

Die neue ePrivacy-Verordnung

1. Worum geht es bei der neuen ePrivacy-Verordnung?

Am 10. Januar 2017 hat die EU-Kommission offiziell den Entwurf für eine neue Verordnung des europäischen Parlaments und des Rates über die Achtung des Privatlebens und den Schutz personenbezogener Daten in der elektronischen Kommunikation und zur Aufhebung der Richtlinie 2002/58/EG (Verordnung über Privatsphäre und elektronische Kommunikation) vorgestellt (ePV). Die durch die neue Verordnung aufzuhebende Richtlinie bildet derzeit die Grundlage zahlreicher u.a. datenschutzrechtlicher Regeln im Telekommunikations- und Onlinebereich. Sie regelt die Vertraulichkeit der Kommunikation, die auch nicht personenbezogene Daten und Daten in Bezug auf juristische Personen enthalten kann. Seit der letzten Aktualisierung im Jahre 2009 ist sie auch unter der Bezeichnung „Cookie-Richtlinie“ bekannt. Die neue Verordnung nimmt diese Regelungsmaterie auf und erweitert sie. Im Mittelpunkt steht neben dem Schutz der Vertraulichkeit der Kommunikation nun vor allem ein erweiterter Endgeräteschutz.

2. Wen betrifft die neue ePrivacy-Verordnung?

Der künftige Anwendungsbereich der neuen Verordnung ist nicht allein auf Betreiber herkömmlicher Telekommunikationsnetze beschränkt. Erklärtes Ziel ist vor allem die Erfassung so genannter OTTs (over-the-top-Dienste). Unter den neuen Begriff der elektronischen Kommunikationsdienste sollen nun auch Internetzugangsdienste und Dienste, die ganz oder teilweise in der Übertragung von Signalen bestehen, sowie interpersonelle Kommunikationsdienste, die nummerngebunden oder nummernunabhängig sein können, beispielsweise VoIP-Telefonie, Nachrichtenübermittlung und webgestützte E-Mail-Dienste fallen. Die Verordnung soll dabei auch für die Übermittlung von Maschine-Maschine-Kommunikation gelten. Da unter Kommunikation damit jeder datengestützte Informationsaustausch verstanden wird, ist praktisch die gesamte Online-Branche erfasst.

Ansprechpartner:

RA Michael Neuber
Justiziar/ Leiter Recht
und Regulierung
BVDW e.V.
T: +49 30 206218612
neuber@bvdw.org

3. Was sind die wesentlichen Gefahren für die Online-Branche?

Sollte der Entwurf wie beabsichtigt Realität werden, bedeutet es nichts anderes als das Ende des werbefinanzierten Internets. Gemäß Art. 8 Abs. 1 ePV sollen Webseitenbetreiber nur noch dann Cookies einsetzen können, wenn sie eine explizite Erlaubnis des Nutzers erhalten haben. Ausnahmen sollen nur dort greifen, diese ausschließlich der Erbringung des vom Nutzer angeforderten Dienstes (z.B. Warenkorb-Cookie) oder der Analyse des eigenen Webtraffics (Besucher auf der Webseite) dienen. So sehr dies nach Selbstbestimmung klingt, so zerstörerisch wirkt dies vor dem Hintergrund der Funktionsweise heutiger Netzwerkstrukturen. Kein Webseitenbetreiber (z.B. ein Blog) hat die personellen oder wirtschaftlichen Ressourcen, Reichenweiten oder die Auslieferungsqualität für Inhalte zu messen. Dafür gibt es einen ganzen Markt von Anbietern der digitalen Wirtschaft. Die neue Regulierung hätte zur Folge, dass diese Reichweitenmessungen mangels Kontaktes zum Nutzer unterbleiben müssten. Dadurch werden objektive, verlässliche Kennzahlen für die Werbewirtschaft und eine Finanzierung einer Vielzahl von Internetangeboten unmöglich. Ehemals kostenfreie Internetangebote würden kostenpflichtig oder vom Internet verschwinden. Der von der EU-Kommission erstrebte digitale Binnenmarkt und ein „free-flow-of-data“ sind damit kaum erreichbar.

4. Verschwinden jetzt wirklich die Cookie-Banner?

Fakt 1: In Deutschland waren Cookie-Banner bislang gar nicht nötig, weil es eine ausgewogene gesetzliche Regelung gab. Die Erhebung von Nutzungsdaten ist legal, wenn die Nutzer transparent darauf hingewiesen werden, Datenprofile zuverlässig pseudonymisiert werden und Nutzern ein Widerspruchsrecht eingeräumt wird (§ 15 Abs. 3 TMG). Dies ist echtes „privacy-by-design“. Für weitere Sicherheit und Transparenz sorgt darüber hinaus die von der EU-Kommission im Jahre 2009 selbst ins Leben gerufene Selbstregulierung der digitalen Wirtschaft, der derzeit ca. 95% aller Unternehmen in Deutschland angeschlossen sind. Über die Plattform www.meine-cookies.org können sich Nutzer über installierte Cookies informieren und ihre Präferenzen individuell definieren.

Fakt 2: Die EU-Kommission propagiert mit den neuen Regeln den Abschied des Einverständnisses über „Webseiten-Informationen“ (Cookie-Banner) hin zu zentralisierten Einwilligungen über Browsereinstellungen. Die neuen Regeln lassen allerdings nur noch Cookies und Webmessungen zu, die der Webseitenbetreiber selbst setzt. Künftig sollen alle Dienste, die der Webseitenbetreiber üblicherweise von Dritten ausführen lässt, gesperrt bleiben. Darüber wachen soll dann die Zugangssoftware, in den meisten Fällen also der Browser. Da das heutige Internet fast ausschließlich über Dienste von externen Anbietern funktioniert, werden die Browser künftig für jeden einzelnen Dienst eine neue Einwilligung einholen müssen. Dies führt zwangsläufig zu wesentlich mehr pop-up-windows als früher. Ein besserer Datenschutz oder aber eine bessere Nutzerfreundlichkeit sind damit nicht erreicht, im Gegenteil.

5. Sorgt nicht künftig der Internet-Browser für mehr Übersicht?

Die Idee der EU-Kommission ist so einfach wie fatal. Künftig soll nicht nur jede Software, welche die elektronische Kommunikation sondern auch jene, welche das Abrufen von Inhalten aus dem Internet ermöglicht, zum Wächter über Cookies & Co. werden. Im neuen Art. 10 Abs. 2 der ePV ist vorgesehen, dass diese Software bei der Installation verbindliche Setting-Einstellungen beim Nutzer abfragen und speichern muss. Diese one-size-fits-all-Lösung wird dazu führen, dass Nutzer bei der Ausschaltung von 3rd-party-Cookies künftig kein oder nur ein sehr eingeschränktes Netzangebot zur Verfügung haben werden. Webseiten mit eigenen 1st-party-Angeboten profitieren hingegen. Soll eine Ausübung von Nutzerrechten gegeben sein, muss der Browser künftig Anfragen von Webseiten verarbeiten, die ohne die Aktivierung externer Dienste nicht funktionieren. Er würde damit zum Super-Cookie.

6. Wird das elektronische Direktmarketing neu definiert?

Nein. Anders als in den Ankündigungen zum Entwurf Glauben gemacht, ändert sich nichts. In Art. 16 Abs. 2 ePV sind Regelungen zur Erlaubnis der Nutzung von elektronischer Post (E-Mail oder SMS) niedergelegt, soweit es sich um Bestandskunden handelt und die übrigen Bedingungen erfüllt sind. Diese Bestimmungen entsprechen nach wie vor den heute geltenden Regelungen des § 7 Abs. 3 UWG. Hier ändert sich überhaupt nichts. Auch künftig könnten Kunden per E-Mail kontaktiert werden, soweit sie bei

Erhebung der E-Mail-Adresse bei entgeltlichen Geschäften auf die Verwendung für die Bewerbung ähnlicher Waren oder Dienstleistungen hingewiesen wurden und vorab keinen Widerspruch erklärt haben.

7. Warum eine ePrivacy-Verordnung, wenn es bereits die EU-DSGVO gibt?

Diese Frage beschäftigt die gesamte digitale Wirtschaft. Vor dem Hintergrund der ab 25. Mai 2018 anwendbaren EU-Datenschutzgrundverordnung (EU-DSGVO) hatte die EU-Kommission ein REFIT-Programm aufgelegt und öffentliche Konsultationen zu der Frage durchgeführt, ob und wo Anpassungen oder Streichungen datenschutzrechtlicher Spezialvorschriften nötig sind. Ausweislich der Erwägungsgründe sowie der Definition des Anwendungsbereichs der EU-DSGVO soll diese den gesamten on- und offline-Bereich erfassen. Online-Identifizierung und Cookies sind ausdrücklich Gegenstand der Regelungen.

Der BVDW hatte daher gefordert, all diejenigen Sachverhalte aus der neuen ePV zu streichen, die nunmehr von der EU-DSGVO erfasst und geregelt sind. Dies betrifft insbesondere Datenverarbeitungen im digitalen (Online-)Umfeld. Trotzdem hat es die EU-Kommission nun für nötig befunden, neue Bestimmungen zu Datenverarbeitungen einzuführen. Diese sollen den Regelungen der EU-DSGVO wegen angeblicher Spezialität vorgehen. Es stellt sich nicht nur die Frage, ob es – neben der (berechtigten und notwendigen) Regulierung des Fernmeldegeheimnisses – überhaupt spezifischer Datenschutzregelungen im Bereich der elektronischen Kommunikation bedarf. Es ist jedenfalls absolut uneinsichtig, dass hier weitere, teilweise widersprechende Regelungen für den Bereich der Dienste der Informationsgesellschaft (Online-Services) geschaffen werden sollen. Im Verlaufe der EU-DSGVO wurde über Jahre darum gerungen, praktikable Regelungen für sämtliche Datenverarbeitungen zu formulieren. Mit ihrem extrem eingeschränkten Erlaubnisbereich und dem einseitigen Abstellen auf die Einwilligung als einzigem Mittel der Erlaubnis wird diese Arbeit beinahe vollständig konterkariert. Der Schutz des Endgerätes gegen illegitime Einwirkungen durch Dritte kann nicht als Grund herhalten, sämtliche, in der EU-DSGVO als legal definierte Datenverarbeitungsszenarien umzuschreiben.

Diese Art der nachträglichen Spezialregulierung hat noch einen weiteren, gravierenden nachteil für die digitale Wirtschaft. Es wird massiv Rechtsunsicherheit geschaffen. Denn solange nicht klar ist, wie die neuen ePV-Regeln aussehen werden, ist auch eine Vorbereitung auf die kommende EU-DSGVO kaum zukunftsfest vorstellbar. Unternehmen haben noch ca. 500 Tage bis zur Geltung der neuen Regeln. Nun kommen weitere hinzu. Derzeit für möglich erachtete Verarbeitungsmodelle können nach ePV-Grundsätzen plötzlich aber unmöglich werden oder einem strikten Einwilligungserfordernis unterfallen.

8. Warum eine Verordnung und was sind die Konsequenzen?

Im Gegensatz zur derzeitigen Rechtslage, sollen die neuen Regelungen im Wege einer EU-Verordnung eingeführt werden. Gemäß Art. 288 Abs. 2 des Vertrags über die Arbeitsweise der Europäischen Union (AEUV) besitzen Verordnungen allgemeine Geltung, sind in allen ihren Teilen verbindlich und unmittelbar in jedem Mitgliedstaat anwendbar. Im Unterschied zu EU-Richtlinien bedürfen Verordnungen also keiner nachträglichen Umsetzung in nationale Gesetze der Mitgliedsstaaten. Sie ist nach Inkrafttreten europaweit unmittelbar und einheitlich anwendbares Recht. Die ePV soll der weiteren Vollharmonisierung des Rechts in Europa dienen. Es gilt dasselbe die für die EU-DSGVO; auch die ePV soll einheitlich und nach dem Marktort-Prinzip gelten. Sie wird für alle Anbieter elektronischer Kommunikationsdienste gelten, die Ihre Dienste in der EU anbieten. Der Sitz des Unternehmens spielt dabei keine Rolle. Auch die Sanktionen für Verstöße sollen vereinheitlicht werden. Wie bei der EU-DSGVO werden die Bußgelder künftig signifikant steigen (10 Mio oder 2% des weltweiten Jahresunternehmensumsatzes).

9. Wann soll die neue Verordnung in Kraft treten?

Die EU-Kommission beabsichtigt derzeit, die ePV zusammen mit der EU-DSGVO (anwendbar ab 25.05.2018) einzuführen. Vor dem Hintergrund der dafür notwendigen Abstimmungen in Brüssel und eingedenk der langen Verhandlungen rund um die EU-DSGVO ein eher ambitioniertes Vorhaben. Derzeit ist nicht klar, ob dieser Zeitrahmen gehalten werden kann.

10. Wo bekomme ich weitere Informationen her?

Der BVDW hat für Fragen und Wissenswertes rund um die künftige EU-DSGVO [hier](#) und zur ePrivacy-Verordnung [hier](#) Informationsseiten angelegt. Diese werden stets aktualisiert. Für weitere Rückfragen steht Ihnen Michael Neuber (neuber@bvdw.org) zur Verfügung.

Stand 27.02.2017