

Dr. Martin Bahr

Die neue E-Privacy-Verordnung: Das Ende aller Online-Tracking- Methoden wie wir sie kennen?

Das neue europaweite Datenschutzrecht – die sogenannte EU-Datenschutzgrundverordnung – wird zum 25. Mai 2018 in Kraft treten.

Parallel dazu ist von Brüssel das Inkrafttreten der neuen E-Privacy-Verordnung (E-Privacy-VO) angedacht. Das Gesetz befindet sich noch im Entwurfsstadium, hat aber bereits erbitterten Widerstand in der Online-Werbeindustrie gefunden. Und diese Kritik ist mehr als berechtigt, wie der nachfolgende Beitrag unseres Online Rechtsexperten, Dr. Martin Bahr, aufzeigt.

Wenn Sie sonst rechtlich orientierte Beiträge vielleicht eher überblättern, sollten Sie diesen auf jeden Fall ganz genau lesen. Was da schon bald auf Sie zukommt, ist kaum zu glauben!

A. Das neue Gesetz: die E-Privacy-Verordnung

Bekanntlich tritt das neue europaweite Datenschutzrecht – kurz EU-Datenschutzgrundverordnung – Ende Mai nächsten Jahres in Kraft. Sämtliche Gesetze sind bereits wirksam verabschiedet und gültig. Es ist also klar, welcher Inhalt und welche Konsequenzen sich hierdurch ergeben.

Ganz anders ist dies für die neue E-Privacy-Verordnung, die aus Brüssel kommt. Dieses neue Gesetzeswerk soll zukünftig speziell den Bereich der elektronischen Kommunikationsdienste regeln, also eine Art datenschutzrechtliche Spezialregelung sein.

1. Aktueller Gesetzgebungsstand:

Am 10. Januar 2017 hat die EU-Kommission ihren ersten Entwurf zur E-Privacy-Verordnung vorgestellt. Das Gesetzeswerk befindet sich auf EU-Ebene derzeit in der näheren Abstimmung. Angestrebt ist ein Inkrafttreten zum 25. Mai 2018, also in weniger als einem Jahr.

Der Entwurf wird in der Öffentlichkeit und von allen Seiten kontrovers diskutiert. Die nachfolgenden Ausführungen erfolgen daher unter dem Hinweis, dass sich in den kommenden Beratungen durchaus noch erhebliche Änderungen ergeben können.

In jedem Fall soll die E-Privacy-VO nach Verabschiedung unmittelbar anwendbar sein, d. h., es bedarf keiner Umsetzung durch den deutschen Gesetzgeber mehr, sondern die Regelung gilt nach Inkrafttreten sofort und direkt in Gesamteuropa.

2. Gilt für (alle) Direktmarketing-Kanäle:

Anders als man zunächst vermuten könnte, gelten die neuen Bestimmungen nicht nur für den Online-Bereich, sondern vielmehr für alle elektronischen Kommunikationsdienste. Damit unterfallen alle gängigen Direktmarketing-Kanäle wie E-Mail, Telefon, Fax oder SMS dem Regelungsbereich. Lediglich die alte klassische Postwerbung bleibt unberührt.

3. Regelungen weit über das Datenschutzrecht hinaus:

Die E-Privacy-Verordnung behauptet zwar an mehreren Stellen, dass sie lediglich datenschutzrechtliche Spezialthemen regeln will. Ein Blick in den Entwurf zeigt aber, dass die Bestimmungen weit über den Bereich des Datenschutzrechts hinausgehen.

DER AUTOR



Die **Kanzlei Dr. Bahr** (<http://www.Dr-Bahr.com>) ist auf den Bereich des Rechts der Neuen Medien und den gewerblichen Rechtsschutz (Marken-, Urheber- und Wettbewerbsrecht) spezialisiert. Unter Suchmaschinen-und-Recht.de betreibt sie seit 2005 ein eigenes Themenportal zur rechtlichen Dimension von Suchmaschinen.

So stellt das neue Gesetz zum Beispiel neue Regelungen für unverlangt zugesandte Werbung auf (Art. 16 E-Privacy-VO). Ebenso sollen telefonische Werbeanrufe eine bestimmte Rufnummer erhalten (Art. 12 ff. E-Privacy-VO).

Diese beiden Beispiele zeigen bereits, dass die neue Materie weit über das Datenschutzrecht hinausgeht und zahlreiche Bestimmungen aus dem Bereich des Wettbewerbsrechts beinhaltet.

Im Weiteren sollen diese Neuerungen aus Platzgründen nicht näher erörtert werden, sondern wir konzentrieren uns vielmehr auf die Bestimmungen, die für den Online-Bereich von Relevanz sind.

4. Die Neuerungen für den Online-Bereich:

a. Keine Third-Party-Cookies mehr:

Die größte und wichtigste Änderung findet sich in Art. 8 Abs. 1 E-Privacy-VO. Danach ist jede Nutzung von Informationen des Endnutzers, also insbesondere Cookies, grundsätzlich verboten. Nur in bestimmten, eng begrenzten Fällen soll zukünftig die Verwendung erlaubt sein:

- » Zur alleinigen Durchführung eines technischen Kommunikationsvorgangs
- » Wenn eine Einwilligung des Users vorliegt
- » Zur Durchführung eines vom User gewollten Dienstes
- » Zur Messung des Webpublikums durch Webseiten-Betreiber

Liegt keine Einwilligung vor, sollen zukünftig nur noch Session-Cookies erlaubt sein, Third-Party-Cookies hingegen sind verboten. Dies bedeutet im Klartext: Sollte sich diese Bestimmung durchsetzen, so dürfte dies das Ende der Online-Werbewirtschaft sein, wie wir sie heute kennen.

Denn zukünftig wäre jedes Online-Tracking, wie es heute tagtäglich millionenfach passiert, nur noch mit Einwilligung erlaubt. Und die rechtlichen

Anforderungen an eine wirksame Einwilligung in diesem Bereich sind kaum zu erfüllen. Es ist daher kein Wunder, dass die Werbewirtschaft derzeit Sturm läuft und kein gutes Haar an dem Entwurf lässt.

b. Einwilligung mittels Browser-Voreinstellung:

Third-Party-Cookies sind somit in Zukunft nur noch mit ausdrücklicher Zustimmung erlaubt. Dabei muss die Erklärung vor Beginn der Nutzung erfolgen, eine nachträgliche Einholung reicht nicht aus.

Der Einwilligung kommt somit eine entscheidende Bedeutung zu.

Nutzer, die ihre Einwilligung in die Nutzung ihrer Online-Informationen gegeben haben, müssen zukünftig alle sechs Monate auf die Möglichkeit des Widerrufs der Einwilligung hingewiesen werden (Art. 9 Abs. 3 E-Privacy-VO).

Einziger Lichtblick in diesem Zusammenhang ist, dass die Verordnung ausdrücklich regelt, dass auch in der Voreinstellung des Browsers eine Einwilligung liegen kann. In den Gesetzesmaterialien heißt es:

„Wegen der allgegenwärtigen Verwendung von Verfolgungs-Cookies und anderer Verfolgungstechniken werden die Endnutzer immer häufiger aufgefordert, ihre Einwilligung in die Speicherung solcher Verfolgungs-Cookies (...) zu geben. Infolge dessen werden die Endnutzer mit Einwilligungsanfragen überhäuft.

Mit Hilfe technischer Mittel für die Erteilung der Einwilligung, z. B. durch transparente und benutzerfreundliche Einstellungen, könnte dieses Problem behoben werden. Deshalb sollte diese Verordnung die Möglichkeit vorsehen, dass die Einwilligung durch die entsprechenden Einstellungen in einem Browser oder einer ande-

ren Anwendung erteilt werden kann.

Die Auswahl, die Endnutzer bei der Festlegung ihrer allgemeinen Einstellungen zur Privatsphäre in einem Browser oder einer anderen Anwendung getroffen haben, sollte für Dritte verbindlich und ihnen gegenüber auch durchsetzbar sein. Webbrowser sind eine Art von Softwareanwendung, die es ermöglicht, Informationen aus dem Internet abzurufen und darzustellen.“

Es ist daher auch wenig verwunderlich, dass das neue Gesetz ausdrücklich die Verpflichtung aufstellt, dass Software zukünftig auf die Einstellungsmöglichkeiten zur Privatsphäre hinweisen muss (Art. 10 Abs. 2 E-Privacy-VO). Wie das aussehen soll, findet sich in den Materialien auch wieder:

„Damit Webbrowser die (...) vorgeschriebene Einwilligung der Endnutzer (...) einholen können, sollten sie unter anderem eine eindeutige bestätigende Handlung von der Endnutzung des Endnutzers verlangen (...).

Eine solche Handlung kann als bestätigend verstanden werden, wenn Endnutzer zur Einwilligung beispielsweise die Option ‚Cookies von Drittanbietern annehmen‘ aktiv auswählen müssen und ihnen die dazu notwendigen Informationen gegeben werden. Hierzu müssen die Anbieter von Software, die den Zugang zum Internet ermöglicht, verpflichtet werden, die Endnutzer zum Zeitpunkt der Installation darauf hinzuweisen, dass die Einstellungen zur Privatsphäre unter den verschiedenen Möglichkeiten ausgewählt werden können, und sie aufzufordern, eine Wahl zu treffen. Die gegebenen Informationen

sollten die Endnutzer nicht davon abschrecken, höhere Einstellungen zur Privatsphäre zu wählen, und sie sollten alle wichtigen Informationen über die mit der Annahme von Cookies von Dritt-anbietern verbundenen Risiken enthalten, wozu auch das Anlegen langfristiger Aufzeichnungen über die Browserverläufe des Betroffenen und die Verwendung solcher Aufzeichnungen zur Übermittlung gezielter Werbung gehören.“

Das Gesetzeswerk geht sogar noch einen Schritt weiter und erlegt allen Anbietern, deren Software bereits auf dem heimischen PC installiert ist, ein Zwangs-Update auf. Bis zum 25.08.2018 müssen alle Betreiber auch ihre bereits installierte Software anpassen. Die Frage, wie das technisch überhaupt gehen soll, bleibt natürlich unbeantwortet.

Hinsichtlich der Ausgestaltung hingegen hat der Gesetzgeber bereits konkrete Vorstellungen:

„Gegenwärtig haben die meisten weitverbreiteten Browser für Cookies die Standardeinstellung ‚Alle Cookies annehmen‘.

Deshalb sollten Anbieter von Software (...) dazu verpflichtet sein, die Software so zu konfigurieren, dass sie die Möglichkeit bietet zu verhindern, dass Dritte Informationen in der Endeinrichtung speichern; diese Einstellung wird häufig als ‚Cookies von Drittanbietern zurückweisen‘ bezeichnet.

Den Endnutzern sollte eine Reihe von Einstellungsmöglichkeiten zur Privatsphäre angeboten werden, die vom höheren Schutz (z. B. ‚Cookies niemals annehmen‘) über einen mittleren Schutz (z. B. ‚Cookies von Drittanbietern zurückweisen‘ oder ‚Nur Cookies von Erstanbietern annehmen‘) bis zum niedrigeren Schutz (z. B. ‚Cookies

immer annehmen‘) reicht. Solche Einstellungen zur Privatsphäre sollten in leicht sichtbarer und verständlicher Weise dargestellt werden.“

5. Massive Sanktionen bei Verstößen:

Während die aktuelle Gesetzeslage Datenschutzverletzungen bislang eher als Kavaliersdelikt einstuft, ändert sich dies grundlegend und massiv durch die E-Privacy-VO.

Zukünftig hat jeder betroffene Endnutzer, dessen Daten zu Unrecht gespeichert wurden, einen Anspruch auf Schadensersatz. Kannte die bisherige Rechtsprechung nur in besonders krasen Einzelfällen Schadensersatzbeträge im dreistelligen oder geringen vierstelligen Euro-Bereich, wird sich dies zukünftig ändern. Schadensersatz wird dann auch bei den leichtesten Rechtsverletzungen gewährt.

Der Gesetzgeber hat ausdrücklich bestimmt, dass diese Regelung „eine wirklich abschreckende Wirkung“ haben soll, um Datenschutzverletzungen zukünftig zu vermeiden. Es dürfte nur eine Frage der Zeit sein, bis findige Anwälte „Schadensersatz-Vereine“ gründen und versucht werden, vermeintliche Ansprüche von Betroffenen gegen entsprechende Provision durchzusetzen.

Dies wird noch durch die zukünftige Beweislast verstärkt. Nicht mehr der betroffene Endnutzer muss in Zukunft nachweisen, dass eine unberechtigte Speicherung vorliegt, sondern die Rechenschaftspflicht obliegt zukünftig dem Unternehmer. Er muss belegen, dass alles einwandfrei war.

Und nicht nur das: Auch die möglichen Geldbußen durch die Datenschutzbehörden werden drastisch erhöht. Zukünftig sind Strafen von bis zu 10 Mio. Euro oder bis zu 2 % des weltweiten Jahresumsatzes möglich (Art. 23 E-Privacy-VO).

Brüssel macht also mehr als Ernst.

B. Ausblick in die Zukunft

Die E-Privacy-VO wird mit großer Wahrscheinlichkeit kommen, alles andere wäre eine echte Überraschung. Auch wenn der Zeitpunkt des Inkrafttretens, nämlich Mai 2018, mehr als sportlich ist, ist zu befürchten, dass der EU-Gesetzgeber an diesem Datum festhalten wird.

Ob das faktische Verbot von Third-Party-Cookies letzten Endes auch in der Schlussfassung des Gesetzes so wiederzufinden sein wird, ist aktuell noch unklar. Möglicherweise gelingt es der Online-Werbeindustrie noch auf den letzten Metern, diese Regelung ein wenig abzumildern.

Eines ist jedoch klar: Der EU-Gesetzgeber wird keine 180-Grad-Wendung vornehmen und komplett von seinen bisherigen Grundsätzen zurückweichen. Der Online-Bereich tut also gut daran, sich bereits heute auf die geänderten Rahmenbedingungen ab Mitte 2018 einzustellen und nicht die Augen zu verschließen vor dem Gewitter, das sich da gerade zusammenbraut.

Die wichtigsten Punkte der angesprochenen EU-Privacy-VO im Überblick:

1. Soll im Mai 2018 in Kraft treten.
2. Gilt unmittelbar für alle EU-Bürger, bedarf keiner Umsetzung durch den nationalen Gesetzgeber.
3. Betrifft den Bereich der elektronischen Kommunikationsdienste (nicht nur online, sondern auch Telefon, Fax oder SMS usw.).
4. Generelles Verbot für Cookies, eng beschränkte Ausnahmen.
5. Insbesondere Verbot von Third-Party-Cookies.
6. Einwilligung in Third-Party-Cookies möglich, aber hohe Voraussetzungen. Möglich durch Browser-Voreinstellung.
7. Sollte das Gesetz so kommen wie im Entwurf, stünden (fast) alle Online-Tracking-Methoden vor dem Aus. ¶

