von **Birgit Gressner**

# Geplante ePrivacy-Verordnung: was gibt es Neues im Herbst?

Welche Positionen vertreten die Mitgliedsstaaten zu den umfangreichen Änderungsvorschlägen der finnischen Ratspräsidentschaft vom 18. September 2019 und lässt sich schon eine Tendenz zur Regelung von Cookies, Tracking, Browsereinstellungen erkennen?

## Der aktuelle finnische Vorschlag

Die finnische Ratspräsidentschaft für die 2. Jahreshälfte 2019 setzt den Themenschwerpunkt auf den Ausbau des digitalen Binnenmarktes. Sie nennt hierbei Online-Marktplätze als einen der wichtigen Wachstumstrends der EU, der für positive wirtschaftliche Effekte sorgt. Finnland setzt sich für Fortschritte bei der Einigung auf eine ePrivacy-Verordnung und hat am 18. September 2019 einen überarbeiteten Entwurf vorgelegt.

Welche Akzente setzt der finnische Entwurf? Schafft er den Spagat zu einer wachstumsfreundlichen Regulierung bei gleichzeitigem Verbraucherschutz? Was heißt das für die Praxis?

Die Kompromissvorschläge der finnischen Präsidentschaft zu den Themen **Cookies, Tracking, Browsereinstellungen**, sehen wie folgt aus (Recitals 20-24):

a. Der Entwurf stellt klar, dass nunmehr als **Alternative** zur Einwilligung des Endnutzers weitere bestimmte und transparente Zwecke als Rechtfertigung für den Einsatz von Cookies ausreichen sollen. (Rec. 20) Vgl. dazu unten Rec. 21 und 21a.

b. Für die Einholung der Einwilligung ist der **Verwender** der Cookies zuständig, der sich aber Dritter dafür bedienen kann. (Rec.20)

c. Die Einwilligung darf sich auch auf die **Nachfolgesitzung** für den Besuch einer Webseite erstrecken. (Rec. 20)

d. Zu sog. **„cookie walls“** (Cookie Mauern), die vorliegen, wenn der Betreiber den Besuch seiner Webseite generell von der Zustimmung des Endnutzers zu Cookies abhängig macht, stellt der Entwurf auf Wahlmöglichkeiten ab (Rec. 20):

- hat der Nutzer einer kostenlosen Webseite die Wahl zwischen der Nutzung mit solchen Cookies und einem vergleichbaren **Angebot ohne diese Cookies**, dann sind „cookie walls“ nicht unverhältnismäßig;
- bestehen **keine alternativen Wahlmöglichkeiten** für den Endnutzer, wie z.B. typischerweise bei Behörden Webseiten, dann können „cookie walls“ unverhältnismäßig sein.

e. Bezogen auf Verfolgungs-Cookies **(„tracking technologies“)** ermuntert der Entwurf die Betreiber der Webseite zum Einsatz nutzerfreundlicher Voreinstellungen zur Einwilligung für einzelne oder mehrere

bestimmte Zwecke oder einen bzw. mehrere Services unter der Voraussetzung der Verfügbarkeit und technischen Machbarkeit. Solche Einwilligungen („whitelists“) für einzelne Anbieter müssen jederzeit widerrufbar sein. (Rec. 20a) Vgl. dazu unten die Abschaffung der Standardvoreinstellungen des Browsers für Cookies (Rec. 22-24).

f. Cookies dürfen **ohne Einwilligung** eingesetzt werden, wenn sie keine oder nur geringe Auswirkungen auf die Privatsphäre haben und nicht unverhältnismäßig eingesetzt werden (Beschränkung auf die konkrete Web-Session), beispielsweise zu folgenden Zwecken:

- wenn die Cookies technisch oder für die Kommunikation erforderlich sind, wie z.B.

?zum Ausfüllen von mehrseitigen online Anträgen,
?zur Authentifizierung des Nutzers
?beim Befüllen von Warenkörben (Rec.21)

- zur Behebung von Sicherheitslücken und sonstigen Sicherheitsfehlern (inklusive Betrugsverhinderung), sofern diese die Privatsphäre-Einstellungen nicht verändern und die automatische Installation zeitlich verschoben bzw. abgeschaltet werden kann. Das gilt nicht für Updates zur Funktionserweiterung (neue Features) oder Performance Verbesserung. (Rec. 21a)

g. Der Betreiber einer Webseite, die sich teilweise oder ganz **durch Werbung** finanziert, kann Tracking-Cookies ohne Einwilligung des Nutzers auf dessen Computer abspeichern, wenn der Nutzer über diesen Einsatz informiert wird und er diesem Einsatz zugestimmt hat. Der Begriff „accept“ der englischen Textfassung, der darauf hindeuten könnte, dass auch eine nachträgliche Einwilligung des Nutzers ausreichend wäre (opt-out), wurde noch nicht verabschiedet. (Rec.21)

h. Eine **zweckfremde** Nutzung der Cookies erfordert in jedem Fall die Einwilligung des Nutzers. (Rec. 21)

i. Cookies, die Rückschlüsse auf die Identität des Nutzers zulassen, erfordern dessen Einwilligung. (Rec. 21a)

j. Die vom EU-Parlament und EU-Kommission angestrebten Regelungen von nutzerfreundlichen Voreinstellungen des Browsers, u.a. auch zur Ablehnung von Cookies, die von Dritten eingesetzt werden, werden gestrichen. (Rec. 22, 22a, 23, 24)

Der EU-Ministerrat (Telekommunikation) berät am 24. September 2019 wieder über die E-Privacy Reform. Die IT-Recht Kanzlei hält Sie weiterhin über die für Onlinehändler relevanten aktuellen Entwicklungen informiert.

**Zusammengefasst:** Die von EU-Parlament und EU-Kommission angestrebten Regelungen zur Verhinderung von pauschalisierten Cookie-Banner, zur Voreinstellung von nutzerfreundlichen Voreinstellungen des Browsers und zur genauen Information hinsichtlich zum Anwendungsbereich und Zweck von Cookies werden aufgeweicht bzw. weitgehend gestrichen. Neue Ausnahmen von der Einwilligungspflicht werden definiert. Sog. „cookie walls“ (Cookie Mauern) die verhindern, dass der Betreiber generell den Besuch seiner Webseite von der Zustimmung des Nutzers abhängig macht, können unverhältnismäßig sein.

# Welche Position vertritt Deutschland bisher?

Die deutsche Verhandlungsdelegation hat im Juni in Luxemburg eine umfassende Stellungnahme zur E-Privacy-Verordnung in Aussicht gestellt, die so bald wie möglich veröffentlicht werden soll.

Am 2. Juli 2019 hat das Justiz- und Verbraucherschutzministerium (BMJV) eine kleine Anfrage beantwortet und sich dabei zur E-Privacy Reform in der Vorabfassung auf Fragen nach (i) einer stärkeren Regulierung von Tracking und (ii) noch konkreteren Regelungen für die elektronische Kommunikation in der E-Privacy-Verordnung wie folgt positioniert:

## 1. Tracking

Der Begriff wird in der politischen Diskussion als die Erfassung und Speicherung des kompletten Verhaltens und der Interaktionen eines Nutzers bei Nutzung eines vernetzten Geräts oder eines Dienstes verstanden. Dies kann insbesondere die Interaktionen mit einer Webseite (z. B. Nachrichtenseite oder soziales Netzwerk), die Surfhistorie, die Kommunikation über webbasierte E-Mail- und Messangerdienste, die Verweildauer auf einer Webseite, die Art und Weise des Eintippens oder die Lesegeschwindigkeit umfassen. Bei Nutzung eines mobilen vernetzten Endgerätes können zusätzlich Informationen über den geografischen Standort und über Uhrzeit, Datum und Dauer eines Anrufs hinzukommen.

## 2. Abgrenzung EU-DSGVO zu E-Privacy Regelung

In der Datenschutz-Grundverordnung ist die Erfassung und Verarbeitung von personenbezogenen Daten bei der Nutzung von vernetzten Geräten im Internet geregelt. Wenn das Tracking auf der Speicherung von Informationen oder dem Zugriff auf Informationen im Endgerät eines Nutzers, z. B. mittels Cookies, basiert, gelten die E-Privacy-Regelungen.

## 3. Gegenüberstellung alte und neue Einwilligungs-Regelung

ALT: Geräte-Identifier wie Cookies dürfen grundsätzlich nur mit Einwilligung des Nutzers verwendet werden, es sei denn, solche Verfahren sind aus bestimmten Gründen technisch erforderlich (Artikel 5 Absatz 3 der geltenden ePrivacy-Richtlinie) (=Richtlinie 2002/ 58/EG in der durch die Richtlinie 2009/136/EG geänderten Fassung)

NEU: In engen Grenzen ist der Zugriff auf Endeinrichtungen des Endnutzers durch Dritte erlaubt, um dort Informationen ohne die Einwilligung des Endnutzers zu speichern und abzurufen (Artikel 8 des Entwurfs einer E-Privacy-Verordnung, über die derzeit im Rat verhandelt wird). Kein Tracking ohne Einwilligung.

## 4. Position Bundesregierung

a. Die E-Privacy-VO müsse ein hohes, über die DSGVO hinausreichendes Schutzniveau gewährleisten (7. Juni 2019 in Luxemburg); ein rasches Fortschreiten der Verhandlungen wird begrüßt. Aber

- der aktuelle Entwurf wird nicht unterstützt
- Änderungen speziell bei Artikel 6 bezüglich der „kompatiblen Weiterverarbeitung" nötig
- Erhalt von Artikel 10 (Einstellungsmöglichkeiten zur Privatsphäre) gewünscht

b. Die von der Kommission vorgeschlagene Regelung des Artikels 8 soll nicht abgeschwächt werden (Bundesregierung im Rat im Rahmen der laufenden Verhandlungen).

c. Eine Regelung zum Schutz der Privatsphäre bei Internetbrowsern soll in die zukünftige Verordnung aufgenommen werden. Endnutzer sollen ihre Privatsphäre über entsprechende Einstellungen in der Browsersoftware bewusst und wirksam schützen können (entspricht ursprünglichem Vorschlag der Kommission; konkreter Vorschlag der Bundesregierung liegt vor).

Interessant: Ob die Geschehnisse um das Unternehmen Cambridge Analytica weitere Regelungen in der EU-DSGVO zum Schutz der Nutzer von Internet und vernetzten Geräten erfordern, bedarf laut Bundesregierung weiterer Prüfung, insbesondere von Regelungen zur Profilbildung und zur weiteren Stärkung der Betroffenenrechte.

# Zur Erinnerung: Was sagt der BITKOM bisher?

Die letzte von der BITKOM publizierte Stellungnahme vom März 2019 bezieht sich noch auf die Entwurfspositionen der rumänischen Ratspräsidentschaft, die der finnischen im 1. Halbjahr 2019 voranging. Die BITKOM verlangt:

- Kohärenz und Regelungshierarchie zwischen E-Privacy-Verordnung und DSGVO.
- Keine neue Einwilligung für Software Updates.
- „Endnutzer" muss charakterisiert werden: Unternehmen müssen als Arbeitgeber für ihre Mitarbeiter für Geschäftszwecke einwilligen können.
- Erweiterung von Art 8 Abs.1 lit.c auf Software Updates.
- Innovationspotential, insbesondere für KI, autonomes Fahren und IoT Plattformen darf nicht behindert werden, d.h. insbesondere muss kompatible Weiterverarbeitung für M2M-Kommunikation möglich sein. Die Basis der Datenverarbeitung für Unternehmen soll vertraglich festgelegt werden können.
- Die Weiterverarbeitung von Metadaten und eine rechtliche Grundlage für eine Verarbeitung aus berechtigtem Interesse muss ermöglicht werden.

Autor:
**Birgit Gressner**
freie jur. Mitarbeiterin der IT-Recht Kanzlei