Was sind Cookies?

Ein HTTP-Cookie ist eine Textdatei, die beim Besuch einer Website auf dem Endgerät des Website-Besuchers abspeichert wird. Diese Textdatei kann im Lauf der Zeit zahlreiche Informationen zu den Präferenzen des jeweiligen Website-Besuchers sowie zu seinem Onlineverhalten sammeln und vom Herausgeber des Cookies ausgewertet werden.

HTTP -Cookies haben die Aufgabe, dass Website-Besucher zu einem späteren Zeitpunkt eindeutig wieder erkannt werden.

Erstanbieter-Cookies und Drittanbieter-Cookies

HTTP -Cookies können sowohl vom Betreiber einer Website (Erstanbieter-Cookies) als auch von anderen Quellen (Drittanbieter-Cookies) im Endgerät des Website-Besuchers abgespeichert werden. Damit ein Drittanbieter-Cookies überhaupt angelegt werden kann, braucht es die aktive technische Beihilfe des Websitebetreibers.

Transiente und persistente Cookies

Transiente Cookies (vorübergehende Cookies) werden nach dem Schliessen des Browsers wieder gelöscht. Man spricht hier von Session-Cookies. Sie werden benötigt, um beispielsweise beim Besuch eines Onlineshops den Warenkorb zu befüllen und diesen Warenkorb beim Abschicken der Bestellung an den Betreiber des Onlineshops zu übermitteln.

Persistente Cookies (dauerhaft Cookies) bleiben auf dem Endgerät des Website-Besuchers über einen längeren Zeitraum (bis zu mehrere Jahre) gespeichert, falls der Website-Besucher diese nicht zwischenzeitlich und willentlich löscht. Persistente Cookies können genutzt werden, um Zugangsdaten (Benutzername, Passwort) zu Onlinediensten zu speichern. Sie können aber auch genutzt werden, um das Langzeitverhalten eines Website-Besuchers zu ergründen und dieser Person auf ihrem Display News und Werbung einzublenden, die den erfassten thematischen Vorlieben dieser Person weitgehend entsprechen.

Was bedeutet das für mich als Website-Besucher?

Transiente Cookies (vorübergehende Cookies) sind nicht daraus ausgelegt, Ihr Onlineverhalten über einen längeren Zeitraum zu ergründen.

Persistente Cookies (dauerhaft Cookies) hingegen zielen darauf ab, Sie über einen möglichst langen Zeitraum und über möglichst viele Endgeräte hinweg zu beobachten und daraus thematische Vorlieben abzuleiten. Das Endziel: Ihnen sollen möglichst oft «massgeschneiderte Informationen» angezeigt werden, die Ihren thematischen Vorlieben entsprechen und die aus Sicht von werbenden Unternehmen, Suchmaschinen und sozialen Netzwerken für Sie «relevant» sind.

Wenn Sie solche «massgeschneiderten und relevanten Informationen» mögen und auch sonst keine Mühe damit haben, dass Ihr Onlineverhalten über längere Zeiträume beobachtet und ausgewertet wird, brauchen Sie sich nicht um die Cookies auf Ihren Endgeräten zu kümmern.

Selbstbestimmender Umgang mit Cookies

Wenn Sie es nicht mögen, über längere Zeiträume beobachtet und klassifiziert zu werden, gibt es mehrere Möglichkeiten, um die Observation durch Cookies weitgehend einzudämmen.

Browsereinstellungen

Jeder moderne Browser gibt seinem Nutzer die Möglichkeit, sowohl das Speichern von Cookies grundsätzlich zuzulassen als auch teilweise oder gänzlich zu verhindern. Zudem hat jeder Nutzer die Möglichkeit, über die Einstellungen seines Browsers nur bestimmten Websites das Speichern von Cookies zu erlauben sowie den Befehl «Do Not Track» zu aktivieren.

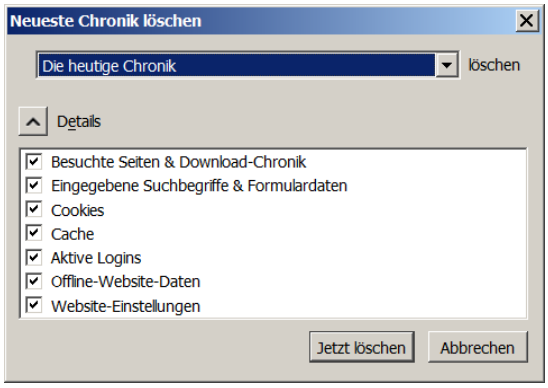
Wenn Sie beispielsweise schätzen, Benutzernamen und Passworte bei Onlinediensten nicht bei jedem Besuch neu eingeben zu müssen, können Sie für die betroffenen Websites das Speichern von Cookies in Ihrem Browser explizit zulassen, alle anderen Websites aber davon auszuschliessen.

Anleitungen zur Handhabung von Cookies in Browsern finden Sie unter den folgenden Links sowie in den Hilfedateien zu Ihrem Browser.

Firefox	https://support.mozilla.org/de/kb/Cookies erlauben und ablehnen
Safari	https://support.apple.com/de-de/HT201265
Google Chrome	https://support.google.com/chrome/answer/95647?hl=de
Internet Explorer	https://support.microsoft.com/de-ch/products/internet-explorer
Microsoft Edge	https://support.microsoft.com/de-ch/products/microsoft-edge
Andere Browser	Lesen Sie bitte die Anweisungen zu Ihrem Browser

Browserverlauf löschen

Unter MS Windows können Sie bei geöffnetem Browser mit dem gleichzeitigen Drücken der drei Tasten



«**Ctrl-Shift-Del**»

die auf Ihrem Endgerät gespeicherten Daten der vorangegangenen Websitebesuche löschen.

Legen Sie im Dropdown-Menü fest, für welchen Zeitraum diese Löschaktion gelten soll und bestimmen Sie unter «Details», welche Inhalte gelöscht werden sollen.

Das Betriebssystem macOS von Apple kennt diese Komfortfunktion nicht. Einzig beim Firefox-Browser unter macOS können Sie mittels gleichzeitigem Drücken der drei Tasten

«**command-shift-delete**»

den Browserverlauf ähnlich komfortabel löschen wie beim Betriebssystem MS Windows. Beim Browser Safari müssen Sie über «Safari» respektive «Verlauf» auf die Löschfunktion zugreifen, bei allen anderen Browsern unter macOS über die Dreipunkte-Steuerung im Browserfenster oben rechts.

Andere Einstellungen

Opt-Out Cookies

Gewisse Dienste, die Drittanbieter-Cookies einsetzen, bieten Ihnen die Möglichkeit, auf Ihrem Endgerät ein so genanntes Opt-Out Cookie zu speichern. Dieses Opt Out Cookie signalisiert dem Diensteanbieter, dass sie keine Cookies dieses Anbieters zulassen wollen.
Diese Variante setzt allerdings voraus, dass Sie für jeden einzelnen dieser Dienste ein solches Opt-Out Cookie zulassen müssen und dass Sie Cookies nie löschen dürfen. Wird beispielsweise der Browserverlauf gelöscht, werden auch die Opt-Out Cookies gelöscht und die Opt-Out Optionen existieren allesamt nicht mehr.

Privatmodus/Inkognitomodus

Alle modernen Browser bieten die Möglichkeit, einen Privat- respektive Inkognitomodus zu aktivieren.

Anleitungen zur Handhabung dieser Modi finden Sie unter den folgenden Links sowie in den Hilfedateien zu Ihrem Browser.

Firefox	Desktop-Browser https://support.mozilla.org/de/kb/privater-modus
	iPhone, iPad https://support.mozilla.org/de/kb/privates-surfen-firefox-fuer-ios
Safari	Desktop-Browser https://support.apple.com/de-ch/guide/safari/ibrw1069/mac
	iPhone, iPad https://support.apple.com/de-ch/ht203036
Google Chrome	Desktop-Browser https://support.google.com/chrome/answer/95464?hl=de&co=GENIE.Platform%3DDesktop&oco=1
	Android-Geräte https://support.google.com/chrome/answer/95464?hl=de&co=GENIE.Platform%3DAndroid&oco=1
	iPhone, iPad https://support.google.com/chrome/answer/95464?hl=de&co=GENIE.Platform%3DiOS&oco=1
Internet Explorer	Gleichzeitig die drei Tasten «Ctrl-Shift-P» drücken
Microsoft Edge	https://support.microsoft.com/de-ch/help/4026200/windows-browse-inprivate-in-microsoft-edge
Andere Browser	Lesen Sie bitte die Anweisungen zu Ihrem Browser

Grenzen des selbstbestimmenden Umgangs mit Cookies und Targeting

Auf Endgeräten mit dem **Betriebssystem Android** ist es kaum möglich, mit einem zumutbaren Aufwand und allein über den Browser das teilweise Zulassen, das Ausschliessen oder das Löschen von Cookies und anderen Funktionen zur Aufzeichnung von persönlichen Daten zu steuern. Zahlreiche vorinstallierte App der Entwicklerin des Betriebssystems sowie der Anbieter der Endgeräte sammeln bei nahezu jeder Gelegenheit zusätzliche Daten, die zur Erstellung von Verhaltens- und Aufenthaltsprofilen genutzt werden.

Wer beispielsweise bei **sozialen Netzwerken** angemeldet (eingeloggt) ist und im Internet surft, dessen Onlineverhalten wird – bei allen Betriebssystemen – ebenfalls ununterbrochen observiert und die erfassten Daten werden an die App-Betreiber übermittelt. Diese verknüpfen die aktuell erfassten Datenspuren mit solchen aus anderen Quellen und solchen aus der Vergangenheit und ergänzen das Profil der erfassten Person.

In diesem Zusammenhang wird oft mit «**zusätzlichen Komfortfunktionen**» und einem «**verbesserten Nutzererlebnis**» argumentiert und man wird eindringlich gebeten, die eine oder andere Funktion auf Ebene Betriebssystem, im Browser oder innerhalb einer App unbedingt zuzulassen respektive wieder zu aktivieren.

Tatsächlich kann der Begriff «**Faulheit**» auch mit dem Synonym «**Komfort**» umschrieben werden und das «**verbesserte Nutzererlebnis**» mündet meistens im Versprechen, dass man «**nur noch relevante und interessante Inhalte**» zu sehen bekomme – im Klartext jene Inhalte, die sich zu einem möglichst hohen Preis an möglichst viele Werbetreibende verkaufen lassen.

Links

«HTTP-Cookies» bei Wikipedia
https://de.wikipedia.org/wiki/HTTP-Cookie

«Do Not Track» bei Wikipedia
https://de.wikipedia.org/wiki/Do_Not_Track_(Software)