10. Mai 2019
RAH

Positionspapier ePrivacy Verordnung

Stand Vorschlag der Rumänischen Ratspräsidentschaft in der Fassung der Ratsdokumente 6771/19 und 7009/19

der ZVEI-Fachverband Consumer Electronics vertritt die Interessen der Hersteller von Unterhaltungselektronik, die mit ihren Produkten den digitalen Alltag der Verbraucher bereichern und prägen. Zunehmend sind die Geräte der Unterhaltungselektronik mit dem Internet vernetzt: So stellen etwa Smart-TV neben Rundfunk auch Web-Inhalte und „Apps“ dar und ermöglichen eine personalisierte und diversifizierte Mediennutzung.

Aufgrund der Vernetzung der Endgeräte findet notwendigerweise ein bi-direktionaler Datenaustausch statt, sei es zum Betrieb des Gerätes oder zur Darstellung von Apps oder HbbTV-Anwendungen oder auch im Rahmen von Smart Home Anwendungen zu anderen Endgeräten. Der aktuelle Vorschlag der ePrivacy Verordnung (ePrivacy VO) hat daher auch Auswirkung auf die Ausgestaltung und Funktionsweise von Smart-TVs.

Die Reglungen der ePrivacy VO sind für vernetzte Endgeräte der Unterhaltungselektronik vielfach unpassend. Der unscharf abgegrenzte Adressatenkreis der Verordnung führt zu einer Gleichbehandlung völlig ungleicher Akteure mit unterschiedlich starken Einfluss auf die Sicherheit der Kommunikation und den Datenschutz. Um Überregulierung in einem Markt mit anhaltend hoher Innovationsdynamik zu vermeiden, ist die Regulierungsintensität dem jeweiligen Gefährdungspotential anzupassen. Wir sprechen uns daher dafür aus, den Entwurf in den weiteren Verhandlungen weiter zu überarbeiten, um verständliche Regelungen mit angemessenen Regulierungsumfang zu erreichen.

ZVEI - Zentralverband Elektrotechnik- und Elektronikindustrie e. V. • Lyoner Straße 9 • 60528 Frankfurt am Main
Fachverband Consumer Electronics
Telefon: +49 69 6302-421 • Fax: +49 69 6314-036 • E-Mail: heyeckhaus@zvei.org

Präsident: Michael Ziesemer • Vorsitzender der Geschäftsführung: Dr. Klaus Mittelbach

Dabei gilt es die folgenden Aspekte zu berücksichtigen.

1. **Klare Abgrenzung des Adressatenkreises**

In der aktuellen Version der ePrivacy VO werden unterschiedliche Datenverarbeiter und ganz unterschiedliche Datenverarbeitungsarten aufgrund fehlender Differenzierung gleichbehandelt. Eine zu weite Fassung des Anwendungsbereichs unterschlägt notwendige Differenzierungen zwischen einzelnen Normadressaten. Gegenüber der bestehenden Rechtslage, die über Regelungen in TMG, TKG oder BDSG zwischen jeweils unterschiedlichen Normadressaten unterscheidet, wird durch die Ausweitung des Anwendungsbereichs in der ePrivacy VO die bestehende rechtliche Klarheit durch Regeln ersetzt, die mehr oder weniger jeden erfassen.

Dies wird insbesondere dann bei den Regelungen des Verordnungsentwurfes deutlich, wenn diese offensichtlich nur einen Adressatenkreis ansprechen wollen, dies aber nicht deutlich benennen. So ergeben die Artikel 5-7 ePrivacy VO nur Sinn, wenn man den Adressatenkreis auf *Electronic Communication Service Provider* beschränkt. So erfasst Art. 5 ePrivacy VO (im Unterschied zu Art. 6 ePrivacy VO) nach dem Wortlaut sämtliche Akteure, sofern sie Kommunikationsdaten im Sinne der Vorschrift verarbeiten.

Diese Unklarheit hinsichtlich des Regelungsgehalts der einzelnen Vorschriften führt zu einer erheblichen Rechtsunsicherheit. Es ist daher notwendig, in jeder Regelung klarzustellen, wer erfasst werden soll, um den persönlichen Anwendungsbereich auf die jeweilige Nutzergruppe zu beschränken. Denn für Smart-TV Hersteller, die ohnehin keinen den Betreibern elektronischen Kommunikationsdienste vergleichbaren Einfluss auf die Vertraulichkeit der Kommunikation haben, ist schlicht unklar, wie die jeweiligen Regeln umgesetzt werden sollen.

Für sämtliche Regelungen der Verordnung ist es erforderlich, den Adressatenkreis klar zu bezeichnen. Die Regelungen, die nur *Electronic Communications Services Provider* oder nur *Internet Service Provider* adressieren sollten diese auch ausdrücklich benennen.

2. **Verdeutlichung des sachlichen Anwendungsbereichs im Bereich M2M/ IoT**

Die ePrivacy VO verweist für die „electronic communication services“ auf die Begriffsdefinition in Art. 2 Nr. 4 des Electronic Communication Code. Danach werden ausdrücklich auch Übertragungsdienste „transmission services“, die für die Maschine-Maschine-Kommunikation genutzt werden erfasst, wohingegen Dienste die auf der „application layer“ betrieben werden, nicht erfasst werden (Erwägungsgrund 12 ePrivacy VO). Jedoch werden in Erwägungsgrund 12 Übertragungsdienste („*transmission services*“) von Anwendungsdiensten („*services*

provided at the application layer“) nicht ausreichend voneinander abgegrenzt. Schon bei einfachen Anwendungen kommt es zu einem komplexen Wechsel- und Zusammenspiel von Diensten auf der Anwendungs- und Transportschicht. Ohne eine Klärung, wann der Übertragungsvorgang abgeschlossen ist und der Anwendungsvorgang beginnt, ist eine rechtliche Einordnung, ob der Anwendungsbereich eröffnet ist, nicht möglich.

Um klare Regelungen zu erreichen, ist es erforderlich, „transmission services“ von „application services“ deutlich voneinander abzugrenzen.

3. Klarere Fassung der Erlaubnisgründe in Art. 8 ePrivacy VO (Endgeräteschutz)

a) Erlaubnisgrund für Softwareupdates, Art. 8 Abs. 1 lit. e) ePrivacy VO

Es ist zu begrüßen, dass in Art. 8 Abs.1 lit. e) ePrivacy VO eine Ausnahme vom Verarbeitungsverbot in Fall von Softwareupdates geschaffen wird. Denn üblicherweise wird ein Softwareupdate erst vollständig auf dem Gerät gespeichert, bevor es installiert werden kann. Grund hierfür ist, dass durch den vorherigen Download sichergestellt wird, dass das Update anschließend vollständig und störungsfrei installiert werden kann. Würde bei einer direkten Installation, ohne vorherigen Download, die Internetverbindung während des Prozesses abreißen, wäre die Installation fehlerhaft und müsste wiederholt werden. Für den Nutzer ist somit durch die vorherige Speicherung, eine möglichst fehlerfreie und bequeme Installation möglich.

Jedoch wird der Anwendungsbereich des Erlaubnisgrunds unter lit. e) unnötig verengt, in dem sie sich nur auf Updates, die aus Sicherheitsgründen erforderlich sind (“*necessary for security reasons*”) beschränkt. In Erwägungsgrund 21 a wird dazu klargestellt, dass es sich um ein ausschließliches Sicherheits-Softwareupdate handeln muss (“*that do not exclusively have a security purpose, for example those intended to add new features to an application or improve its performance, should not fall under this exeption“).* Dieser Satz ist zu streichen. Er führt ansonsten dazu, dass der Erlaubnisgrund nicht angewandt werden kann. In der Praxis gibt es bei vernetzten Endgeräten keine Updates die ausschließlich Sicherheitszwecken dienen. In der Regel handelt es sich bei Updates immer um “gemischte” Updates, etwa eine Kombination aus Bug fixes zur Verbesserung der Funktionalität und zum Schließen von Sicherheitslücken. Zudem ist auch unklar, wann ein Sicherheitsupdate nur als „Update zu Sicherheitszwecken“ eingeordnet werden kann. Denn selbst bei einem Update, dessen primärer Zweck die Behebung einer Sicherheitslücke ist (z.B. ein Update zur Verhinderung der Überhitzung des Geräts), kann dies gleichzeitig dazu führen, dass sich auch die Leistung des Gerätes insgesamt verbessert. Nach der in Erwägungsgrund 21 a getroffenen Einschränkung wäre es dann, bereits vom Anwendungsbereich des Erlaubnisgrundes in Art. 8 Abs. 1 lit e ePrivacy VO ausgeschlossen.

In Art 8 Abs.1 lit e) ePrivacy VO ist der Zusatz "are necessary for security reasons and" zu streichen. Erwägungsgrund 21 a ist dementsprechend anzupassen.

b) Erlaubnisgrund im Zusammenhang mit der Vermeidung von Sicherheitsrisiken Art. 8 Abs. 1 lit. da) ePrivacy VO

Ferner gilt es auch in Art. 8 Abs.1 lit. da) ePrivacy VO im Zusammenhang mit der Vermeidung von Sicherheitsrisiken klarzustellen, dass diese sich nicht nur auf Risiken bei "*information society services*" beschränkt werden. Sofern es Schutzzweck des Erlaubnisgrundes ist, akute Sicherheitsrisiken schnell einzudämmen, macht es für den Nutzer keinen Unterschied, ob sich ein Sicherheitsrisiko über einen Informationsdienst oder über das Gerät selbst realisiert. Es muss daher die Möglichkeit geben, schnell und ohne vorherige Einwilligung auf ein bestehendes Sicherheitsrisiko reagieren zu können, auch wenn sich ein Sicherheitsrisiko auf dem vernetzten Endgerät selbst manifestiert. Dies kann etwa der Fall sein, wenn die installierte Software, das Betriebssystem oder sogar die Hardware selbst kompromittiert ist.

In Art. 8 Abs. 1 lit. da) ePrivacy VO ist "of information society services" zu streichen.

c) Erlaubnisgrund bei Erbringung eines Dienstes, Art. 8 Abs. 1 lit. c ePrivacy VO

Art. 8 Abs. 1 lit c ePrivacy VO bildet einen Erlaubnisgrund zum Datenverarbeitungsverbot sofern die Datenverarbeitung zur Erbringung eines Dienstes erforderlich ist. Diese Ausnahme sollte so verstanden werden, dass dies auch Softwareupdates umfasst, die notwendig werden, um etwa die Funktionalität eines Dienstes zu erhalten oder die Leistung zu verbessen. Dies ist in den korrespondierenden Erwägungsgründen in 19b und 21 a entsprechend anzupassen.

Sofern weder der Erlaubnisgrund unter lit. c) noch lit. da) angepasst würde, wären Softwareupdates zukünftig nur mit vorheriger Einwilligung des Nutzers möglich. Es ist unklar, warum Softwareupdates, die die Funktionalität der Geräte erhalten, jeweils von der Einwilligung des Nutzers abhängig gemacht werden sollten. Es findet eine Verarbeitung rein technischer Daten statt, i.d.R. erfolgt lediglich eine Versionsabfrage des Gerätetyps. Sofern Softwareupdates Auswirkungen auf persönliche Daten des Nutzers haben, ist ohnehin eine Einwilligung nach den Vorschriften der EU DSGVO erforderlich. In den übrigen Fällen kann auf das Einwilligungserfordernis verzichtet werden.

Dies gilt umso mehr als bei vernetzten Endgeräten wie Smart-TVs, keine Übung der Nutzer, wie bei Smartphone, Tablet oder PC, besteht, direkt mit dem Gerät zu interagieren. Der Smart-TV ist nach wie vor ein Mittel zur passiven Mediennutzung. Eine Überblendung des Bildes mit Dialogfenstern und Aufforderungen eine Einwilligung abzugeben, fällt hier noch störender aus, als bei Endgeräten die auf

eine aktive Teilnahme des Nutzers ausgerichtet sind. Das Einwilligungserfordernis sollte daher nicht gezwungenermaßen zum „Regel-Ausnahmefall“ werden, weil die anderen Erlaubnisgründe in Art. 8 Abs. 1 ePrivacy VO entweder zu praxisfern sind oder aufgrund ihres zu engen Tatbestands nicht zur Anwendung kommen.

In den zu Art 8 Abs.1 lit. c) korrespondierenden Erwägungsgründen 19 b und 21 a ist klarzustellen, dass auch Softwareupdates erfasst werden.

d) Art. 8 Abs. 1 b) ePrivacy VO Ausnahme bei Vorliegen einer Einwilligung

Die Möglichkeit eine Einwilligung abzugeben ist auf Smart-TVs kein geeignetes Mittel. Anders als bei Endgeräten zu aktiven Mediennutzung, wie Smart Phones, Tablet oder PC, wird der Smart-TV weitüberwiegend passiv genutzt. „Kommunikation“ mit dem Nutzer ist außerhalb des Installationsprozesses ein Fremdkörper und wird auf TV-Bildschirmen, die dem Nutzer ein immer besseres Seherlebnis bieten, als noch störender empfunden werden als auf anderen Bildschirmen.

Es ist daher zu begrüßen, dass wie Erwägungsgrund 19b erläutert, das Einwilligungserfordernis auf den Zeitpunkt des Vertragsschlusse („at the time of the conclusion of the contract“) vorverlegt werden kann. Bei vernetzten Endgeräten, besteht jedoch zwischen Endnutzern und Geräteherstellern keine direkte Vertragsbeziehung. Es sollte daher klargestellt, werden, dass die Einwilligung auch ohne direkte Vertragsbeziehung im Vorfeld und grundsätzlich abgegeben werden kann. Ein dem Vertragsschluss vergleichbarer Moment ist etwa bei vernetzten Verbraucherendgeräten der Installationsprozess.

Erwägungsgrund 19b ist dahingehend zu ergänzen, dass unabhängig von einer Vertragsbeziehung, die Möglichkeit besteht, eine vorrausgehende Einwilligung abzugeben.

e) Notwendige Klärung des Regelungsumfangs in Artikel 8 Abs. 2 ePrivacy VO

Artikel 8 Abs. 2 ePrivacy VO verbietet „*the collection of information sent by terminal equipment in order to connect with other devices or network systems*“. Dabei ist auch bei dieser Regelung unklar, wer Adressat dieses Verbots ist. Der Wortlaut lässt die Auslegung zu, dass jeder dieses Verbot zu beachten hat.

So wie die Regelung gefasst ist, wären z. B Anwendungen in denen ein Smart TV mit einem mobilen Endgerät gekoppelt wird, erfasst. Hierunter fallen zahlreiche Anwendungen. So kann das Smartphone genutzt werden um eine App auf dem Fernseher oder den Fernseher selbst zu steuern. Das mobile Gerät wird dabei letztlich zur Fernbedienung. Oder ein auf dem Fernseher oder auf dem mobilen

Endgerät angezeigter Inhalt wird auf das jeweilig andere Gerät übertragen. Oder auf dem Smartphone lassen sich Apps starten, die dann auf den großen Bildschirm (Smart TV) übertragen werden. Ferner würden auch sämtliche Smart-Home-Anwendungen erfasst. Wird von der Haustür oder dem Kühlschrank eine Nachricht auf den Fernseher übertragen und dort angezeigt, wäre der Tatbestand erfüllt.

Sämtliche dieser Anwendungsbeispiele erfordern es, dass zwei Endgeräte miteinander gekoppelt werden. Dies erfordert einen Mindestaustausch an Daten, damit sich die Geräte gegenseitig erkennen (z.B. Abfragen der MAC-Adresse bei Bluetooth-Verbindung). Es handelt sich hierbei ausschließlich um technische Daten, die notwendig sind, um die Kopplung durchzuführen.

Soll das mobile Endgerät etwa als Fernbedienung des Smart-TV eingesetzt werden, so ist es erforderlich, dass das Modell des jeweiligen Gerätes abgefragt wird (i.d.R. über Abfrage der herstellereigenen Geräte-ID), um festzustellen, ob ein entsprechendes Angebot für den Gerätetyp unterstützt wird. Auch über andere Protokolle wie DIAL (Discovery and Launch) kann der 1st screen (Smart TV) mit einem 2nd screen (mobiles Endgerät) verbunden werden, so dass Apps auf dem einen Screen gestartet werden können und über den 2nd screen gesteuert werden können. Hierfür ist es notwendig, abzufragen, ob der 1st screen das Protokoll unterstützt. Über Miracast (Screen Mirroring) ist es möglich, dass der Bildschirminhalt von einem auf den anderen Bildschirm übertragen wird. Auch hierbei wird zum Verbindungsaufbau zwischen mobilen Endgerät und Smart-TV notwendig, dass sich das jeweilige Endgerät zu erkennen gibt, dass es Miracast unterstützt.

Abgesehen davon, dass es sich bei den Informationen die von den Endgeräten ausgesandt werden, um rein technische Angaben handelt, erfasst Art. 8 Abs. 2 ePrivacy VO zudem Geräteverbindungen, die ausschließlich im Kontrollbereich des Nutzers liegen. Denn sowohl bei einer Bluetooth als auch einer LAN-Verbindung, bleibt der Nutzer in einem geschlossenen Netzwerk. Es ist daher nicht nachvollziehbar, warum im Zusammenhang mit dem Endgeräteschutz in Erwägungsgrund 13 am Ende, der Anwendungsbereich auf geschlossene Heimnetze erweitert werden soll. Wohingegen die Verordnung ansonsten auf einen Zugang zu einem „*public* electronic communications network“ abstellt.

Ferner ist auch der Regelungsumfang des Verbots unter Absatz 2 unverständlich. Denn das Verhältnis des Verbots in Artikel 8 Abs. 2 ePrivacy VO zum Erlaubnisgrund unter Art. 8 Abs. 2 a ePrivacy VO führt zu einem Zirkelschluss. Denn zum einen ist es verboten, Daten des Endgeräts zu erfassen, um eine Verbindung mit einem anderen Gerät zu ermöglichen („to enable it to connect“, Art 8 Abs. 2 ePrivacy VO), zum anderen, ist es jedoch erlaubt Daten zu verarbeiten, sofern diese notwendig sind, um ebendiese Verbindung herzustellen oder aufrechtzuerhalten („establishing or maintaining a connection“, Art. 8 Abs. 2 lit. a ePrivacy VO). In Konsequenz würde der Erlaubnisgrund unter lit. a so schließlich das Verbot aufheben.

Der Regelungsumfang der Vorschrift ist klarzustellen. Zumindest sollte präzisiert werden, wer Adressat dieser Regelung ist, um unnötige Überregulierung zu vermeiden.

In Erwägungsgrund 13, ist der letzte Satz zu streichen