PRIVATSPHÄRE UND ELEKTRONISCHE KOMMUNIKATION

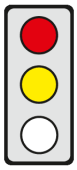
cep**Analyse** Nr. 16/2017

Centrum für Europäische Politik

KERNPUNKTE

Ziel der Verordnung: Die Kommission will die Vertraulichkeit der elektronischen Kommunikation und die darin enthaltenen Daten der Endnutzer effektiver schützen und zugleich deren freien Verkehr gewährleisten.

Betroffene: Endnutzer und Betreiber elektronischer Kommunikationsdienste, Hersteller von Software, die den Zugang zum Internet ermöglicht, Personen, die Informationen in Endgeräten von Endnutzern speichern oder aus diesen erheben, Direktwerbetreibende, Betreiber öffentlicher Verzeichnisse.



Pro: Einheitliche, auch für neue Kommunikationsdienste wie WhatsApp („OTT-Dienste“) geltende Regeln zum Schutz der Vertraulichkeit der elektronischen Kommunikation schaffen EU-weit gleiche Wettbewerbsbedingungen.

Contra: (1) Zahlreiche Unklarheiten der Verordnung machen ihre einheitliche Anwendung nahezu impraktikabel. Dies schafft Rechtsunsicherheit, die die EU als Standort für die Datenwirtschaft schwächt.

(2) Die angestrebte Kohärenz zwischen der Verordnung und der Datenschutzgrundverordnung (DSGVO) wird nicht erreicht. Die Verordnung muss grundlegend überarbeitet werden.

INHALT

Titel

Vorschlag COM(2017) 10 vom 10.01.2017 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)

Kurzdarstellung

- **Hintergrund und Ziele**
  - Nach der Reform des Schutzes personenbezogener Daten durch die Datenschutzgrundverordnung [(EU) 2016/679, s. cep**Analyse**] will die Kommission nun die Datenschutzrichtlinie 2002/58/EG für elektronische Kommunikation („E-Datenschutz-Richtlinie“) durch eine Verordnung ersetzen.
  - Die Verordnung soll die Datenschutzgrundverordnung (DSGVO) „präzisieren und ergänzen“, nicht hinter deren Schutzniveau zurückfallen und zeitgleich mit dieser ab dem 25.05.2018 gelten (Erwägungsgrund 5, Art. 29).
  - Ziel der Verordnung ist es (Begründung S. 2-6, 10),
    - die Grundrechte der Endnutzer auf Privatsphäre, Vertraulichkeit der Kommunikation und Schutz ihrer personenbezogenen Daten bei der Nutzung elektronischer Kommunikationsdienste zu gewährleisten,
    - den freien Verkehr von Kommunikationsdaten, -geräten und -diensten in der EU zu gewährleisten,
    - die bestehenden Regelungen auf neuartige Kommunikationsdienste wie Whatsapp oder Skype (Over-the-Top- oder kurz OTT-Dienste) auszuweiten, um gleiche Wettbewerbsbedingungen zu schaffen,
    - die Kohärenz mit der DSGVO sicherzustellen und Rechtssicherheit zu schaffen.
- **Anwendungsbereich und Definitionen**
  - Die Verordnung gilt für die Verarbeitung elektronischer Kommunikationsdaten bei der Bereitstellung und Nutzung elektronischer Kommunikationsdienste (EKD). Sie schützt ferner alle „Informationen in Bezug auf die Endeinrichtungen (nachfolgend: ‚Endgeräte‘) der Endnutzer“. (Art. 2 Abs. 1)
  - Sie schützt sowohl natürliche als auch juristische Personen (Art. 1 Abs. 1, 2).
  - EKD sind (Art. 4 Abs. 1 lit. b, Abs. 2, i.V.m. Art. 2 Ziff. 4 und 5 COM(2016) 590, s. cep**Analyse**)
    - Internetzugangsdienste,
    - Dienste, die zumindest überwiegend in der Übertragung von Signalen bestehen, z.B. die Festnetz- und Mobilfunktelefonie sowie die Maschine-zu-Maschine-Kommunikation (M2M), sowie
    - interpersonelle Kommunikationsdienste (IKD), die den direkten Informationsaustausch zwischen Personen ermöglichen, z.B. Webmail-Dienste, Internettelefonie, Messengerdienste und Chat-Funktionen.
  - „Elektronische Kommunikationsdaten“ sind (Art. 4 Abs. 3 lit. a-c):
    - Kommunikationsinhalte – z.B. Texte, Videos –, die mittels EKD übermittelt werden, sowie
    - Metadaten, die in elektronischen Kommunikationsnetzen verarbeitet werden, um Inhalte überhaupt übermitteln oder auszutauschen zu können, z.B. Standortdaten und der Kommunikationszeitpunkt.
  - Endgeräte sind etwa PCs, Tablets, Smartphones und Satellitenfunkanlagen (Art. 4 Abs. 1 lit. c).
  - Die Verordnung gilt für (Art. 3 Abs. 1 lit. a-c, Erwägungsgrund 9)
    - alle Betreiber, die EKD für Endnutzer in der EU „bereitstellen“, auch wenn die Bereitstellung von außerhalb der EU erfolgt oder die Kommunikationsdaten nicht in der EU verarbeitet werden,
    - alle „Nutzer“ dieser Dienste und
    - die Endgeräte der Endnutzer in der EU.

Autoren: Dr. Anja Hoffmann, LL.M. (Eur.) und Philipp Eckhardt, | hoffmann@cep.eu
cep | Kaiser-Joseph-Straße 266 | 79098 Freiburg | Telefon 0761 38693-107 | www.cep.eu

- **Vertraulichkeit elektronischer Kommunikationsdaten**
  Elektronische Kommunikationsdaten sind vertraulich. Das Abhören, Speichern, Scannen oder sonstige Abfangen, Überwachen oder Verarbeiten solcher Daten durch andere Personen ist grundsätzlich verboten. (Art. 5)
- **Zulässigkeit der Verarbeitung elektronischer Kommunikationsdaten**
  - Elektronische Kommunikationsdaten – sowohl Kommunikationsinhalte als auch -metadaten – dürfen ausnahmsweise verarbeitet, z.B. gespeichert werden, wenn und solange dies nötig ist, um
    - die Übermittlung der Kommunikation durchzuführen (Art. 6 Abs. 1 lit. a),
    - die Sicherheit von EKD und Netzen zu gewährleisten oder um Defekte zu erkennen (Art. 6 Abs. 1 lit. b).
  - Elektronische Kommunikationsmetadaten dürfen darüber hinaus nur verarbeitet werden (Art. 6 Abs. 2),
    - wenn der „betreffende" Endnutzer in ihre Verarbeitung für bestimmte Zwecke eingewilligt hat, z.B. um vom Betreiber Zusatzdienste zu erhalten, sofern diese Zwecke bei Anonymisierung der Daten unerreichbar sind,
    - um EU-rechtliche Qualitätsanforderungen – z.B. an Verzögerungsschwankungen – einhalten zu können, oder
    - um die Dienste abzurechnen oder um deren missbräuchliche Nutzung zu bekämpfen.
  - Elektronische Kommunikationsinhalte dürfen darüber hinaus nur verarbeitet werden,
    - wenn die Inhalte allein zu dem Zweck verarbeitet werden, einen bestimmten Dienst „für einen Endnutzer" bereitzustellen, der ohne Verarbeitung dieser Inhalte nicht erbracht werden kann, und wenn „der oder die betreffenden" Endnutzer ihre Einwilligung erteilt haben (Art. 6 Abs. 3 lit. a), oder
    - wenn die Inhalte für bestimmte sonstige Zwecke verarbeitet werden, die bei Anonymisierung der Inhalte nicht erreichbar sind, und „alle betreffenden" Endnutzer eingewilligt haben; zudem muss der Betreiber die Aufsichtsbehörde konsultieren und deren Empfehlungen beachten (Art. 6 Abs. 3 lit. b, Art. 36 DSGVO).
  - Sobald die elektronischen Kommunikationsdaten nicht mehr zu den erlaubten Zwecken benötigt werden, endet die Verarbeitungserlaubnis, und der Betreiber muss sie löschen oder anonymisieren (Art. 7 Abs. 1–3).
  - Die Einwilligung des Endnutzers muss die Bedingungen der DSGVO erfüllen: Sie muss freiwillig, in Kenntnis der Sachlage und unmissverständlich für einen bestimmten Fall erteilt werden und jederzeit widerrufbar sein (Art. 9 Abs. 1 i.V.m. Art. 4 Nr. 11, Art. 7 DSGVO).
- **Schutz von „Informationen in Bezug auf die Endeinrichtungen der Endnutzer"**
  - Grundsätzlich darf niemand außer dem betreffenden Endnutzer die „Verarbeitungs- und Speicherfunktionen" der Endgeräte der Endnutzer nutzen – z.B. um Cookies zu speichern – oder Informationen aus diesen Endgeräten erheben, z.B. dort gespeicherte Fotos oder Kontaktdaten (Art. 8 Abs. 1).
  - Ausnahmen sind zulässig, wenn der Endnutzer eingewilligt hat oder die Nutzung bzw. Erhebung nötig ist
    - für die Übermittlung der Kommunikation oder
    - für die Bereitstellung eines vom Endnutzer gewünschten „Dienstes der Informationsgesellschaft", etwa wenn Cookies zur Authentifizierung des Endnutzers in einem Online-Shop erforderlich sind; der Eingriff in die Privatsphäre darf hier nur geringfügig sein (Erwägungsgrund 21); oder
    - für die Messung der Nutzerzahlen, jedoch nur wenn die Messung vom Betreiber des Dienstes der Informationsgesellschaft selbst – und nicht von Dritten – vorgenommen wird.
  - Die Einwilligung kann über die Software, die den Abruf von Informationen aus dem Internet ermöglicht, etwa über Webbrowser und Apps, erteilt oder verweigert werden (Art. 9 Abs. 2). Anbieter müssen ihre Software so konfigurieren, dass Endnutzer sich bei Installation oder Update für eine „verbindliche" und gegenüber Dritten „durchsetzbare" Privatsphäreeinstellung entscheiden müssen (Art. 10, Erwägungsgrund 22).
  - Grundsätzlich darf niemand Informationen erheben, die von Endgeräten ausgesendet werden, um sich mit anderen Geräten oder Netzen zu verbinden, z.B. Teilnehmerkennungen, Bluetooth- und WLAN-Signale (Art. 8 Abs. 2, Erwägungsgrund 25). Ein solches „Offline-Tracking" ist ausnahmsweise zulässig,
    - wenn und solange dies nötig ist, um eine Verbindung herzustellen, oder
    - wenn der Erhebende geeignete Datensicherheitsmaßnahmen ergreift und die Endnutzer in einem „deutlichen Hinweis" u.a. über den Zweck der Erhebung und die Möglichkeit informiert, diese zu beenden.
- **Schutz vor unerbetener Direktwerbung**
  - Direktwerbung aller Art, einschließlich Wahlwerbung, darf nur über EKD an natürliche Personen gerichtet werden, wenn diese eingewilligt haben („Opt-in", Art. 16 Abs. 1, Erwägungsgrund 32). Die Mitgliedstaaten können für persönliche Werbeanrufe ein Widerspruchsrecht ausreichen lassen („Opt-out", Art. 16 Abs. 4).
  - Innerhalb bestehender Kundenbeziehungen sind Werbe-E-Mails für „eigene ähnliche Produkte oder Dienstleistungen" zulässig, wenn der Kunde dem nicht widersprochen hat („Opt-Out", Art. 16 Abs. 2).
- **Einschränkungen und Durchsetzung der Verordnung, Schadensersatz**
  - Die Mitgliedstaaten dürfen die Vertraulichkeit zum Schutz wichtiger Interessen gesetzlich beschränken (Art. 11).
  - Die Einhaltung der Verordnung wird von den für die DSGVO zuständigen unabhängigen nationalen Aufsichtsbehörden überwacht (Art. 18). Diese haben die in der DSGVO geregelten Befugnisse und können ggf. Bußgelder, auch in Millionenhöhe, verhängen (Art. 23 Abs. 1-3 i.V.m. Art. 58 Abs. 2 lit. i) DSGVO).
  - Endnutzer können Schadensersatz verlangen und haben – mit Ausnahme von Verbandsklagen – die gleichen Beschwerderechte und gerichtlichen Rechtsbehelfe wie unter der DSGVO (Art. 21 und 22).

Wesentliche Änderungen zum Status quo

- Künftig werden die Vorgaben in einer Verordnung und nicht wie bislang in einer Richtlinie geregelt.
- Bisher gelten die Regelungen nur für klassische Kommunikationsdienste, künftig auch für OTT-Dienste.

- Das bisherige Opt-in-Erfordernis für Cookies wird zu einem generellen Schutz von Informationen in Endgeräten ausgeweitet. Demgegenüber wird das „Offline-Tracking“ ohne Einwilligung erlaubt.
- Neu ist, dass künftig jede Software, die den Zugang zum Internet ermöglicht (Browser, App), den Endnutzer bei Installation auffordern muss, eine verbindliche Privatsphäreeinstellung zu wählen.
- Bisher überwachen in den Mitgliedstaaten verschiedene Behörden die Einhaltung der Verordnung; künftig muss die auch für die DSGVO zuständige nationale Behörde dies tun. Die Geldbußen werden erhöht.

Subsidiaritätsbegründung der Kommission

Im transnationalen Markt der elektronischen Kommunikation kann nur ein Handeln auf Unionsebene einen EU-weit einheitlichen Grundrechtsschutz, den freien Datenverkehr und einen fairen Wettbewerb gewährleisten.

Politischer Kontext

Im Rahmen ihrer Strategie für einen digitalen Binnenmarkt [COM(2015) 192, s. cep**Analyse**] will die Kommission auch die Regelungen zum Schutz der Privatsphäre der Nutzer von EKD reformieren.

Stand der Gesetzgebung

10.01.17	Annahme durch Kommission
Offen	Annahme durch Europäisches Parlament und Rat, Veröffentlichung im Amtsblatt, Inkrafttreten

Politische Einflussmöglichkeiten

Generaldirektionen:	GD Kommunikationsnetze, Inhalte und Technologien (federführend)
Ausschüsse des Europäischen Parlaments:	Bürgerliche Freiheiten, Justiz und Inneres (federführend), Berichterstatter: Marju Lauristin (S&D)
Bundesministerien:	Bundeswirtschaftsministerium (federführend)
Ausschüsse des Deutschen Bundestags:	Wirtschaft (federführend);
Entscheidungsmodus im Rat:	Qualifizierte Mehrheit (Annahme durch 55% der Mitgliedstaaten, die 65% der EU-Bevölkerung ausmachen)

Formalien

Kompetenznorm:	Art. 16 Abs. 2 AEUV (Datenschutz), 114 AEUV (Binnenmarkt)
Art der Gesetzgebungszuständigkeit:	Geteilte Zuständigkeit (Art. 4 Abs. 2 AEUV)
Verfahrensart:	Art. 294 AEUV (ordentliches Gesetzgebungsverfahren)

BEWERTUNG

Ökonomische Folgenabschätzung

Ordnungspolitische Beurteilung

Einheitliche, auch für OTT-Dienste geltende Vorschriften zum Schutz der Privatsphäre und **der Vertraulichkeit der elektronischen Kommunikation** stärken den Binnenmarkt, denn sie führen zu geringeren Kosten für datenverarbeitende Unternehmen und **schaffen EU-weit gleiche Wettbewerbsbedingungen.** Letzteres wird insbesondere auch dadurch erreicht, dass künftig nicht nur traditionelle, sondern auch neuartige elektronische Kommunikationsdienste (OTT-Dienste) die Vorgaben erfüllen müssen.

Der Kommissionsvorschlag weist jedoch gravierende Schwachstellen auf. Zum einen ist das Verhältnis zur Datenschutzgrundverordnung (DSGVO) in vielen Fällen unklar. Zum anderen enthält der Vorschlag eine Vielzahl unklarer Vorschriften (s. juristische Bewertung). Dies **schafft erhebliche Rechtsunsicherheit, die** in der Konsequenz investitionshemmend wirkt und **die EU als Standort für die Datenwirtschaft schwächt. Die Verordnung** ist in ihrer jetzigen Form daher abzulehnen. Sie **muss grundlegend überarbeitet werden**, auch wenn dies dazu führen dürfte, dass ein gleichzeitiges Inkrafttreten mit der DSGVO nicht zu realisieren sein wird.

Juristische Bewertung

Kompetenz

Unproblematisch, die Verordnung wird zu Recht auf die Datenschutzkompetenz (Art. 16 Abs. 2 AEUV und auf die Binnenmarktkompetenz (Art. 114 AEUV) gestützt.

Subsidiarität

Die Vertraulichkeit der grenzenlosen Kommunikation kann die EU besser schützen als die Mitgliedstaaten.

Verhältnismäßigkeit gegenüber den Mitgliedstaaten

Ein EU-weit einheitlicher und mit der DSGVO kohärenter Schutz kann nur durch eine Verordnung gewahrt werden, weil bei ihr u.U. divergierende Umsetzungen in nationales Recht entfallen. **Die Verordnung lässt** jedoch **die für unmittelbar geltendes Recht nötige Normenklarheit vermissen, ist** daher unverhältnismäßig und **damit rechtswidrig. Zahlreiche Unklarheiten machen ihre einheitliche Anwendung nahezu impraktikabel.** Dies betrifft z.B. unklare Definitionen durch Verweise auf den noch nicht beschlossenen „Kodex für die elektronische Kommunikation“ [COM(2016) 590], vage Erlaubnistatbestände – z.B. welcher „betreffende“ Endnutzer muss einwilligen? –, eine intransparente Verquickung von Datenschutz- und Vertraulichkeitsregeln – die Verordnung schützt die Vertraulichkeit der Kommunikation unabhängig von einem Personenbezug, will aber den „Schutz per-

sonenbezogener Daten" gewährleisten –, und die mangelnde Abgrenzung zur DSGVO (s.u.). Alle zentralen Begriffe sind in der Verordnung zu definieren. Klarzustellen ist, welche Regelung welche Adressaten verpflichtet.
Die Verpflichtung der Mitgliedstaaten, die Verordnung durch ihre unabhängige Datenschutzbehörde überwachen zu lassen, greift unverhältnismäßig in die nationale Behördenorganisation ein. Die EU-Grundrechtecharta (GRCh) schreibt die Überwachung durch eine unabhängige Behörde nur für die Einhaltung der Vorschriften über den Schutz personenbezogener Daten, nicht aber für den Schutz der Kommunikation vor. Weniger eingreifend wäre daher eine Pflicht der bisherigen Aufsichtsbehörde zur effektiven Zusammenarbeit mit den Datenschutzbehörden.

Sonstige Vereinbarkeit mit EU-Recht

Das grundsätzliche Verarbeitungsverbot für elektronische Kommunikationsdaten gewährleistet einerseits das Grundrecht auf Achtung der Kommunikation im Sekundärrecht und greift andererseits in die durch Art. 16 GRCh geschützte unternehmerische Freiheit der EKD-Betreiber ein. Wann solche Daten ausnahmsweise verarbeitet werden dürfen, lässt sich derzeit jedoch kaum verlässlich beurteilen, weil die Verordnung hierfür teils schwer voneinander abgrenzbare Erlaubnistatbestände mit teilweise unklaren Voraussetzungen vorsieht. Klarstellungsbedürftig ist u.a., welcher Tatbestand welche Fälle erfassen soll, welche „betreffenden Endnutzer" einwilligen müssen und in welchem Verhältnis Einwilligung und Anonymisierung zueinander stehen. **Dass die Verordnung für die Datenverarbeitung weithin die Einwilligung der Endnutzer verlangt, stärkt zwar den Grundrechtsschutz. Das Einwilligungserfordernis ist jedoch nicht überall praktikabel**, z.B. für den Spam- und Virenschutz sowie für die M2M-Kommunikation einschließlich des autonomen Fahrens**. Insoweit müssen zusätzliche Ausnahmetatbestände geschaffen werden.** Zu prüfen ist, ob die Verarbeitung ohne Einwilligung zum Schutz lebenswichtiger Interessen einer Person oder in bestimmten Fällen, in denen der Eingriff in die Vertraulichkeit durch ergänzende Sicherheitsmaßnahmen wie Pseudonymisierung und/oder Verschlüsselung minimalisiert werden kann, unter flexibleren Bedingungen erlaubt werden kann.
Die angestrebte Kohärenz zwischen der Verordnung und der DSGVO wird nicht erreicht, obwohl sich deren Anwendungsbereiche überschneiden. Das Verhältnis der Regelungen zueinander ist oft unklar. Es muss klargestellt werden, wann nur die DSGVO gilt – z.B. nach Abschluss des Kommunikationsvorgangs? –, wann die Regelungen der Verordnung die DSGVO „ergänzen" – z.B. inwieweit deren allgemeine Grundsätze auch hier gelten – und wann sie die Regelungen der DSGVO „präzisieren", d.h. verdrängen – also ein Rückgriff auf deren Erlaubnistatbestände ausgeschlossen ist. Strengere Regelungen als unter der DSGVO sind nur dort gerechtfertigt, wo die spezifischen Risiken der Nutzung elektronischer Kommunikationsdienste es erfordern. Teilweise bleibt die Verordnung entgegen der erklärten Absicht der Kommission sogar hinter dem Schutzniveau der DSGVO zurück. So bietet die bloße Option, Cookies abzulehnen, weniger Schutz als eine Software, die – getreu dem „Privacy by Default"-Grundsatz der DSGVO – bereits entsprechend voreingestellt ist. Auch wird das Offline-Tracking schon bei bloßem Hinweis und Opt-Out-Möglichkeit erlaubt. Konsequenter wäre es, auch hier grundsätzlich eine Einwilligung zu fordern, das Tracking aber auch darüber hinaus in engen Grenzen zuzulassen, etwa zur Ermittlung von Personenzahlen.
Auch die Regelungen zu den Privatsphäreeinstellungen sind verfehlt. Die entsprechenden Konfigurationspflichten der Softwarehersteller greifen unverhältnismäßig in deren unternehmerische Freiheit (Art. 16 GRCh) und ihr Eigentumsrecht (Art. 18 GRCh) ein. Ihr Zweck, benutzerfreundliche Einwilligungsmöglichkeiten zu schaffen, wird verfehlt, da eine „vereinfachte" Einwilligung in Einstellungen oft kaum rechtswirksam erteilt werden kann. Nach der DSGVO muss der Endnutzer stets „informiert" und „für den bestimmten Fall" einwilligen. Dies ist nicht gewährleistet, wenn er Cookies in den Browsereinstellungen generell erlaubt, weil es unmöglich ist, die konkreten Zwecke aller Datenverarbeitungen auf evtl. später besuchten Webseiten zu antizipieren. Eine solche „Vorab-Pauschaleinwilligung" bietet dem Endnutzer keine Differenzierungsmöglichkeit und ist zudem intransparent. Eine generelle Ablehnung von Cookies ist zwar in Einstellungen möglich. Die Verordnung regelt aber nicht, wie sich diese Einstellungen zu unabhängig davon abgegebenen Einwilligungen verhalten. Unklar ist auch, in welchem Umfang Anbieter ihre Dienste an eine Zustimmung zur Datenerhebung durch Cookies koppeln dürfen und inwiefern Cookie-Gegner Webseiten evtl. nicht mehr uneingeschränkt nutzen können.

Auswirkungen auf das deutsche Recht

Die direkt anwendbaren Regelungen der Verordnung verdrängen die deutschen bereichsspezifischen Regeln zum Telekommunikationsdatenschutz in §§ 91 ff. TKG, zum Fernmeldegeheimnis (§ 88 TKG), zum Datenschutz bei Telemedien (§ 11 ff. TMG) sowie zum Direktmarketing in § 7 UWG. Diese werden ohnehin teilweise bereits von der DSGVO verdrängt. Die Regelungen sollten aufgehoben werden, sofern sie nicht durch Öffnungsklauseln der Verordnung erlaubt werden oder sonst über zwingendes EU-Recht hinausgehen.

Zusammenfassung der Bewertung

Einheitliche, auch für OTT-Dienste geltende Regeln zum Schutz der Vertraulichkeit der elektronischen Kommunikation schaffen EU-weit gleiche Wettbewerbsbedingungen. Die Verordnung lässt jedoch die für unmittelbar geltendes Recht nötige Normenklarheit vermissen und ist damit rechtswidrig. Zahlreiche Unklarheiten machen ihre einheitliche Anwendung nahezu impraktikabel. Dass die Verordnung für die Datenverarbeitung weithin die Einwilligung der Endnutzer verlangt, stärkt zwar den Grundrechtsschutz. Das Einwilligungserfordernis ist jedoch nicht überall praktikabel. Insoweit müssen zusätzliche Ausnahmetatbestände geschaffen werden. Die angestrebte Kohärenz zwischen der Verordnung und der DSGVO wird nicht erreicht. Auch die Regelungen zu den Privatsphäreeinstellungen sind verfehlt. All dies schafft erhebliche Rechtsunsicherheit, die die EU als Standort für die Datenwirtschaft schwächt. Die Verordnung muss grundlegend überarbeitet werden.