

# COOKIEBANNER AUF WEBSEITEN

(STAND: Juni 2024)

## Nervige Cookiebanner

Nervt es Sie auch, sich ständig auf jeder Webseite durch die Cookiebanner durchklicken zu müssen, bevor es weiter geht? Es macht auch mir als Datenschützer keinen Spaß. Dennoch sind diese lästigen Banner wichtig. Für Sie als Betreiber einer Webseite hingegen kommen einige Pflichten zu, welche Sie nicht ignorieren sollten.

Wann und wozu brauchen wir diese Banner? Consent Manager, also Cookiebanner, kommen immer dann zum Einsatz, wenn über die Webseite Cookies gespeichert oder Scripte aktiviert werden, die das Verhalten des Webseitenbesuchers analysieren (Tracking) oder beeinflussen (Marketing) sollen. Zum Schutz der Privatsphäre aller Internetnutzer hat der Gesetzgeber hierzu in [§ 25 TDDDG](#) Vorgaben erlassen, wonach der Webseitenbesucher aktiv seine Einwilligung für diese Dienst geben muss. Gleiches gilt auch für die Dienste, die unsichtbar im Hintergrund agieren und Daten von Nutzern, angefangen bei der IP-Adresse, sammeln und irgendwohin übermitteln. Der Gesetzgeber möchte so verhindern, dass ungefragt Profile erstellt werden, welche zu einem späteren Zeitpunkt für einen anderen Zweck gebraucht oder sogar missbraucht werden könnten. Aus Erfahrung können wir sagen, dass fast auf jeder Webseite bekannte Dienste wie z.B. Google Analytics oder Facebook eingebunden sind.

Möchte ein Webseitenbetreiber wissen, welche Personengruppen sich wie auf seinen Webseiten bewegen, hat er schnell das Nachsehen, wenn niemand in die Cookies einwilligt. Hier liegt es nahe, den Nutzer durch hervorgehobene farbliche Akzente auf den Button „alle akzeptieren“ zu lenken und die anderen eher unscheinbar darzustellen. Diese Vorgehensweise wird auch als Nudging bezeichnet. Das ist allerdings nach Auffassung des LG Rostock nicht zulässig.



In einem Urteil wurde entschieden, dass alle Button gleichrangig und gleichfarbig darzustellen sind, um die Besucher nicht zu beeinflussen. Gestalten Sie den Cookie-Layer mit gleichrangigen Button und vermeiden Sie rechtliche Risiken!

## Fehlerhafte Einbindung von Buchungs- und Reservierungsportalen

In der täglichen Datenschutzpraxis mit Hotels und Restaurants treffen wir immer wieder auf die Problematik, dass auf deren Webseiten Buchungs- und Reservierungsportale von Drittanbietern eingebunden sind, die ebenfalls Scripte und Cookies zum Tracking und für Werbung auf Endgeräten speichern.

Als Webseitenbetreiber ist jeder Hotelier oder Gastwirt dafür verantwortlich, dass auch die eingebundenen Dienste der Drittanbieter, also eine Booking Engine, ein Programm zur Tischreservierung oder einem Gutscheinverkauf sowie ein Terminplaner den gesetzlichen Anforderungen entsprechen. Es empfiehlt sich, unabhängig ob bereits ein Consent-Manager auf der Webseite implementiert ist, eine erneute Prüfung durchzuführen. Im Rahmen unserer Beratertätigkeit als Datenschutzbeauftragte haben wir in der Praxis die Erfahrung gemacht, dass entweder kein Consent Manager für diese Dienste eingebunden ist oder dieser falsch

konfiguriert ist. Tracking- und Werbedienste werden oft ohne Einwilligung des Webseitenbesuchers geladen. Für die fehlende oder falsche Einbindung haftet der Webseitenbetreiber, nicht der Anbieter der Dienste.

Es ist sicherzustellen, dass die Webseiten den datenschutzrechtlichen Anforderungen entsprechen. Zu prüfen sind die Webseiten, die implementierten Buchungs- und Reservierungssysteme und die datenschutzrechtlichen Vereinbarungen mit den Systemanbietern. Wir berichteten bereits in der letzten Ausgabe von zusätzlichen Anforderungen einer Prüfung von Systemanbietern, wenn diese aus einem unsicheren Drittland, zumeist den USA kommen.

Für Betreiber von Webseiten ist oft schwer zu erkennen, ob der Consent Manager richtig funktioniert. Es ist bekannt, dass die Aufsichtsbehörden bereits Webseiten prüfen und dafür geeignete Tools einsetzen, um hinter die Kulissen zu schauen. Wir empfehlen eine regelmäßige Prüfung der eigenen Webseiten, auch wenn bereits ein Consent Manager im Einsatz ist. Mehr dazu in unserem Artikel „[Webseiten prüfen](#)“.

Ergibt die Webseitenanalyse, dass ein Consent Manager fehlt oder dieser fehlerhaft implementiert wurde, empfiehlt sich eine sofortige Kontaktaufnahme zum Systemanbieter oder zum Webseitenprogrammierer, um eine Lösung herbeizuführen.

## Google Analytics

Im Frühjahr 2024 hat Google auf **Google Analytics 4** umgestellt. Es ist zu prüfen, ob auf der Webseite noch das alte Google Analytics (UA) eingebunden ist. Sollte das der Fall sein, ist der Dienst unbedingt zu entfernen, da weiterhin Cookies gesetzt werden. In diesem Zusammenhang ist darauf hinzuweisen, dass die Aufsichtsbehörden für Datenschutz der Auffassung sind, dass der Einsatz von Google Analytics, egal in welcher Form, grundsätzlich nicht mit der DSGVO vereinbar ist. Wir müssen hier auch auf den neuen Google Consent Mode v2 zu sprechen kommen. Aus datenschutzrechtlicher Sicht kann zur Risikominimierung nur empfohlen werden, den **Basic-Modus** einzurichten. Der **Advanced-Modus** entspricht nach Ansicht der Aufsichtsbehörden ebenfalls nicht den datenschutzrechtlichen Grundsätzen, ist also nicht mit den Datenschutzgesetzen vereinbar. Dabei ist es unerheblich, dass Google schreibt, dass die Übertragung anonymisiert erfolgt. Zu überprüfen sind die Einstellungen, die Datenschutzerklärung ist anzupassen!

Ein falsch eingesetztes oder fehlendes Cookiebanner kann gemäß [§ 28 TDDDG](#) mit einem Bußgeld bis zu einer Höhe von 300.000 € bestraft werden. Als Datenschutzbeauftragte und Fördermitglied der Dehoga Berlin bieten wir einen Webseitencheck inkl. Überarbeitung ihrer Datenschutzerklärung mit 20 Prozent Preisnachlass an. Besuchen Sie uns für weitere Informationen auf unserer Webseite [www.datenschutzberater365.de/branchen](http://www.datenschutzberater365.de/branchen) oder QR Code

