

---

## Deutscher Industrie- und Handelskammertag

---

### **Stellungnahme zum Vorschlag für eine 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) - E-Privacy-VO**

Der Deutsche Industrie- und Handelskammertag (DIHK) ist die Dachorganisation der 79 Industrie- und Handelskammern (IHKs), die 3,6 Millionen Unternehmen als Mitglied haben. Der DIHK vertritt die Interessen der deutschen Wirtschaft gegenüber der Bundespolitik und den europäischen Institutionen und betreut und koordiniert darüber hinaus das Netzwerk der Deutschen Auslandshandelskammern (AHKs) mit 130 Standorten in 90 Ländern weltweit. Der DIHK ist im Register der Europäischen Kommission registriert (Registriernummer 22400601191-42).

#### **I. Vorbemerkungen**

Mit dem Vorschlag legt die EU-Kommission einen nächsten Baustein für die Schaffung eines digitalen Binnenmarkts vor. Nach der EU-Datenschutz-Grundverordnung ist die geplante VO eine weitere Datenschutzregelung, die aufgrund ihres Rechtscharakters als VO mehr Einheitlichkeit und Verbindlichkeit in den EU-Mitgliedstaaten herstellen soll. Dieser Ansatz ist zu begrüßen, weil auch die Dienste, die dieser Regelung unterfallen sollen, mindestens europäisch, wenn nicht gar weltweit tätig sind. Daher ist auch Erwägungsgrund 7 ein Systembruch, der beseitigt werden sollte.

Die Vorstellung der EU-Kommission, die E-Privacy-VO mit der EU-Datenschutz-Grundverordnung (DS-VO) am 25.05.2018 zusammen in Kraft treten zu lassen, halten wir ebenfalls für sinnvoll. So wissen Unternehmen spätestens zu diesem Zeitpunkt, welche rechtlichen Vorschriften sie einzuhalten haben, wenn sie sich datenschutzkonform verhalten wollen. Allerdings ist zu berücksichtigen, dass für die Umsetzung der DS-GVO zwei Jahre Übergangszeit vorgesehen sind, während bei der E-Privacy-VO zu befürchten ist, dass sie erst recht kurzfristig vor dem Termin ihres Inkrafttretens offiziell verkündet wird. Insofern muss geprüft werden, ob nicht doch eine gewisse Übergangszeit zwischen Verkündung und Inkrafttreten notwendig ist.

Die E-Privacy-VO ist im Verhältnis zur DS-GVO eine bereichsspezifische Regelung. Dennoch sollte sie die Ansätze der DS-GVO übernehmen und so Wertungswidersprüche vermeiden. Insbesondere vor dem Hintergrund des Anspruchs der EU-Kommission, die Datenschutzregelungen in der EU zu vereinheitlichen, ist es misslich, wenn es Diskrepanzen zur DS-GVO gibt. Das gilt für die Technikneutralität ebenso wie für Regelungen zur Zulässigkeit der Datenverarbeitung. Es ist nicht erkennbar, warum der VO-Vorschlag wesentlich engere Vorschriften vorsieht als die DS-GVO. Denn das Schutzziel ist dasselbe: das Persönlichkeitsrecht der betroffenen Person. Die unterschiedlichen Regelungen führen insbesondere bei kleineren und mittleren Unternehmen zu Problemen der Nachvollziehbarkeit: Ein einheitliches Datenschutzniveau ist leichter umzusetzen als jeweils bereichsspezifische Anforderungen, deren Unterschiedlichkeit aber nicht verständlich sind.

Andererseits verweist die E-Privacy-VO in etlichen Bereichen auf die DS-GVO, so dass sich die Frage stellt, ob diese Vorschriften nicht gestrichen werden können, da die DS-GVO als *lex generalis* ohnehin gilt.

Die E-Privacy-VO deckt von ihrem Anwendungsbereich sämtliche Dienste ab, mit denen elektronisch kommuniziert werden kann. Hierunter fallen alle Telefondienste ebenso wie internetbasierte Kommunikationsdienste. Mit der Ausdehnung des Anwendungsbereichs ist gleichzeitig ein Paradigmenwechsel verbunden, der bisher implementierte Geschäfts- und Finanzierungsmodelle der Internet-/Digitalwirtschaft erschwert, wenn nicht gar unmöglich macht. Der Entwurf verkennt die wichtige Rolle von Werbung für die Finanzierung kostenloser Onlineinhalte. Für den Verbraucher bedeutet dies, dass Content und Dienstleistungen für ihn im Internet künftig an einer Paywall enden. Die Verordnung hat damit gravierende Folgen für die Internetwirtschaft und die Informationsgesellschaft.

## **II. Zu den einzelnen Vorschriften**

### **Zu Art. 3**

Das hier verankerte Marktortprinzip ist zu begrüßen, wobei weiterhin die Rechtsdurchsetzung fraglich erscheint, wenn ein Dienst, der in einem Drittstaat ansässig ist, keinen Vertreter in der EU benennt.

### **Zu Art. 4**

Gerade angesichts kurzer Entwicklungszyklen solcher Dienste kann eine umfangreiche Aufzählung oder gar technische Beschreibung nicht erfolgreich und zielführend sein. Im Hinblick auf den

Grundsatz der Technikneutralität sollten die technischen Begriffe allgemein bzw. neutraler gefasst sein.

#### **Zu Art. 5**

Ziel dieser Vorschrift sind Werbeeinblendungen (vgl. Erwägungsgrund 19 Satz 4 - 7), bei denen E-Mails zuvor mit Suchbegriffen gescannt werden, um diese zu personalisieren. Es bleibt jedoch offen, wie dies technisch realisiert werden könnte. Denn persönliche E-Mail-Nachrichten lassen sich nicht allein dadurch anonymisieren, dass der Name des Versenders und Empfängers gelöscht wird. In der Regel enthalten E-Mails Inhalte, die eine eindeutige Personenbeziehbarkeit ermöglichen. Damit könnte diese Vorschrift in der Praxis nicht umgesetzt werden.

Ein Wertungswiderspruch ergibt sich hier zu Art. 6 DS-GVO: Danach ist bereits verboten, personenbezogene Daten aus E-Mails zu speichern und diese zu verwenden, um Werbung zu personalisieren.

#### **Zu Art. 6**

Die Regelung enthält höhere Anforderungen an die Erlaubnis als Art. 6 DS-GVO, wobei die Notwendigkeit dafür nicht erkennbar ist.

Nach Abs. 2 lit. c, Abs. 3 lit. b werden Einwilligung und Anonymisierung in ein Unter-/Überordnungsverhältnis gesetzt, das weder dem individuellen Recht zur Entscheidung über Art und Umfang einer Datenverarbeitung entspricht, noch der Einwilligung als Ausprägung des Rechts auf Datenschutz gerecht wird.

Die Notwendigkeit der Konsultation der Aufsichtsbehörde nach Art. 6 Abs. 3 lit. b ist nicht nachvollziehbar, denn der Schutz der betroffenen Person erfolgt bereits entweder über ihre Einwilligung oder die Anonymisierung, so dass ein sehr hoher Schutzbedarf nicht erkennbar ist.

Onlinemarketing nach der DS-GVO wird auch auf der Grundlage eines Vertrages oder der Rechtsgrundlage "berechtigtes Interesse" (Art. 6 Abs. 1 f DS-GVO) ermöglicht. Art. 6 des VO-Vorschlags sieht dies nicht vor. Gerade die Rechtsgrundlage "berechtigtes Interesse" spielt in der Wirtschaft (bei Geschäftsmodellen wie beim Onlinemarketing und u. a. auch für Big Data) eine erhebliche Rolle.

#### **Zu Art. 8**

Zwar sind nach dem Verordnungsentwurf u. a. Cookies zu Konfigurationszwecken, z. B. der Warenkorb im Onlineshop, auch ohne Einwilligung der Nutzer zulässig, jedoch ist der Ausnahmekatalog insgesamt zu restriktiv. Deutlich wird dies an Art.8 Abs. 1 lit. d, wonach eine Webanalyse nur

noch zulässig sein soll, wenn der Anbieter sie selbst vornimmt. Gerade mittelständische und kleine Unternehmen werden hierfür aber nicht die finanziellen und personellen Mittel, geschweige denn das erforderliche Wissen aufbringen können. Die gängigen Dienste von Drittanbietern können nicht mehr wie bisher genutzt werden.

Ebenso betroffen sind Anbieter von kostenlosen Internetdiensten oder Inhalten, da diese regelmäßig werbefinanziert sind. Fallen kostenlose Angebote weg, wird der Informationsfluss/Austausch und Wissenszuwachs eher gehemmt. Innovative Ideen/Produkte können nicht mehr ohne Weiteres entgeltfrei angeboten werden.

#### **Zu Art. 9**

Abs. 3 sieht eine Frist von sechs Monaten vor, nach der der Endnutzer daran erinnert werden soll, dass er seine Einwilligung widerrufen kann. Dies stellt eine erhebliche, zusätzliche Belastung für Betreiber elektronischer Kommunikationsdienste dar, deren Erfüllung gerade für kleinere und mittlere Unternehmen erheblichen Aufwand bedeutet, ohne dass erkennbar ist, dass damit dem Datenschutz tatsächlich mehr genützt würde.

#### **Zu Art. 10**

Cookies, insbesondere Third-party-Cookies, sind die Grundlage des werbefinanzierten Kostenlos-Internets. Es sollte klargestellt werden, dass das Weitersurfen eines Nutzers nach dem Einblenden eines Pop-up-Fensters/Banners bzw. das Wegklicken eines solchen als Einwilligung in das Setzen von Cookies gilt, denn Cookies müssen auch künftig möglich sein. Zudem bedarf es einer Klarstellung, dass Webseiten für Nutzer nur eingeschränkt oder gar nicht besucht werden können, falls sie Cookies nicht zustimmen.

Nutzer sollen künftig bei der Browser-Installation entscheiden, ob sie Third-Party-Cookies akzeptieren wollen oder nicht. Verweigert der Nutzer Third-Party-Cookies auf Browser-Ebene, kann keine der danach besuchten Webseiten einen Third-Party-Cookie setzen. Eine Cookie-Einwilligung des Nutzers nach Art. 8 Abs. 1 lit. b ist aber dann völlig wirkungslos, weil die Browser-Hersteller keinen Bottom-up-Dialog von der Website zum Browser erlauben. Der Nutzer kann seine allgemeinen Cookie-Einstellungen auf Browser-Ebene für eine attraktive und vertrauenswürdige Webseite nicht individuell ändern.

#### **Zu Art. 16**

Die VO nennt als Ziel für die Regulierung von Direktwerbung allgemein "elektronische Kommunikationsdienste", und die Begründung erklärt, Direktwerbung gegenüber Endnutzern technikunabhängig regulieren zu wollen. Dies erscheint richtig, da es keinen Unterschied macht, ob elektronische

Kommunikation per E-Mail, SMS, per Whatsapp oder sonstige bisher noch gar nicht erfundene Dienste direkt i. S. d. Direktwerbung an den Endnutzer gelangt. Nicht sinnvoll erscheint hingegen, dass nicht danach differenziert wird, ob der Endnutzer Verbraucher oder Gewerbetreibender/Unternehmer ist. Deren Schutzbedürftigkeit ist unterschiedlich zu bewerten, wie auch an Art. 16 Abs. 5 deutlich wird. Die Anknüpfung an die Rechtsform ist daher unpassend.

Artikel 16 Abs. 3 Buchstabe b verschärft das geltende Verbot der Rufnummernunterdrückung durch die – wenn auch alternativ als „oder-Vorschrift“ formulierte Pflicht, bereits anhand "eines Codes/einer Vorwahl kenntlich zu machen, dass es sich um einen Werbeanruf handelt". Schon heute ist es aber nicht möglich, Unternehmen zu ahnden, die gegen das Verbot der Rufnummernunterdrückung bewusst verstoßen, um ihre Identität zu verschleiern. Das würde so auch für "Kode-Verweigerer" gelten. Denn es ist davon auszugehen, dass diese auch keine korrekte Rufnummer anzeigen. Darüber hinaus wäre zu klären, wer diese Codes vergibt und wie der Verbraucher in diesen den Überblick bewahren soll. Durch die Möglichkeit, entweder die Rufnummer anzuzeigen oder einen Code zu verwenden, wird das Problem der fehlenden Identifizierbarkeit bei Verstoß gegen diese Vorschrift nicht gelöst. Allerdings mag ein solcher Code eine technische Anknüpfungsmöglichkeit bieten, solche Anrufe gar nicht erst durchzustellen, sondern von vorneherein zu unterdrücken. Dann ist aber zu vermuten, dass Unternehmen ihn ohnehin nicht nutzen werden. Aus unserer Sicht ist daher insgesamt die Kode-Anzeige anstelle der Rufnummernanzeige entbehrlich.

In Erwägungsgrund 29 ist im Übrigen die Rede vom Sperren stiller Anrufe und anderer betrügerischer und belästigender Anrufe. Das Sperren stiller Anrufe, also solcher mit Rufnummernunterdrückung, ist nachvollziehbar. Wie allerdings technisch festgestellt werden soll, dass ein Anruf betrügerisch oder belästigend ist, erschließt sich nicht. Dann müsste die Technik schließlich vorausschauend den Inhalt des Anrufs erkennen und bewerten, was faktisch nicht möglich ist. Ein ähnliches Problem ist in Erwägungsgrund 34 genannt, wonach „unerbetene Werbung eindeutig als solche erkennbar sein sollte“. Auch hier müsste im Vorhinein ein subjektives Element auf Seiten des Adressaten festgestellt werden.

Art. 16 Abs. 4 ist in der deutschen Fassung sprachlich unverständlich. Sprachlich richtig müsste es lauten: „Ungeachtet des Abs. 1 können Mitgliedstaaten durch Rechtsvorschriften vorsehen, dass die Tätigkeit persönlicher Direktwerbeanrufe an Endnutzer, die natürliche Personen sind, nur erlaubt ist, wenn diese dem Erhalt solcher Kommunikation nicht widersprochen haben.“ Durch die Verweisung auf Abs. 1 ist die Eigenschaft als natürliche Person schon umfasst, und die doppelte Nennung des Endnutzers in der bisherigen Fassung ist eher verwirrend. Inhaltlich gibt es derartige Opt-Out-Systeme in Deutschland bisher nicht. Es erscheint sehr unwahrscheinlich, dass die Öffnungsklausel in Deutschland genutzt werden wird.

In Art. 16 Abs. 5 wird geregelt, dass bei Endnutzern, die juristische Personen sind, lediglich ein ausreichender Schutz vor unerbetener Kommunikation sichergestellt werden muss. Gemeint ist wohl, dass die Anforderungen bei B2B-Kommunikation niedriger sein können. Allerdings sollte dann eher zwischen Verbrauchern und Gewerbetreibenden differenziert werden, da nicht jeder Gewerbetreibende eine juristische Person ist. Eine Differenzierung ausschließlich nach der Rechtsform knüpft unseres Erachtens an ein falsches Merkmal an. Vielmehr sollte formuliert werden „dass die berechtigten Interessen von Endnutzern, die als Unternehmen angesprochen werden, in Bezug auf unerbetene Kommunikation ... ausreichend geschützt werden.“

Artikel 16 Abs. 6 verpflichtet die Verwender elektronischer Kommunikationsdienste für Direktwerbung, diese Werbung als solche zu kennzeichnen. Hierdurch wird eine neue Informationspflicht geschaffen, die für Unternehmen Aufwand schafft und Angriffspunkte bei fehlerhafter oder fehlender Information bietet, da solche Fehler in Deutschland auch mittels Abmahnung durch jeden Wettbewerber und durch Verbraucherschutzvereine verfolgt werden können.

Wegen der generalklauselartigen Formulierung der VO dürfte es künftig zu Rechtsunsicherheit kommen, ab wann das Kennzeichnungsgebot beispielsweise für einen elektronischen Newsletter gilt, der Informationen, aber auch Werbung enthält.

### **Zu Art. 18**

Hiernach sollen die unabhängigen Aufsichtsbehörden unerbetene Kommunikation überwachen. Damit werden die Datenschutzbehörden zu Aufsichtsbehörden über Marketingmaßnahmen. Dies widerspricht dem bisher bewährten Grundsatz, dass Werbeverstöße zivilrechtlich geahndet werden von Mitbewerbern, Verbänden und Industrie- und Handelskammern (vgl. Art. 80 DS-GVO).

So droht für die betroffenen Unternehmen Rechtsunsicherheit durch divergierende Entscheidungen und unterschiedliche Akteure.

### **Ansprechpartnerinnen:**

Annette Karstedt-Meierrieks

E-Mail: [karstedt-meierrieks.annette@dihk.de](mailto:karstedt-meierrieks.annette@dihk.de)

Dr. Katrin Sobania

E-Mail: [sobania.katrin@dihk.de](mailto:sobania.katrin@dihk.de)