

Cookies nur noch mit Einwilligung rechtmäßig?

I. Ausgangssituation

In der Rechtssache C-673/17¹ („Planet49“) hatte der Europäische Gerichtshof (EuGH) nicht darüber zu entscheiden, ob eine Einwilligung vorliegen müsse, sondern ausschließlich über die Frage diskutiert, wie eine solche Einwilligung ausgestaltet werden müsse. Im Rahmen eines Vorabentscheidungsersuchens nach Art. 267 AEUV, eingereicht vom Bundesgerichtshof (BGH) ging es darum:

- ob ein bereits gekreuztes Kästchen, welches derartige Cookies setzt, eine „wirksame Einwilligung“ darstellt,
- ob es einen Unterschied macht, ob ein Cookie „personenbezogene Daten“ verarbeitet oder nicht,
- ob die Einwilligung nach der Datenschutz-Grundverordnung (DS-GVO) wirksam wäre
- und welche Informationen für eine wirksame Einwilligung zu erteilen sind.

II. Rechtsprechung des EuGH

Das Urteil des EuGH v. 1.10.2019 hat für viel Aufmerksamkeit gesorgt. Vielfach wurde die Entscheidung aus Luxemburg so interpretiert, dass danach Cookies zukünftig nur noch mit Einwilligung der betroffenen Person rechtmäßig gesetzt werden können.

Was verlangt der EuGH aber nun konkret?

Nutzer müssen zukünftig die Möglichkeit haben, aktiv in Werbe-Cookies einzuwilligen. Entscheidungsgegenstand für EuGH-Richter war die Frage, wie die notwendige Einwilligung in werbliche Cookies auszusehen hat und welche Informationspflichten in diesem Fall zu erfüllen sind. Das betont das Gericht auch ausdrücklich in seinem Urteil.² Nach der EuGH-Entscheidung liegt keine wirksame Einwilligung vor, wenn der Nutzer zur Verweigerung seiner Einwilligung ein bereits angekreuztes Kästchen abwählen muss. Vielmehr wird als Voraussetzung für eine wirksame datenschutzrechtliche Einwilligung auch online ein aktives Verhalten des Betroffenen vorausgesetzt.

Dies bedeutet für die Praxis, grundsätzlich ein sogenanntes „informed opt-in“, also eine informierte Einwilligung des Nutzers, beim Setzen von Cookies einzuholen. In Deutschland lässt sich seit diesem Urteil auch nicht mehr auf § 15 Telemediengesetz (TMG) verweisen, welcher nach wie vor geltendes Recht darstellt und nur die Opt-Out-Möglichkeit vorsieht. Schließlich verlangte die ePrivacy-Richtlinie (RL 2002/58/EG) in der Fassung der Änderung durch die Cookie-Richtlinie (RL 2009/136/EG) schon lange eindeutig eine Einwilligung, was aber bis heute nicht im nationalen Recht umgesetzt wurde.

¹ EuGH, Urteil v. 1.10.2019 – Planet49 GmbH.

² EuGH, Urteil v. 1.10.2019, Rn. 75 – Planet49 GmbH

Nicht alle Cookies benötigen eine Einwilligung

Technisch notwendige Cookies können hingegen wohl weiterhin auf Grundlage eines **überwiegenden berechtigten Interesses im Sinne des Art. 6 Abs. 1 lit. f DS-GVO** genutzt werden. Cookies selbst enthalten häufig keine nennenswerten Informationen über die Person. Dennoch unterliegen sie – u.a. wegen der möglichen Erfassung der IP-Adresse – dem Regelungsregime der DS-GVO. Dies hat der EuGH nun in seinem Urteil bestätigt und betont, dass alle anwendbaren Regelwerke einheitlich auszulegen sind. Es macht demnach keinen Unterschied, ob mit den Cookies nun tatsächlich personenbezogene Daten abgerufen würden oder nicht. Das Unionsrecht solle den Nutzer nämlich vor jedem Eingriff in seine Privatsphäre schützen, insbesondere gegen die Gefahr, dass „Hidden Identifiers“ oder ähnliche Instrumente in sein Gerät eindringen, so die Luxemburger Richter.

Transparenz verlangt

Der Websitebetreiber muss dem Nutzer klare und umfassende Informationen bereitstellen, damit die Einwilligung wirksam erteilt werden kann. Hierzu gehören auch die Angaben zur Funktionsdauer der Cookies und dazu, ob Dritte Zugriff auf die Cookies erhalten können.

III. Konsequenzen in der Praxis

Das Setzen und Abrufen von Cookies oder anderen Informationen, die im Endgerät des Nutzers gespeichert sind, bedarf **grundsätzlich** einer Einwilligung. Dem Grundsatz nach gibt es aber auch Ausnahmen, in denen Cookies keine Einwilligung verlangen.

1. Cookies mit Einwilligung

Eine **Einwilligung muss ein Opt-In sein** und darf nicht als Opt-Out gestaltet sein. Es braucht nun zukünftig immer eine aktive Handlung, wenn eine rechtmäßige Einwilligung für Cookies eingeholt werden soll. Diese ist bei vorangekreuzten Häkchen jedenfalls nicht gegeben. Nach Auffassung des EuGH ist es irrelevant, ob ein Cookie personenbezogene Daten zum Gegenstand hat oder nicht. Denn die relevante Richtlinie zur elektronischen Kommunikation 2002/58/EG spricht in Art. 5 Abs. 3 S. 1 lediglich von „Speicherung von Informationen“ und vom „Zugriff auf Informationen, die bereits [...] gespeichert sind“. D.h., hier kommt es eben nicht darauf an, ob personenbezogene Daten tatsächlich vorliegen.³

Praxisbeispiel: Danach bedarf es für websiteübergreifende Cookies und Tools, die das Nutzerverhalten website- oder geräteübergreifend zusammenfassen (Tracking), in der Regel einer vorherigen informierten Einwilligung der Nutzer.

2. Cookies ohne Einwilligung

In Ausnahmefällen ist das Setzen von Cookies auch ohne Einwilligung rechtmäßig. Cookies, die nicht erforderlich für die Bereitstellung des vom Nutzer aufgerufenen Dienstes sind, bedürfen in aller Regel keiner Einwilligung. Bei der Verwendung von IP-Adressen, Cookies oder anderen Nutzungsdaten, die für den Betrieb des Telemediendienstes **notwendig** sind, können sich Verantwortliche häufig auf das berechnete Interesse nach Artikel 6 Abs. 1 lit. f DS-GVO berufen.⁴

³ EuGH, Urteil v. 1.10.2019, Rn. 68 – Planet49 GmbH

⁴ LDI NRW, EuGH-Urteil zur wirksamen Einwilligung in die Verwendung von Cookies auf Websites, online abrufbar unter: https://www.lidi.nrw.de/mainmenu_Aktuelles/Inhalt/EuGH-Urteil-zur-wirksamen-Einwilligung-in-die-Verwendung-von-Cookies-auf-Websites/EuGH-Urteil-zur-wirksamen-Einwilligung-in-die-Verwendung-von-Cookies-auf-Websites.html.

Wichtig ist die Differenzierung: Dies gilt nicht für Cookies, die nicht „**unbedingt erforderlich**“ sind (Art. 5 Abs. 3 S. 2 RL 2002/58/EG). Nur technisch erforderliche Speicherungen von Informationen können somit ohne Einwilligung stattdessen aufgrund eines berechtigten Interesses nach Art. 6 Abs. 1 lit. f DS-GVO rechtmäßig gesetzt werden.

Praxisbeispiel: Dies könnten bspw. **Warenkorb-Cookies oder Session-Cookies** sein.

Schwierigere Grenzfälle: Sind Retargeting-Identifizierer jeglicher Art und Weise technisch erforderlich? **Tendenz: nein!**

- Argument: Retargeting-Identifizierer sind für Unternehmen hilfreich, um Produkte und Dienstleistungen digital zielgenau an den Kunden richten zu können. Aber sie sind wohl nicht unbedingt erforderlich, um ein Website-Angebot zu erbringen.⁵

3. Transparenzpflichten nicht vergessen

Neben der Rechtmäßigkeit muss eine Verarbeitung personenbezogener Daten nach Art. 5 Abs. 1 lit. a DS-GVO auch transparent sein. **Die Informationspflichten nach Art. 12 ff. DS-GVO sind deswegen zusätzlich zu ggf. einzuholenden Einwilligungen einzuhalten!** Dementsprechend sollte die Datenschutzerklärung darüber aufklären, ob und wenn ja, welche Cookies verarbeitet werden. Zudem ist die Rechtsgrundlage der jeweiligen Verarbeitung zu nennen: Einwilligung oder berechtigtes Interesse? Und schließlich ist die Löschfrist für die Cookies noch von Bedeutung!

⁵ *Diercks*, Zum EuGH Urteil „Planet49“, Az. C-673/17 – Benötigen Cookies ab jetzt immer einer Einwilligung? (Spoiler: Nein), 1.10.2019, online abrufbar unter: <https://diercks-digital-recht.de/2019/10/zum-eugh-urteil-planet49-az-c-673-17-benoetigen-cookies-ab-jetzt-immer-einer-einwilligung-spoiler-nein/>.

Seminartipp zum Arbeitspapier

Die ePrivacy-Verordnung im Zusammenspiel mit der DS-GVO

Unternehmen müssen seit Mai 2018 nicht nur die DS-GVO umgesetzt haben. Zusätzlich zur DS-GVO sind die Vorschriften der ePrivacy-Verordnung (VO) zu beachten. Sie wird den Datenschutz für Onlinedienste von der Homepage bis zu sozialen Netzwerken regeln und die DS-GVO für den Bereich der elektronischen Kommunikation präzisieren und ergänzen. Das erweiterte EU-Recht enthält nicht nur verbindliche Vorgaben für Anbieter von Kommunikationsdiensten, sondern richtet sich an jedermann, der Tools zur Reichweitenmessung einsetzt oder jede Art von Gerätedaten verarbeitet.

Das Seminar gibt einen Überblick über die wesentlichen Neuerungen und bietet dem Verantwortlichen praxistaugliche Hinweise zur Umsetzung.

Weitere Infos finden Sie [hier](#).



Websites datenschutzkonform gestalten

Nahezu jeder bietet heutzutage eine Website an. Die DS-GVO nennt zwar eine Vielzahl an abstrakten Pflichten. Diese müssen spezifisch auf den Online-Bereich übertragen werden. Dabei stellen sich viele Fragen bei der Umsetzung:

- Wie muss die Datenschutzerklärung aussehen? Wo gehört sie hin?
- Wie erkenne ich, ob und welche Dienste, z.B. Videos, Social Plugins oder sonstige Dienste von Drittanbietern eingebunden sind?
- Was ist beim Einsatz von Cookies zu beachten?
- Wie muss das Opt-Out-Verfahren ausgestaltet sein?
- Wann wird eine Einwilligung vom Nutzer benötigt?
- Welche technischen Anforderungen gelten z.B. bei der elektronischen Kommunikation?

In dem Seminar werden die datenschutzrechtlichen Anforderungen erläutert und die häufigsten Fragen rund um das Thema Websites beantwortet. Dabei lernen die Teilnehmer nicht nur die wesentlichen Anforderungen für Websites kennen. Auch allgemeine Kenntnisse über die Funktionsweise des Internets und den Aufbau von Websites werden vermittelt. Außerdem werden kostenlose Tools und Prüftechniken eingesetzt. Wer diese Tipps und Tricks kennt, kann ohne weiteres selbst prüfen, ob Websites die rechtlichen und technischen Anforderungen der DS-GVO erfüllen.

Weitere Infos finden Sie [hier](#).



DataAgenda

ist das Informationsportal zum Datenschutzrecht und fokussiert sich auf die inhaltlichen Entwicklungen in diesem Feld. Das DataAgenda-Experten-Team bietet Videos, News, Whitepaper und Seminartipps rund um den Datenschutz.

Datakontext

ist einer der führenden Fachinformationsdienstleister in den Bereichen Datenschutz und IT-Sicherheit und bietet Kompetenz aus einer Hand: Fachbücher, Fachzeitschriften und Seminare, Zertifizierung und Beratung.



Autoren

Prof. Dr. Rolf Schwartmann

Vorsitzender der Gesellschaft für Datenschutz und Datensicherheit e.V. (GDD), Leiter der Kölner Forschungsstelle für Medienrecht (TH Köln) und Mitglied der Datenethikkommission.



Dr. Tobias Jacquemain, LL.M.

Wissenschaftlicher Referent bei der Gesellschaft für Datenschutz und Datensicherheit e.V. (GDD), Bonn

