



# BDI

Bundesverband der  
Deutschen Industrie e.V.

## Entwurf einer ePrivacy-Verordnung – Stellungnahme der deutschen Industrie

### Datenverarbeitung in der elektronischen Kommunikation ausgewogener ausgestalten

- Die Europäische Kommission hat mit dem Entwurf der Verordnung über die Achtung des Privatlebens und den Schutz personenbezogener Daten in der elektronischen Kommunikation eine Diskussion über die Vertraulichkeit der Kommunikation angestoßen. Der BDI beschränkt sich in der vorliegenden Stellungnahme auf die daten(schutz)rechtlichen Artikel der Verordnung und sieht bei diesen noch erheblichen Handlungsbedarf.
- Es ist zu begrüßen, dass die Europäische Kommission das Potenzial der Datenökonomie erkannt hat und deren Aufbau entsprechend fördern will (vgl. etwa Mitteilung der Europäischen Kommission vom Januar 2017 zur Schaffung einer europäischen Datenwirtschaft). Es ist allerdings zu befürchten, dass der vorliegende Entwurf wegen bestehender Rechtsunsicherheiten, Abgrenzungsschwierigkeiten und restriktiver Datennutzungsmöglichkeiten gegenteilige Effekte nach sich ziehen wird.
- Für die deutsche Industrie stellt sich inzwischen die Frage nach der Sinnhaftigkeit einer sektorspezifischen Datenschutzregulierung für den Telekommunikationsbereich. Der BDI fordert den europäischen Gesetzgeber deshalb auf, den Verzicht auf die bestehenden Datenschutzregelungen ernsthaft zu erwägen.
- Darüber hinaus besteht aus Sicht des BDI an zahlreichen Stellen des Verordnungsentwurfs noch Veränderungsbedarf. Dies bezieht sich insbesondere auf den Anwendungsbereich, die Datenverarbeitungstatbestände sowie den beabsichtigten Zeitpunkt des Inkrafttretens.

## Inhaltsverzeichnis

A.	Sinnhaftigkeit der Regulierung insgesamt überdenken .....	4
B.	Anwendungsbereich anpassen .....	4
C.	Rechtsgrundlagen für Datenverarbeitungen zu eng.....	5
D.	Zeitpunkt des Inkrafttretens verschieben .....	6

Die Europäische Kommission hat mit dem Entwurf der Verordnung über die Achtung des Privatlebens und den Schutz personenbezogener Daten in der elektronischen Kommunikation und zur Aufhebung der Richtlinie 2002/58/EG eine Diskussion über die Vertraulichkeit der Kommunikation angestoßen. Der vorgelegte Verordnungsvorschlag (ePrivacy-VO-E) soll die Richtlinie von 2002 modernisieren. Der ePrivacy-VO-E ist ergänzend im Licht der im Mai 2018 in Kraft tretenden Datenschutzgrundverordnung zu sehen. Als Verordnung wird sie unmittelbar in den Mitgliedstaaten Anwendung finden.

Zielsetzung der Richtlinie aus dem Jahre 2002 war der Schutz der Privatsphäre und personenbezogener Daten im Bereich der elektronischen Kommunikation. Neben der Vertraulichkeit der Kommunikation (von Endgeräten und Webseiten) sind Sicherheitsaspekte, Berichtspflichten bei Datenschutzverstößen sowie Vorschriften zur Nutzung von Cookies wichtige Regelungsaspekte.

Elektronische Kommunikationsanbieter sind ein zentraler Baustein der digitalen Industrie in Deutschland und Europa. Sie bieten nicht nur die Netzinfrastruktur, sondern stehen wie kaum eine andere Branche im Rampenlicht der digitalen Transformation. Zugleich kommt netzbasierten Kommunikationsdiensten, sog. Over-the-top (OTT) Diensten, eine wachsende Bedeutung zu. Diese finden sich nicht nur im Consumer-Markt, auch Maschinen der Industrie 4.0 nutzen OTT-Dienste zur Kommunikation. Beide Bereiche unterliegen dem Regelungsbezug der Datenschutz-Grundverordnung (DSGVO).

Für die deutsche Industrie stellt sich – nach Verabschiedung der DSGVO und damit der Einführung eines harmonisierten, hohen Datenschutzstandards in der gesamten EU – die Frage nach der Sinnhaftigkeit einer sektorspezifischen Datenschutzregulierung für den Telekommunikationsbereich. Dies gilt umso mehr, als der ePrivacy-VO-E nicht nur mehr klassische Telekommunikationsunternehmen, sondern umfassend netzbasierte Kommunikationsdienste in einem noch unbekanntem Ausmaß betreffen wird. Zudem besteht Unklarheit darüber, welche Daten unter den ePrivacy-VO-E bzw. unter den Regelungsbezug der DSGVO fallen. Die Europäische Kommission hat es mit dem vorliegenden Entwurf verpasst, nach den Grundsätzen der besseren Rechtsetzung (*Better Regulation Principle*) vorzugehen.

Eine besondere Herausforderung stellt zudem der sehr ambitionierte Zeitplan – die Verordnung soll zeitgleich zur DSGVO verabschiedet werden – dar. Aufgrund der Vielzahl an ungelösten Fragestellungen empfiehlt der BDI einen längeren Konsultations- und Ausarbeitungszeitraum. Im aktuellen Entwurf würde die ePrivacy-Verordnung zu enormer Rechtsunsicherheit führen und somit den Innovationsstandort Deutschland und Europa schädigen.

Die deutsche Industrie bekennt sich zu hohen Datenschutz- und Vertraulichkeitsstandards in der digitalen Wirtschaft. Die DSGVO zielt auf einen ausgewogenen Kompromiss zwischen dem Schutz personenbezogener Daten und dem Innovationspotenzial für zukünftige Geschäftsmodelle ab. Der Entwurf der ePrivacy-VO stellt an vielen Stellen die mühsamen gefundenen Kompromisse nun wieder in Frage.

## A. Sinnhaftigkeit der Regulierung insgesamt überdenken

Bevor im Einzelnen auf die Regelungsaspekte des Verordnungsentwurfs eingegangen wird, ist die Sinnhaftigkeit eines sektorspezifischen Datenschutzrechts in Frage zu stellen. So hatte die Vorgängervorschrift, die im Jahr 2002 verabschiedete E-Privacy-Richtlinie, durchaus ihre Berechtigung. Denn ein einheitliches Datenschutzrecht gab es in Europa nicht, und die im Jahr 1995 verabschiedete Datenschutz-Richtlinie stammte noch aus der Vor-Internet-Ära. Damals kamen Unternehmen der Telekommunikationsindustrie noch am ehesten mit personenbezogenen Daten in Berührung.

Dies ist heute anders. Personenbezogene Daten haben für immer mehr Branchen Bedeutung – und fallen in immer mehr Branchen an. Es ist nicht mehr davon auszugehen, dass im Bereich der elektronischen Kommunikation Daten anfallen, die sensibler als in anderen Industrien sind. Es ist deshalb auch nicht ersichtlich, warum gerade für diesen Wirtschaftsbereich strengere Anforderungen als für den Rest der datenverarbeitenden Wirtschaft gelten sollen. Darüber hinaus legt die DSGVO einen hohen, einheitlichen Datenschutzstandard für alle Unternehmen in Europa fest. Schutzlücken, die die DSGVO in Bezug auf die Anforderungen an die Verarbeitung personenbezogener Daten hinterlassen hätte und die nun durch den ePrivacy-VO-E dringend geschlossen werden müssten, sind nicht bekannt. Alle Fragen des Umgangs mit personenbezogenen Daten durch Betreiber elektronischer Kommunikationsdienste können auch durch das neue europäische Datenschutzrecht umfassend gelöst werden.

Vor dem Hintergrund der im Mai 2018 in Kraft tretenden DSGVO spricht sich der BDI dafür aus, die fortbestehende Notwendigkeit einer sektorspezifischen Datenschutzregulierung einer kritischen Überprüfung zu unterziehen und auch den Mut zu haben, auf ein einmal bereits geschaffenes Gesetz bei Wegfall der Erforderlichkeit zu verzichten. Im Ergebnis würde größere Rechtssicherheit und weniger Rechtsfragmentierung herrschen – zum Nutzen von Wirtschaft und Verbraucher gleichermaßen.

## B. Anwendungsbereich anpassen

Unabhängig von den oben genannten grundsätzlichen Kritikpunkten begegnet der ePrivacy-VO-E auch im Einzelnen Bedenken.

So erweitert etwa der Entwurf den Adressatenkreis in einem nicht mehr vertretbaren Maße.

Zwar ist zu begrüßen, dass die Regelungen gem. Art. 3 Abs. 1 ePrivacy-VO-E für alle Marktakteure gelten sollen. Damit gilt das Marktortprinzip, das schon die DSGVO festschreibt, sinnvollerweise auch für das Datenschutzrecht in der elektronischen Kommunikation. Die Einführung dieses Prinzips ist notwendig, um für alle auf dem europäischen Markt tätigen Unternehmen gleiche Wettbewerbsbedingungen und für alle in der EU lebenden Verbraucher gleiche Schutzstandards zu gewährleisten. Auch ist sinnvoll, dass die Bestimmungen nicht mehr nur für die klassischen Kommunikationsdienste wie Sprachtelefonie und SMS, sondern auch für neuartige und von vielen Verbrauchern inzwischen genutzten Substitutionsdiensten wie VoIP-Telefonie, Messagingdienste und webbasierte E-Mail-Dienste ausgeweitet wird. Die Gewährleistung eines Level Playing Fields zwischen traditionellen Betreibern von Kommunikationsnetzen und OTTs (over the top) ist ein richtiges und wichtiges Anliegen.

Zu weit geht der Entwurf aber insofern, als dass auch sämtliche Kommunikationsvorgänge zwischen Maschinen erfasst sein sollen (vgl. etwa Erwägungsgrund 12). Diese M2M-Kommunikation, in der vernetzte Maschinen gegenseitig automatisiert Informationen untereinander austauschen, ist ein wesentlicher Baustein einer funktionierenden digitalen Industrie. Er betrifft so unterschiedliche Bereiche wie

vernetzt Fahrzeuge, automatisierte Lieferketten in der Logistikbranche oder vernetzte Produktionsstätten im verarbeitenden Gewerbe. Diesen Informationsaustausch umfassend den strengen Anforderungen der Verordnung, insbesondere den von der DSGVO abweichenden Regelungen zur Datenverarbeitung zu unterstellen, kann so vom Gesetzgeber nicht gewollt sein.

Auch kann eine M2M-Kommunikation mit der Kommunikation zwischen Menschen nicht grundsätzlich gleichgestellt werden. Eine solche Gleichstellung würde in vielen Fällen zu ungewollten Ergebnissen führen. So dürften die zwischen Maschinen ausgetauschten Informationen nicht bzw. nur unter den Bedingungen der Art. 5 ff. ePrivacy-VO-E verarbeitet werden – es gilt das datenschutzrechtliche Verbot mit Erlaubnisvorbehalt. Das bedeutet, dass Informationen nur dann verarbeitet werden dürfen, wenn die Beteiligten ihre Einwilligung gegeben haben. Wie dies etwa im Fall von automatisierter Kommunikation zwischen Maschinen, die nichtpersonenbezogene Daten austauschen, geschehen soll, bleibt mehr als unklar. Es sollte in Erwägungsgrund 12 mindestens klargestellt werden, dass nach eingehender Prüfung im Einzelfall auch M2M-Kommunikation in den Anwendungsbereich fallen *kann*, aber nicht muss. Auch sollte klargestellt werden, dass reine M2M-Plattformbetreiber nicht in den Kreis der Normadressaten fallen. Insgesamt empfiehlt es sich, M2M-Kommunikation nur in engen, begründeten Grenzen in den Regelungsbereich aufzunehmen. Denn der Entwurf weitet den Anwendungsbereich aktuell umfassend auf solche Kommunikation aus, die nicht zwischen Personen stattfindet. Sinn und Zweck einer staatlichen Regulierung „über die Achtung des Privatlebens und den Schutz personenbezogener Daten in der elektronischen Kommunikation“ ist es aber, das gesprochene bzw. geschriebene Wort zwischen Menschen unter besonderen Schutz zu stellen.

Schließlich ist zwar grundsätzlich nicht zu beanstanden, dass der Entwurf auch elektronische Kommunikationsdaten schützen möchte, die zwischen juristischen Personen ausgetauscht werden. Hier ist aber darauf zu achten, dass es nicht zu einer überschießenden Regulierung kommt, die Datenverarbeitungsprozesse zwischen Unternehmen in Kontext der Industrie 4.0 behindert oder unmöglich macht.

### C. Rechtsgrundlagen für Datenverarbeitungen zu eng

Auffällig ist, dass der ePrivacy-VO-E den Betreibern elektronischer Kommunikationsnetze und -dienste weit geringere Möglichkeiten zur Datenverarbeitung einräumt als unter dem Regelungsregime der DSGVO üblich. So gilt zwar einerseits auch im Rahmen des Verordnungsentwurfs der datenschutzrechtliche Grundsatz des Verbots mit Erlaubnisvorbehalt. In Art. 6 und Art. 8 ist aber andererseits vorgesehen, dass eine Datenverarbeitung grundsätzlich nur zum Zwecke der Leistungserbringung oder nach erfolgter Einwilligung des Betroffenen bzw. Endnutzers erlaubt ist. Insbesondere fehlen die anerkannten Möglichkeiten der Datenverarbeitung aufgrund berechtigten Interesses oder die Weiterverarbeitung zu kompatiblen Zwecken. Eine solche Beschränkung grenzt die Verarbeitungsmöglichkeiten unzulässig ein und führt darüber hinaus zu Beschränkungen der Unternehmen, die auch vom Gesetzgeber nicht gewollt sein können. So dürfen etwa nach Art. 6 Abs. 3 lit. b) ePrivacy-VO-E Betreiber von elektronischen Kommunikationsdiensten Kommunikationsinhalte nur dann verarbeiten, nachdem beide Kommunikationsteilnehmer ihre Einwilligung erteilt haben und nachdem die Aufsichtsbehörde konsultiert wurde. Dies würde etwa zu dem Ergebnis führen, dass ein E-Mail-Anbieter seine Spamfilter-Funktion seinem Kunden nur noch dann anbieten dürfte, wenn auch der Spam-Absender seine Einwilligung zu diesem Datenverarbeitungsvorgang gibt. Der BDI plädiert deshalb eindringlich dafür, im Laufe der weiteren Gesetzesberatungen die Verarbeitungstatbestände denen der DSGVO grundsätzlich anzugleichen.

In diesem Zusammenhang sollte ebenfalls die Sinnhaftigkeit des Art. 9 Abs. 3 Halbsatz 2 ePrivacy-VO-E überdacht werden. Danach sind Endnutzer alle 6 Monate daran zu erinnern, dass sie ihre Einwilligung widerrufen können. Die Rechtfertigung für eine solche Regelung, die dem Datenschutzrecht bislang fremd ist, ist nicht nachvollziehbar.

## **D. Zeitpunkt des Inkrafttretens verschieben**

Der Gesetzgeber hat den Anspruch, die neuen ePrivacy-Regelungen zeitgleich mit den Vorschriften der DSGVO zum Mai 2018 in Kraft treten zu lassen. Zwar ist es auch aus Unternehmenssicht grundsätzlich besser, wenn gesetzliche Reformen im selben Bereich gleichzeitig und nicht nachgelagert in Kraft treten. Die deutsche Industrie spricht sich dennoch dafür aus, für das Beratungsverfahren die Fristen von denen der DSGVO zu entkoppeln. Denn zum einen geht Gründlichkeit vor Schnelligkeit: Der Beratungsbedarf zum Reformgesetz ist offensichtlich noch zu groß, um dieses innerhalb weniger Wochen und Monate zu beschließen. Zum anderen sind viele Unternehmen, die tatsächlich und potenziell in den Anwendungsbereich der ePrivacy-VO-E fallen, zur Zeit mit dem Umstellen ihrer Datenverarbeitungsprozesse beschäftigt, um Compliance mit den Regelungen der DSGVO herzustellen. Viele Unternehmen müssten ihre Umstellungsprozesse nun stoppen oder nach kurzer Zeit erneut umstellen, um den Vorgaben gerecht zu werden. Zudem muss dem durch die ePrivacy-VO erneut entstehenden Anpassungsbedarf der Prozesse in den Unternehmen durch eine angemessene Implementierungsfrist nach Inkrafttreten Rechnung getragen werden.