte Ausnahmen in der Praxis:

COOKIE-TYP	BEISPIEL	EINWILLIGUNG NOTIG?
Session / Login	Authentifizierung nach Login	Nein
Warenkorb	E-Commerce Produktspeicherung	Nein
Consent-Cookie	Speichert Ihre eigene Banner-Entscheidung	Nein
Load Balancing	Verteilt Traffic auf Server	Nein
Sicherheits-Cookie	CSRF-Schutz	Nein
Statistik (extern)	<u>Google</u> Analytics	Ja
Marketing	Facebook Pixel	Ja
Funktional	Spracheinstellung via Drittanbieter	Ja

Was bedeutet das konkret?

Eine einfache Website — zum Beispiel eine Unternehmenswebsite, ein Portfolio, ein Branchenverzeichniseintrag — die **ausschließlich** technisch notwendige Cookies setzt und **keine externen Dienste** einbindet, braucht keinen Cookie-Banner. Über die eingesetzten Cookies muss trotzdem in der Datenschutzerklärung informiert werden.

Die Bedingung ist aber eng zu verstehen. Sobald auch nur ein einziger externer Dienst eingebunden ist — ein YouTube-Video, ein Google Font, ein Instagram-Feed, ein Chat-Widget, ein Analysetool — ändert sich die Lage.

Der Fall reCAPTCHA: Wie eng die Grenze wirklich ist

Das österreichische Bundesverwaltungsgericht (BVwG) hat 2024 entschieden, dass selbst Google reCAPTCHA — ein Sicherheitstool zur Bot-Abwehr — **nicht** als unbedingt erforderlich gilt, wenn es gleichzeitig Daten an Google zur Analyse weiterleitet. Das heißt: Auch für dieses Sicherheits-Tool brauchen Sie eine Einwilligung, solange Sie keine datenschutzfreundliche Alternative nutzen.

Die Botschaft ist klar: Im Zweifel ist ein Banner nötig. Die Ausnahme ist eng — und wird von Behörden und Gerichten eng ausgelegt.

Vergleichstabelle „Cookie-Banner: Pflicht oder nicht?": Kein Banner nötig und Banner erforderlich im Vergleich nach Cookies, Externe Services, Rechtliche Basis, Info erforderlich.

Wann brauche ich definitiv einen?

Sobald eines dieser Elemente auf Ihrer Website aktiv ist:

- Google Analytics oder ähnliche Analysetools (Matomo in der Cloud-Variante eingeschlossen)
- Facebook Pixel, LinkedIn Insight Tag, TikTok Pixel
- YouTube-Videos eingebettet via Standard-Iframe
- Google Fonts direkt von Google-Servern geladen
- Google Maps eingebettet
- Live-Chat-Tools (z. B. Intercom, Tidio, Freshchat) mit externem Backend
- Affiliate-Tracking-Codes
- Retargeting-Pixel jeder Art

Der gemeinsame Nenner: Diese Dienste übermitteln Daten an externe Server — oft in die USA. Damit liegt eine Verarbeitung personenbezogener Daten vor, die eine Einwilligung nach DSGVO und TKG voraussetzt.

Was einen rechtssicheren Banner ausmacht

Ein Banner zu haben reicht nicht. Das BVwG und die DSB haben klare Anforderungen definiert, die in der Praxis überraschend oft verletzt werden.

Der Ablehnen-Button auf Ebene 1

Das wichtigste Kriterium: Auf der ersten sichtbaren Ebene des Banners müssen sowohl „Zustimmen“ als auch „Ablehnen“, als gleichwertige Buttons vorhanden sein. Es ist nicht zulässig, die Ablehnung hinter einem „Einstellungen“-Link zu verstecken, während die Zustimmung mit einem Klick möglich ist.

Das Verbot von Dark Patterns

Studien zeigen, dass rund drei Viertel aller Cookie-Banner manipulative Designelemente enthalten — sogenannte Dark Patterns. Dazu zählen:

- Ein grüner, auffälliger „Akzeptieren“-Button neben einem grauen, kaum lesbaren „Ablehnen“-Link
- Formulierungen wie „Ich stimme zu und unterstütze diese Website“, versus „Weiter ohne Unterstützung“
- Vorausgewählte Checkboxes für optionale Cookies

Die Anforderungen im Überblick:

ANFORDERUNG	WAS DAS BEDEUTET
Gleichwertigkeit	Annehmen und Ablehnen optisch gleichwertig
Aktive Handlung	Kein Consent durch Weiterscrollen oder Schließen
Voreinstellungen	Alle optionalen Kategorien initial deaktiviert
Widerruf	Einwilligung muss jederzeit einfach zurückziehbar sein
Transparenz	Zwecke, Empfänger und Speicherdauer klar benannt

US-Dienste: Die Drittland-Pflicht

Beim Einsatz amerikanischer Dienste muss der Banner explizit darüber informieren, dass Daten in die USA übermittelt werden. Das EU-U.S. Data Privacy Framework schafft zwar seit 2023 wieder eine Rechtsgrundlage — ist aber weiter umstritten und unterliegt strengen Informationspflichten.

Was passiert, wenn kein oder ein fehlerhafter Banner vorhanden ist?

Das Risiko ist real — und betrifft KMU anders als Konzerne, aber nicht weniger schmerzhaft.

Behördliche Sanktionen: Die DSB verhängt regelmäßig Bußgelder. Bei KMU liegen diese typischerweise im vier- bis fünfstelligen Bereich — 5.900 € bis 50.000 € sind dokumentierte Fälle. Der DSGVO-Strafraahmen reicht theoretisch bis zu 20 Millionen Euro.

Beschwerdeverfahren: Organisationen wie noyb (None of Your Business) führen systematische Beschwerden gegen fehlerhafte Cookie-Banner durch — automatisiert, skalierbar und ohne Rücksicht auf Unternehmensgröße.

Vertrauensverlust: Zunehmend bewerten Nutzer den Umgang mit ihren Daten als Qualitätsmerkmal. Ein manipulativer Banner ist sichtbar — und wird als solcher wahrgenommen.

Es gibt einen anderen Weg – und den kennen die wenigsten

Hier wird es interessant. Und hier beginnt mein eigentlicher Arbeitsbereich.

Die meisten Betriebe, die ich berate, wollen eigentlich dasselbe: **verstehen, wie Nutzer ihre Website verwenden**. Welche Seiten funktionieren? Wo springen Besucher ab? Welche Inhalte konvertieren?

Das ist eine vollkommen legitime Anforderung. Jedes Unternehmen hat das Recht, die eigene digitale Präsenz zu verstehen.

Die Standardlösung — Google Analytics einbinden, Banner davor — ist nur eine Möglichkeit. Und sie hat einen Preis: Ihre Nutzungsdaten verlassen Ihren Server. Sie landen bei einem amerikanischen Konzern. Sie müssen einen Banner bauen, eine Einwilligung einholen, und Sie wissen nie, wie viele Nutzer ablehnen und damit aus Ihrer Statistik herausfallen.

Es gibt eine Alternative, die die meisten nicht kennen: Self-Hosted Analytics.

Wenn ein Analysetool auf Ihrem eigenen Server läuft — von Ihnen betrieben, von Ihnen verwaltet — verlassen die Daten niemals Ihre Infrastruktur. Es gibt keinen Drittlandtransfer. Es gibt keinen externen Empfänger. Und unter bestimmten, sorgfältig konfigurierten Bedingungen entfällt damit auch die Einwilligungspflicht für Statistik-Cookies vollständig.

Das ist kein Trick. Das ist eine technisch und rechtlich saubere Architektur — die jedoch eine präzise Umsetzung erfordert. Die Konfiguration entscheidet: Welche Daten werden erhoben? Werden sie anonymisiert? Wie lange gespeichert? Wer hat Zugriff?

Ich halte das bewusst allgemein — nicht weil ich etwas verbergen will, sondern weil die richtige Lösung von Ihrer konkreten Situation abhängt: Ihrer Hosting-Infrastruktur, Ihrem Datenvolumen, Ihren Anforderungen an die Auswertung.

Was ich sagen kann: Es ist machbar. Wir setzen genau das für Kunden um.

Sie fragen sich vielleicht

„Ich habe eine einfache Wordpress-Seite. Muss ich mir wirklich Gedanken machen?“

Ja — gerade bei WordPress. Viele Themes und Plugins setzen im Hintergrund automatisch Tracking-Cookies, ohne dass Sie das aktiv entschieden haben. Google Fonts werden oft direkt von Google geladen. Kontaktformulare nutzen manchmal externe reCAPTCHA-Dienste. Ein Cookie-Audit lohnt sich fast immer.

„Mein Webdesigner hat mir gesagt, der Banner ist in Ordnung.“

Webdesigner sind oft exzellent in Design und Technik — aber nicht zwingend im Datenschutzrecht. Ein visuell schöner Banner kann rechtlich trotzdem fehlerhaft sein, wenn der Ablehnen-Button fehlt, Cookies schon vor dem Klick gesetzt werden oder die Informationspflichten nicht erfüllt sind.

„Wir sind ein kleines Unternehmen. Ist das wirklich relevant für uns?“

neoyb hat in den vergangenen Jahren Tausende von Beschwerden eingereicht — darunter gegen sehr kleine Betriebe. Die Größe schützt nicht. Die korrekte Umsetzung schützt.

„Gilt das auch für österreichische Kunden mit Kunden nur in Österreich?“

Ja. Das TKG 2021 und die DSGVO gelten für alle Websites, die Nutzer in der EU ansprechen — unabhängig von der Größe des Unternehmens oder dem geographischen Fokus.

Was ich konkret empfehle

Wenn Sie nach diesem Artikel eine Sache mitnehmen wollen, dann diese: **Machen Sie zuerst einen ehrlichen Cookie-Audit.** Wissen Sie wirklich, welche Skripte auf Ihrer Website aktiv sind? Welche Daten wohin fließen?

Ein Tool wie ein Browser-Netzwerkanalysator oder ein spezialisierter Cookie-Scanner zeigt Ihnen innerhalb von Minuten, was tatsächlich passiert — oft zum Erstaunen der Betreiber.

Danach teilt sich der Weg:

- Websites ohne externe Dienste können den Banner weglassen — müssen aber in der Datenschutzerklärung klar informieren.
- Websites mit externen Diensten brauchen einen rechtssicheren Banner mit echtem Ablehnen-Button auf Ebene 1 und vollständiger Transparenz über Datenflüsse.
- Betriebe, die Nutzungsdaten erheben wollen, ohne externe Abhängigkeit und ohne Einwilligungspflicht, können mit Self-Hosted Tracking arbeiten — wenn die Konfiguration stimmt.

Die dritte Option ist die, über die am wenigsten gesprochen wird. Und die häufig die sauberste Lösung ist.

Ihre Website, Ihre Daten – lassen Sie uns drüber reden

Bei Strukturaflow analysiere ich gemeinsam mit Kunden genau diese Fragen: Welche Cookies setzt Ihre Website wirklich? Wo fließen Daten hin, die Sie dort nicht erwartet hätten? Und wie lässt sich Ihre Anforderung an Nutzungsanalyse rechtssicher — und ohne externe Abhängigkeit — umsetzen?

Das Ergebnis ist keine generische Vorlage, sondern eine konkrete Einschätzung Ihrer Situation mit klaren nächsten Schritten.

Wenn Sie wissen wollen, wie das für Ihr Unternehmen aussieht: [Kontakt aufnehmen](#).

NÄCHSTER SCHRITT

Mehr praktische KI-Anleitungen für KMU

Dieser Artikel ist Teil des KI-Hubs von Strukturaflow — einer deutschsprachigen Plattform für den praktischen KI-Einsatz in kleinen und mittleren Unternehmen.

<https://wissen.strukturaflow.it.com>