



## **Positionspapier der PdF zum Thema "Cookiebanner"**

# Positionspapier der PdF zum Thema "Cookiebanner"

## 1. Begriffsklärung:

Unter „Cookie“ versteht man „eine Textinformation, die im Browser auf dem Computer des Benutzers jeweils zu einer besuchten Website gespeichert werden kann“ - so erklärt es zumindest Wikipedia. [1]

„Cookiebanner“ werden jene Abfragen auf Websites genannt, in denen Besucher ihre Cookie-Einstellungen vornehmen können. Netzpolitik.org schreibt dazu: „Cookie-Banner sind so etwas wie die Rache der Werbe-Industrie, nachdem EU-Gesetze die Rechte von Nutzern stärken sollten. Statt auf Datensammelei zu verzichten, setzen viele kommerzielle Websites den Nutzern manipulative Cookie-Banner vor. Die Pop-ups zeigen Textwüsten in kleiner Schriftgröße. Wer keine Tracking-Cookies möchte, muss meist mehrere Klicks machen – und bloß nicht den freundlichen „Alles akzeptieren“-Button klicken. Motto: So lange nerven, bis der Wille der Nutzer gebrochen ist.“ [2]

Diese Praktik ist unter dem Begriff „Dark Patterns“ bekannt geworden: Der „Alles Ablehnen“-Knopf ist in Untermenüs versteckt – sofern es ihn überhaupt gibt. Der Aufwand, alle Cookies abzulehnen ist um ein Vielfaches höher als der Aufwand einfach alles zu erlauben. Der „Alles Erlauben“ Knopf ist vorausgewählt, riesig groß, farblich hervorgehoben... Alles das sind „Manipulative Designs“ der Cookiebanner, um Nutzer zur Zustimmung zu überreden. Ob sie legal sind? Fraglich.

Diese kleinen Texte, die von Websites auf dem Gerät eines Nutzers gespeichert werden, sind teilweise wichtig, um die technische Funktion von Websites zu ermöglichen, da diese erhalten bleiben, auch wenn der Benutzer zu einer anderen Seite innerhalb der Website wechselt. Der Server könnte so z. B. feststellen, ob ein Benutzer sich angemeldet hat, welche Sprache er bevorzugt oder welches Farbschema ihm angenehm ist. Diese Cookies werden von der Website gespeichert, die der Benutzer aktiv aufgerufen hat und werden daher Erstanbieter-Cookies (englisch First Party Cookies) genannt. Das Zulassen dieser Cookies ist oft essentiell notwendig, damit man die Inhalte anschauen kann.

Es ist allerdings auch möglich, dass ein anderer Anbieter Cookies speichert, dessen Identität dem Benutzer nicht unbedingt bekannt ist. Diese "verstecken" sich z. B. in Werbebannern, die von Servens eines Anzeigenkunden geladen werden oder hinter „Social Media Buttons“. Diese Cookies heißen Drittanbieter-Cookies (Third Party Cookies). Der (eventuell dem Benutzer unbekannte) Drittanbieter kann diese z. B. benutzen, um Benutzerprofile zu erstellen, diese eventuell zu verkaufen oder für gezieltes Einblenden von Werbung auf anderen Websites zu nutzen. So erscheinen z. B. plötzlich auf der eigenen Facebook-Seite Anzeigen für Winterkleidung, wenn man zuvor bei einem Modeanbieter nach warmen Jacken gesucht hat. Drittanbieter-Cookies sind daher oft unerwünscht und sollten blockiert werden.

## **2. Unser Standpunkt:**

In der breiten Gesellschaft werden Cookiebanner primär als negativ und unnötig wahrgenommen, beziehungsweise um es deutlich zu sagen: Sie nerven!

Dabei stellen sie einen großen Sieg für die Rechte der Bürger dar, da mit ihnen endlich ein längst überfälliges Recht zur Wahl gegeben wird: Endlich können nicht nur technisch Versierte sondern auch Fachfremde selbst entscheiden, welche Daten in ihren Browsern hinterlegt werden sollen.

In unseren Augen ist der Gesetzgeber hierbei allerdings nicht weit genug gegangen: Während die Auswahlmöglichkeit toll ist, fehlt es eindeutig an einer Vereinfachung für die Bürger, die derzeit in aufdringlichen Bannern mit semi-legalen „Dark Patterns“ ertrinken.

Wir fordern daher die Schaffung einer Möglichkeit, seitenübergreifend die eigenen Cookie-Präferenzen verpflichtend für alle Websites festzulegen. Diesbezüglich gibt es zwar mittlerweile diverse Browser-Addons (=Erweiterungen für den Browser) wie Consent-o-matic [2], die zumindest einen Großteil der Websites abdecken, aber nur technisch versierten Nutzern zur Verfügung stehen.

[1]: <https://de.wikipedia.org/wiki/HTTP-Cookie>

[2]: <https://netzpolitik.org/2022/nervenschoner-neue-browser-erweiterung-entfernt-cookie-banner/>

