Neue ePrivacy-Verordnung: Die wichtigsten Änderungen im Überblick

von Dr. Frank Eickmeier und Prof. Dr. Christoph Bauer

Hamburg, 16. Januar 2017 Bereits im Dezember 2016 ist der Entwurf einer neuen ePrivacy-Verordnung der Europäischen Kommission geleakt worden. Nun wurde die finale Version vom 10.01.2017 als offizieller Vorschlag der EU Kommission veröffentlicht. Die neue Verordnung soll die in die Jahre gekommene ePrivacy-Richtlinie 2002/58/EG ablösen und die Datenschutz-Grundverordnung (DSGVO) flankieren, die zum 25. Mai 2018 in Kraft tritt. Anders als die alte ePrivacy-*Richtlinie* ist die geplante ePrivacy-*Verordnung* unmittelbar in allen Mitgliedstaaten anwendbar und hat Vorrang gegenüber nationalen Gesetzen. Insoweit in der Vergangenheit diskutiert worden war, ob die ePrivacy-Richtlinie in Deutschland vollständig umgesetzt wurde, erübrigt sich diese Frage bei der nun vorgeschlagenen Verordnung, die keine Umsetzung durch den deutschen Gesetzgeber erfordert.

Der europäische Verband der Onlinewerbebranche *IAB Europe* hat den Entwurf in einer ersten Stellungnahme scharf kritisiert:

> *„Die Kommission hatte die perfekte Gelegenheit, ihr Interesse an besseren und klügeren Regeln durch die Abschaffung des veralteten und unnötigen Cookie Law unter Beweis zu stellen“,*

so Townsend Feehan, Geschäftsführer von IAB Europe.

> *„Endlich erkennt die Kommission die wichtige Rolle von Werbung für die Finanzierung kostenloser Onlineinhalte an und stellt gleichzeitig ein Gesetz vor, das diesem Geschäftsmodell klar Schaden zufügen wird – ohne den Nutzern echte Vorteile für den Schutz ihrer Privatsphäre und ihrer Daten zu bieten. Wer dachte, dass Cookie-Banner nerven, wird enttäuscht sein, dass es nicht besser wird.“*

Auch aus der deutschen Wirtschaft kam deutliche Kritik. Der Bundesverband Digitale Wirtschaft (BVDW) warnte vor „*einer fundamentalen Gefährdung der heutigen Informationsgesellschaft“.*

Im nachfolgenden soll daher aufgezeigt werden, worin die Bedrohung traditioneller Geschäftsmodelle der Onlinewirtschaft liegen könnte.

1) Aktuelle Situation

Die Verwendung von Third Party Cookies ist nach der derzeit in Deutschland geltenden Rechtslage auch ohne die Einwilligung des betroffenen Nutzers zulässig, solange dem Nutzer ein Recht zum Widerspruch („Opt-out“) eingeräumt wird. Dies, obwohl die geltende ePrivacy-Richtlinie etwas anderes vermuten lässt:

> *„Die Mitgliedstaaten stellen sicher, dass die Speicherung von Informationen oder der Zugriff auf Informationen, die bereits im Endgerät eines Teilnehmers oder Nutzers gespeichert sind, nur gestattet ist, wenn der betreffende Teilnehmer oder Nutzer auf der Grundlage von klaren und umfassenden Informationen, die er gemäß der Richtlinie 95/46/EG u.a. über die Zwecke der Verarbeitung erhält, seine Einwilligung gegeben hat.“*
> (Artikel 5 Abs. 3 ePrivacy-RL 2002/58/EG in der Fassung der RL 2009/136/EG)

Wie der Bundesgerichtshof nämlich 2008 im „Payback-Urteil“ entschied (BGHZ 177, 253 – *Payback*), stellt § 15 Abs. 3 Telemediengesetz (TMG) klar, dass es bei der Nutzung von Verbindungsdaten ausreicht, eine Opt-out Lösung für den Widerspruch des Nutzers anzubieten.

Der Gesetzeswortlaut des § 15 Abs. 3 TMG besagt:

> *„Der Diensteanbieter darf für Zwecke der Werbung, der Marktforschung oder zur bedarfsgerechten Gestaltung der Telemedien Nutzungsprofile bei Verwendung von Pseudonymen erstellen, sofern der Nutzer dem nicht widerspricht. Der Diensteanbieter hat den Nutzer auf sein Widerspruchsrecht im Rahmen der Unterrichtung nach § 13 Abs. 1 hinzuweisen. Diese Nutzungsprofile dürfen nicht mit Daten über den Träger des Pseudonyms zusammengeführt werden.“*

In einer Stellungnahme des deutschen Bundeswirtschaftsministeriums zur Umsetzung der ePrivacy-Richtlinie heißt es, dass die auch als „Cookie-Richtlinie“ bekannte Regelung durch die Vorschriften des Telemediengesetzes ausreichend umgesetzt sei. Solange in Third Party Cookies keine personenbezogenen Informationen enthalten sind, sind diese jedenfalls als

Pseudonyme im Sinne von § 15 Abs. 3 TMG zu qualifizieren mit der Folge, dass ihr Einsatz zulässig war, solange dem User auf der jeweiligen Website eine Opt-out Möglichkeit gegeben wird.

Weil andere Mitgliedstaaten, zum Beispiel das Vereinigte Königreich, bei der Umsetzung der ePrivacy-Richtlinie deutlich strenger vorgingen und vor allem aufgrund der strengeren Datenschutz-Anforderungen von Google gegenüber den Nutzern von Google AdSense, sind auch viele deutsche Websitebetreiber und Cookie-Verwender in der Praxis auf die Einholung der Nutzereinwilligung ausgewichen, indem sie ein „Cookie-Banner“ einblenden.

2) Inhalt der geplanten ePrivacy-Verordnung

Die ePrivacy-Verordnung soll ergänzend zu der ab Ende Mai 2018 geltenden Datenschutz-Grundverordnung speziell den Bereich der elektronischen Kommunikation und den Umgang mit personenbezogenen Daten regeln.

Die für Cookies interessanten Regelungen finden sich in Artikel 8 und Artikel 9. Besonders interessant sind die der Verordnung vorangestellten Erwägungsgründe 21 bis 24, die sich explizit mit der Verwendung von Tracking Cookies und Third Party Cookies auseinandersetzen. Die Erwägungsgründe einer Verordnung sind freilich nicht selbst Teil des Gesetzestexts. Sie spiegeln jedoch die Gedanken und Erwägungen der EU-Kommission wieder und helfen bei der Auslegung des Gesetzeswortlauts. Die genannten Erwägungsgründe lauten wie folgt:

> *“(21) Exceptions to the obligation to obtain consent to make use of the processing and storage capabilities of terminal equipment or to access information stored in terminal equipment should be limited to situations that involve no, or only very limited, intrusion of privacy. For instance, consent should not be requested for authorizing the technical storage or access which is strictly necessary and proportionate for the legitimate purpose of enabling the use of a specific service explicitly requested by the end-user. This may include the storing of cookies for the duration of a single established session on a website to keep track of the end-user’s input when filling in online forms over several pages. Cookies can also be a legitimate and useful tool, for example, in measuring web traffic to a website. Information society providers that engage in configuration checking to provide the service in compliance with the end-user's settings and the mere logging of the fact that the end-user’s device is unable to receive content requested by the end-*

user should not constitute access to such a device or use of the device processing capabilities.

(22) The methods used for providing information and obtaining end-user's consent should be as user-friendly as possible. Given the ubiquitous use of tracking cookies and other tracking techniques, end-users are increasingly requested to provide consent to store such tracking cookies in their terminal equipment. As a result, end-users are overloaded with requests to provide consent. The use of technical means to provide consent, for example, through transparent and user-friendly settings, may address this problem. Therefore, this Regulation should provide for the possibility to express consent by using the appropriate settings of a browser or other application. The choices made by end-users when establishing its general privacy settings of a browser or other application should be binding on, and enforceable against, any third parties. Web browsers are a type of software application that permits the retrieval and presentation of information on the internet. Other types of applications, such as the ones that permit calling and messaging or provide route guidance, have also the same capabilities. Web browsers mediate much of what occurs between the end-user and the website. From this perspective, they are in a privileged position to play an active role to help the end-user to control the flow of information to and from the terminal equipment. More particularly web browsers may be used as gatekeepers, thus helping end-users to prevent information from their terminal equipment (for example smart phone, tablet or computer) from being accessed or stored.

(23) The principles of data protection by design and by default were codified under Article 25 of Regulation (EU) 2016/679. Currently, the default settings for cookies are set in most current browsers to 'accept all cookies'. Therefore providers of software enabling the retrieval and presentation of information on the internet should have an obligation to configure the software so that it offers the option to prevent third parties from storing information on the terminal equipment; this is often presented as 'reject third party cookies'. End-users should be offered a set of privacy setting options, ranging from higher (for example, 'never accept cookies') to lower (for example, 'always accept cookies') and intermediate (for example, 'reject third party cookies' or 'only accept first party cookies'). Such privacy settings should be presented in a an easily visible and intelligible manner.

(24) For web browsers to be able to obtain end-users' consent as defined under Regulation (EU) 2016/679, for example, to the storage of third party tracking cookies, they should, among others, require a clear affirmative action from the end-user of terminal equipment to signify his or her freely given, specific informed, and unambiguous agreement to the storage and access of such cookies in and from the terminal equipment. Such action may be considered to be affirmative, for example, if end-users are required to actively select 'accept third party cookies' to confirm their agreement and are given the necessary information to make the choice. To this end, it is necessary to require providers of software enabling access to internet that, at the moment of installation, end-users are informed about the possibility to choose the privacy settings among the various options and ask them to make a choice. Information provided should not dissuade end-users from selecting higher privacy settings and should include relevant information about the risks associated to allowing third party cookies to be stored in the computer, including the compilation of long-term records of individuals' browsing histories and the use of such records to send targeted advertising. Web browsers are encouraged to provide easy ways for end-users to change the privacy settings at any time during use and to allow the user to make exceptions for or to whitelist certain websites or to specify for which websites (third) party cookies are always or never allowed."

In den Erwägungsgründen 21 bis 24 schätzt die EU-Kommission die derzeitige Lage des Datenschutzes im Internet ein. Es würden derzeit viel zu viele Anfragen zur Einwilligung an den Nutzer gestellt. Diese vielen Einwilligungsanfragen würden den Internetnutzer überfordern (Erwägungsgrund 22). Daher sei es erforderlich, *einerseits* Datenverarbeitungen mit niedriger Relevanz von dem Erfordernis einer Einwilligung auszuklammern. So soll es zum Beispiel keiner Einwilligung bedürfen, wenn ein Session Cookie gesetzt wird, das das Ausfüllen eines mehrseitigen Formulars ermöglicht. Dieses soll ohne gesonderte Einwilligung gesetzt werden dürfen sein (Erwägungsgrund 21). Auch zu „technisch erforderlichen" Tracking Cookies, etwa zur Messung des Traffics einer Website, müsse der User nicht gesondert befragt werden.

Nach der vorgeschlagenen Verordnung der Kommission soll dagegen bei allen übrigen Third Party Cookies und anderen Tracking Cookies die Einwilligung des betroffenen Users erforderlich werden. Nach unserer ersten Einschätzung hätte diese Regelung erhebliche Auswirkungen auf die gesamte Onlinebranche.

Zur Form der Einwilligung priorisiert die EU-Kommission in den Erwägungsgründen 21 - 25 das Konzept, dass die Einwilligung künftig über die Datenschutzeinstellungen im Browser des betroffenen Users erfolgen könne. Dies sei dann möglich, wenn dem Nutzer beim Festlegen der entsprechenden Einstellungen klar ist, dass er dadurch etwa in das Setzen von Tracking Cookies einwilligt. Unter Bezug auf die in der Verordnung 2016/679/EU geplanten Vorschriften zu einem Privacy by Design ruft die EU Kommission die Browser-Hersteller zu mehr Transparenz und Klarheit bei den Einstellungen zum Datenschutz auf. Auf einem einfachen und verständlichen Weg sollten die Hersteller dem Nutzer in den Browser-Einstellungen die Auswahl eröffnen, zwischen beispielsweise „Keine Cookies akzeptieren", „Third Party Cookies ablehnen" und „Nur First Party Cookies akzeptieren" zu entscheiden. Bereits bei der Installation des Browsers soll der Nutzer über die möglichen Einstellungen zum Datenschutz informiert werden und zur Auswahl aufgefordert werden.

Eine erst einmal erteilte Einwilligung soll nach den Erwägungsgründen 34 und 35 widerruflich sein, und zwar jederzeit und möglichst einfach.

Abgesehen von dem Einsatz von Cookies hat Erwägungsgrund 20 noch eine besondere Relevanz. Danach wird für die Nutzung vieler Techniken, die Informationen des Verbraucherendgeräts verarbeiten, eine Einwilligung des Nutzers erforderlich.

> *(20) […] "Given that such equipment contains or processes information that may reveal* ***details of an individual's emotional, political, social complexities, including the content of communications, pictures, the location of individuals by accessing the device's GPS capabilities, contact lists, and other information*** *already stored in the device, the information related to such equipment requires enhanced privacy protection. Furthermore, the so-called* ***spyware****,* ***web bugs****,* ***hidden identifiers****,* ***tracking cookies*** *and other similar unwanted tracking tools can enter end-user's terminal equipment without their knowledge in order to gain access to information, to store hidden information and to trace the activities. Information related to the end-user's device may also be collected remotely for the purpose of identification and tracking, using techniques such as the so-called '****device fingerprinting'****, often without the knowledge of the end-user, and may seriously intrude upon the privacy of these end-users.* ***Techniques that surreptitiously monitor the actions of end-users****, for example by tracking their activities online or the location of their terminal equipment, or subvert the operation of the end-users' terminal equipment pose a serious threat to the privacy of end-users.*

*Therefore, any such interference with the end-user's terminal equipment should be allowed **only with the end-user's consent** and for specific and transparent purposes."*

Demgegenüber meint die EU Kommission laut Erwägungsgrund 25, dass Verbindungsdaten, beispielsweise die MAC-Adresse oder die IMEI-Nummer von Endgeräten, auch ohne Einwilligung des Nutzers genutzt werden dürfen, sofern kein hohes Risiko für die Datensicherheit der Nutzer besteht. Insoweit solche Verbindungsdaten erhoben werden, müssen den Nutzern bereits vor der Erhebung deutliche Hinweise aufgezeigt werden, damit sich der Nutzer wie bei videoüberwachten Bereichen der Erfassung entziehen kann.

In Erwägungsgrund 32 der Verordnung wird der Begriff des „direct marketing" als jede Art von Werbung beschrieben, die über elektronische Kommunikation dem End-User zugesandt wird. Das beinhaltet auch Nachrichten von politischen Parteien und Non-Profit-Organisationen.
Die EU Kommission sieht in Erwägungsgrund 17 das Erfordernis der Nutzung von Metadaten („electronic communications metadata") durch Anbieter von Kommunikationsdienstleistungen beispielsweise zur Verbesserung von öffentlichem Transport und Infrastruktur. Zu diesen Zwecken sei eine Anonymisierung der Daten nicht erforderlich, vielmehr könne die Nutzung der Metadaten mit einem „identifier" (Pseudonymisierung) zulässig sein. Wenn hohe Risiken bei der Verarbeitung dieser Metadaten bestehen, muss im Wege der Artikel 35 und 36 der DSGVO 2016/679/EU eine Datenschutz-Folgenabschätzung und die vorherige Konsultation der Aufsichtsbehörde vorgenommen werden.

3) Die Regelungen im Einzelnen

Gesetzestechnisch geht die Kommission folgendermaßen vor: Nach Art. 8 Abs. 1 des Verordnungsvorschlags ist die Nutzung von „Rechen- und Speicherleistung" des „Nutzerendgerätes" grundsätzlich verboten, es sei denn, der Nutzer erklärt seine Einwilligung oder die Nutzung von Rechten- und Speicherleistung ist erforderlich für die Darstellung der Website und für Messungen des Web Traffics.

"Article 8 Protection of information stored in and related to end-users' terminal equipment

1. *The use of processing and storage capabilities of terminal equipment and the collection of information from end-users' terminal equipment, including about its software and hardware, other than by the end-user concerned shall be prohibited, except on the following grounds:*

(a) it is necessary for the sole purpose of carrying out the transmission of an electronic communication over an electronic communications network; or

(b) the end-user has given his or her consent; or

(c) it is necessary for providing an information society service requested by the end-user; or

(d) if it is necessary for web audience measuring, provided that such measurement is carried out by the provider of the information society service requested by the end-user."

Art. 8 Abs. 1 lit. a kommt vor allem den Websitebetreibern zugute, die nun zum Einsatz von zwingend erforderlichen Cookies, ohne die ein Abruf der Websiteinhalte nicht möglich wäre, keine gesonderte Einwilligung des Nutzers brauchen. Doch auch weitere Cookies, wie beispielsweise Tracking und Session Cookies, sind ohne Einwilligung zulässig, wenn sie für die Darstellung von Diensten der Informationsgesellschaft *erforderlich* sind, die der Nutzer abruft.
Dabei wird der Begriff „Dienste der Informationsgesellschaft" wie einst in Artikel 1 Nummer 2 der Richtlinie 98/34/EG in der Fassung der Richtlinie 98/48/EG definiert weit verstanden.

"2. 'Dienst': eine Dienstleistung der Informationsgesellschaft, d. h. jede in der Regel gegen Entgelt elektronisch im Fernabsatz und auf individuellen Abruf eines Empfängers erbrachte Dienstleistung.

Im Sinne dieser Definition bezeichnet der Ausdruck

- 'im Fernabsatz erbrachte Dienstleistung' eine Dienstleistung, die ohne gleichzeitige physische Anwesenheit der Vertragsparteien erbracht wird;

- 'elektronisch erbrachte Dienstleistung' eine Dienstleistung, die mittels Geräten für die elektronische Verarbeitung (einschließlich digitaler Kompression) und Speicherung von Daten am Ausgangspunkt gesendet und am Endpunkt empfangen wird und die vollständig über Draht, über Funk, auf optischem oder anderem elektromagnetischem Wege gesendet, weitergeleitet und empfangen wird;

- 'auf individuellen Abruf eines Empfängers erbrachte Dienstleistung' eine Dienstleistung, die durch die Übertragung von Daten auf individuelle Anforderung erbracht wird."

In den Erwägungsgründen beispielhaft genannt sind Tracking Cookies für Webformulare und Session Cookies für Web-Traffic Messungen.

Ob unter die Ausnahmen nach Art. 8 Abs. 1 lit. c auch Analyse-Tools wie Google Analytics fallen, hängt von der Auslegung der Einschränkung „carried out by the provider" ab. Das ist hier problematisch, da Google Analytics nicht identisch ist mit dem Websitebetreiber, der den gewünschten Dienst der Informationsgesellschaft anbietet. Jedenfalls ist Google Analytics kein Fall von Art. 8 Abs. 1 lit. a, da der Service nicht zur Übermittlung der Inhalte erforderlich ist.

Art. 8 Abs. 2 der Verordnung befasst sich daneben mit den Daten, welche das Endgerät des Nutzers bei der Kommunikation im Netz von sich aus übermittelt. Dabei ist insbesondere an die IP-Adresse und an den User agent zu denken. Das Speichern dieser Daten soll grundsätzlich verboten sein, es sei denn, dies ist „zur Herstellung einer Verbindung erforderlich".

Ausnahmsweise dürfen diese Daten gesammelt werden, wenn ein „eindeutiger und deutlich sichtbarer" Hinweis angezeigt wird, der angibt, wie, von wem und aus welchem Grund die Daten gespeichert werden, sowie die Schritte erläutert, die der Nutzer zur „Minimierung" dieser Datenverarbeitungen unternehmen kann. Hierzu dürfte auch das Tracking von Verbindungsdaten gehören, etwa durch die MAC-Adresse oder die IMEI-Nummer. Diesbezüglich verhalten sich die Erwägungsgründe 20 und 25 zueinander auf den ersten Blick widersprüchlich. Es ist vermutlich wertend zu beachten, in welcher Intensität das Tracking des Nutzers in dessen Privatsphäre eindringt.

> *"Article 8 Protection of information related to end-users' terminal equipment*
>
> *[…]*
>
> *2. The collection of data emitted by terminal equipment to enable it to connect to another device and or network equipment by natural or legal persons other than end-users concerned shall be prohibited, except:*
>
> *(a) if it is done exclusively in order and for the time necessary to establish a possible connection;*
>
> *(b) if a clear and prominent notice is displayed to the public informing of, at least, the modalities of the collection its purpose, the person responsible for it and of any measure the end-user of the terminal equipment can take to minimise the collection, and,*

When such data is used for direct marketing and profiling, the end-user shall have the right to object as provided for in Article 21 of the GDPR […].”

Art. 9 des Verordnungsvorschlags regelt die Form der Einwilligung des Nutzers, die sich vorrangig nach Art. 7 der kommenden Datenschutz-Grundverordnung bestimmt. Danach ist die Einwilligung grundsätzlich formlos möglich, muss aber nachweisbar dokumentiert werden und kann jederzeit widerrufen werden.

Nach Artikel 9 Abs. 2 des Verordnungsvorschlags kann die Einwilligung auch durch eine Einstellung des Nutzers im Browser erfolgen, jedoch nur, „soweit dies technisch möglich und praktikabel ist“. Sollte der Nutzer nach dieser Vorschrift in seinem Browser die Datenschutzeinstellungen so konfigurieren, dass Third Party Cookies zugelassen werden, so willigt er beim Besuch einer Website in die Setzung dieser Cookies ein:

“Article 9 Consent

1. *The definition of and conditions for consent provided for under Articles 4(11) and 7 of Regulation (EU) 2016/679/EU shall apply.*
2. *Without prejudice to paragraph 1, where technically possible and feasible, for the purposes of point (b) of Article 8(1), consent may be expressed by using the appropriate technical settings of a software application enabling access to the internet.*
3. *End-users who have consented to the processing of electronic communications data as set out in point (c) of Article 6(2) and points (a) and (b) of Article 6(3) shall be given the possibility to withdraw their consent at any time as set forth under Article 7(3) of Regulation (EU) 2016/679 and be reminded of this possibility at periodic intervals of 6 months, as long as the processing continues.”*

Beachtet man die oben erörterten Erwägungsgründe, so müssen die Begriffe „technically possible and effective“ dahingehend gedeutet werden, dass der verwendete Browser dem Nutzer hinreichend transparent und einfach die Konfiguration der Datenschutzeinstellung ermöglicht, so dass es dem tatsächlichen Willen des Nutzers entspricht, wenn er der Setzung von einwilligungsbedürftigen Third Party Cookies oder Tracking Cookies zustimmt. Genaueres lässt sich an dieser Stelle nicht sagen, da unklar ist, ob und wie sich Art. 25 Abs. 1 der kommenden Datenschutzgrundverordnung 2016/670/EU (Privacy by Design) mit der Pflicht für Hersteller zur datenfreundlichen Gestaltung von Produkten überhaupt durchsetzt.

Diesbezüglich hat die EU Kommission in Artikel 10 der Verordnung festgelegt, dass jede Software, die eine elektronische Kommunikation eröffnet, eine Option anbieten *soll*, um die Speicherung von Informationen auf dem Endgerät oder die Nutzung der Prozessorleistung des Endgeräts durch Dritte zu verhindern. Nach Absatz 2 und Absatz 3 soll der Hersteller bereits bei Installation oder aber durch ein Update den Nutzer über die entsprechenden Optionen zum Datenschutz aufklären.

Nach Artikel 9 Abs. 3 der Verordnung muss eine erteilte Einwilligung durch den Nutzer widerruflich sein, und zwar zu jeder Zeit. Der Nutzer muss im Intervall von sechs Monaten an die Option des Widerrufs erinnert werden. Dies jedoch nur, wenn die Daten weiterhin verarbeitet werden. Wird folglich nach einer erfolgten Einwilligung ein Cookie platziert, so muss der Nutzer nach Ablauf von sechs Monaten die Möglichkeit haben, die Einwilligung in das Cookie zu widerrufen. In der Folge muss das Cookie gelöscht oder inaktiviert werden.

Sollte der Verordnungsvorschlag daher so umgesetzt werden, wird die Rechtslage für Cookies in der EU deutlich erschwert. Es entspricht wohl nicht dem Willen der EU-Kommission, der von Cookies abhängigen Onlinewerbebranche das Wasser abzugraben, da sie die Entscheidung über den Umgang mit Userdaten in die Hände der User selbst geben möchte.

Zur Stärkung der Rechtsposition des Nutzers soll sich der Verordnungsvorschlag jedoch auch gegen die heimliche Überwachung der Nutzer („surreptitious monitoring“) richten. Immerhin soll die Nutzung von Rechen- und Speicherleistung des Endnutzergerätes stärker reglementiert werden, was voraussichtlich weitreichende Folgen haben wird.

Vielmehr soll die geplante Verordnung den Ansatz des „Privacy by Design“ verfolgen. Softwarehersteller sollen ihre Produkte so anpassen, dass die Nutzer mehr Klarheit über die Verwendung ihrer Daten erhalten und diese besser steuern können. Wie die großen Browserhersteller darauf reagieren werden, lässt sich bislang nicht abschätzen.

Solange nicht geklärt ist, wie nach den Vorstellungen der EU-Kommission „technisch mögliche und effektive“ Browsereinstellungen auszusehen haben, wird die geplante ePrivacy-Verordnung dazu führen, dass sowohl das Setzen von Cookies als auch die Verarbeitung von IP-Adressen und User Agents europaweit von der vorherigen Einwilligung der betroffenen Nutzer abhängig ist. Die Lösung des Problems durch einen Opt-out, einen Hinweis in der Datenschutzerklärung oder ein einfaches Hinweisbanner wäre damit passé.

Schließlich wird die ePrivacy-Verordnung aufgrund ihrer Kopplung mit der Datenschutz-Grundverordnung viel weitreichendere Wirkung auch für Unternehmen außerhalb der Europäischen Union entfalten, da sie die Rechte von den Websitebesuchern aus der EU gleichsam beachten müssen.

4) Ausblick

Anders als bei der Datenschutz-Grundverordnung mit ihrer langen Übergangsfrist soll die ePrivacy-Verordnung bereits sechs Monate nach ihrer Veröffentlichung in Kraft treten (Art. 31 Abs. 2). Daher gilt es, das weitere Gesetzgebungsverfahren genau im Auge zu behalten.

Im Falle eines Verstoßes gegen die dargestellten Vorschriften kann die zuständige Aufsichtsbehörde drakonische Strafen von bis zu 20 Millionen Euro oder 4 % der Unternehmenseinkünfte verhängen. Betroffene Unternehmen sollten sich daher unbedingt auf die Umsetzung der neuen Regelungen vorbereiten.

5) Zusammenfassung

Nach dem aktuellen Vorschlag der ePrivacy-Verordnung darf allein der Besuch einer Website durch den Endverbraucher nicht mehr als Einwilligung in eine gesonderte Datenverarbeitung verstanden werden. Die derzeit gebräuchlichen Banner mit dem Inhalt „Mit dem Besuch dieser Website akzeptieren sie (konkludent) die Verwendung von Cookies“ oder dem Hinweis „Wir benutzen Cookies“ und einem OK-Button werden unzulässig sein, da dem Nutzer keine echte Wahl bezüglich der Abgabe einer Einwilligung verbleibt. Es genügt auch nicht, darauf hinzuweisen, dass der betroffene Nutzer in seinem Browser bestimmte Datenschutzeinstellungen vornehmen kann.

Vielmehr muss dem Nutzer beim ersten Aufruf der Website und noch vor der ersten Platzierung eines einwilligungsbedürftigen Cookies ein Hinweis auf die Verwendung von Cookies dargestellt werden, bei dem der Nutzer die Wahl hat, dem zuzustimmen oder es abzulehnen. Die Darstellung kann durch ein Banner oder ein Hinweisfenster erfolgen, das nicht übersehen werden kann. Die Zustimmung muss per Opt-In abgefragt werden. Opt-In bedeutet dabei, dass im Fall einer Checkbox diese nicht bereits mit einem Häkchen versehen sein darf. Der Nutzer muss zur Zustimmung unzweideutig selbst auf „Zustimmen“ klicken, als würde er einen Internetkauf abschließen. Tut er dies nicht und lässt das Banner/den Hinweis unbeachtet, dürfen keine einwilligungsbedürftigen Cookies platziert werden.

Sollte der Nutzer ablehnen, darf die Website für ihn jedoch nicht gesperrt sein. In dem Erwägungsgrund 42 der Datenschutz-Grundverordnung heißt es nämlich, dass die Gestaltung so erfolgen muss, dass der Nutzer „[…] *in der Lage ist, die Einwilligung zu verweigern oder zurückzuziehen, ohne Nachteile zu erleiden.*“ Hier spricht einiges dafür, einen Nachteil anzunehmen, wenn einem Nutzer, der nicht Einwilligt, der Inhalt der Website vorenthalten würde. Dies lässt sich jedoch nicht mit letztendlicher Sicherheit sagen, da bisher unklar ist, wie ein „Nachteil“ definiert werden wird.

Außerdem muss der Websitebetreiber auch den Nutzern, die ihre Einwilligung bereits erklärt haben, jederzeit ein Opt-out, also eine Option zum späteren Widerruf der Einwilligung, anbieten.

Nicht zuletzt sollten Websitebetreiber zukünftig auch die Browsereinstellung „Do Not Track“ von jedem Nutzer abfragen, da dies bereits das Nicht-Einwilligen des Nutzers festlegt.

Für die Websitebetreiber wird das stringente Einhalten der neuen Regeln der ePrivacy-Verordnung einen nicht unerheblichen Aufwand zur Anpassung der Websites und Kosten bedeuten. Insbesondere beim Website-Monitoring müssen die Unternehmen in Zukunft sehr genau abwägen, welche Datenerhebungen einer Nutzereinwilligung bedürfen. Bis zum Inkrafttreten der Norm ist noch mit intensiven Verhandlungen und viel Lobbyarbeit zu rechnen.