Datensouveränität statt digitaler Hürdenlauf

Die Auswirkungen der geplanten ePrivacy-Verordnung auf Wettbewerb und Wachstum in Europa

Policy Paper

Roland Berger

IEF

Vorwort

Die europäische Digitalwirtschaft steht vor einem Umbruch. Die EU-Datenschutzgrundverordnung (DSGVO), die im Mai 2018 in Kraft tritt, ist ein Meilenstein auf dem Weg zu einheitlichen Regeln für die Nutzung von Kundendaten in allen 28 EU-Staaten. Neben der Stärkung des Datenschutzes und der Kundenrechte wird mit ihr auch ein wichtiger Schritt für die Schaffung eines effektiven digitalen Binnenmarkts gemacht.

Ironischerweise wird diese Wachstumsvision gerade durch eine andere Initiative der Europäischen Kommission getrübt: die sogenannte ePrivacy-Verordnung. Ursprünglich als Spezialgesetzgebung zur DSGVO angelegt, die deren Regeln im Hinblick auf elektronische Kommunikation präzisieren und ergänzen soll, geht die Verordnung in ihrer jetzigen Form über die Regeln der DSGVO hinaus und schafft zusätzliche Hürden für die Verarbeitung personenbezogener Daten. Während sie in maßgeblichen Bereichen für erhebliche rechtliche Unsicherheit sorgt, ist der Anwendungsbereich dennoch so weit gefasst, dass nahezu alle europäischen Unternehmen davon betroffen wären.

Die ePrivacy-Verordnung droht deshalb – mutmaßlich unbeabsichtigt –, die digitale Wertschöpfung in ganz Europa und die Entwicklung von hiesigen Digitalunternehmen auszubremsen. Wir fordern daher eine Überarbeitung der vorgeschlagenen Regulierung, um eine faire Balance zwischen Datenschutz und Datennutzung entlang des Prinzips der Datensouveränität zu gewährleisten.

Dieses Policy Paper basiert auf einer Stellungnahme der Internet Economy Foundation vom Juli 2017. Seitdem hat sich in Europas Digitalwirtschaft – von Startups über etablierte Internetunternehmen bis hin zu Unternehmen der Old Economy mit Digitalisierungsbemühungen – der Konsens herausgebildet, dass die erfolgreiche digitale Zukunft Europas durch die vorgeschlagene ePrivacy-Verordnung gefährdet wird. Zahlreiche Akteure haben uns ermutigt, auch in ihrem Namen zu sprechen, diese Bedenken aufzunehmen und darüber aufzuklären. Die Analyse setzt sich daher mit den möglichen Auswirkungen der vorgeschlagenen Regulierung im wirtschaftlichen Kontext auseinander, präsentiert Fallstudien, die diese veranschaulichen und demonstriert, was auf dem Spiel steht. Wir hoffen, mit diesem Papier einen konstruktiven Beitrag zur aktuellen Debatte und zur Gestaltung der digitalen Zukunft Europas zu leisten.

Friedbert Pflüger
Vorsitzender
Internet Economy
Foundation

Clark Parsons
Geschäftsführer
Internet Economy
Foundation

Drei Punkte für wirksamen Datenschutz und faire Wettbewerbsbedingungen:

1. Flexibilität für Datenverarbeitung erhalten
2. Unabhängigkeit digitaler Dienste von Browsern gewährleisten
3. Übergangsfristen für die Umsetzung neuer Regeln einräumen

Inhalt

1 WORÜBER WIR SPRECHEN:

Der Entwurf für eine ePrivacy-Verordnung

Wirksamer und fairer Datenschutz bringt die Interessen der Bürger und der Wirtschaft in Einklang. Er ermöglicht der Wirtschaft, ihren Kunden eine große Bandbreite digitaler Produkte anzubieten. Und er gewährleistet die Datensouveränität der Bürger, die auf Grundlage transparenter Regeln Klarheit über die Verarbeitung ihrer personenbezogenen Daten haben. Ein derart gestalteter Datenschutz wird auf europäischer Ebene bislang nur ansatzweise umgesetzt. Die im Jahr 2016 verabschiedete Datenschutzgrundverordnung (DSGVO) der EU sorgt zwar für eine europaweite Vereinheitlichung des Datenschutzes und stärkt die Rechte der Konsumenten. Gleichzeitig schränkt die DSGVO jedoch die Möglichkeiten der Unternehmen zur Verarbeitung personenbezogener Daten ein und stellt die Verwirklichung datengetriebener Geschäftsmodelle damit vor große Herausforderungen.

Im Januar 2017 hat die Europäische Kommission nun den Entwurf einer ePrivacy-Verordnung[1] vorgelegt, welche die bislang gültige eDatenschutz-Richtlinie aus dem Jahr 2002[2] ersetzen soll. Am 21. Juni hat die zuständige Berichterstatterin des federführenden Ausschusses für bürgerliche Freiheiten, Justiz und Inneres (LIBE) im Europäischen Parlament, Marju Lauristin, den Berichtsentwurf zum Vorschlag der Europäischen Kommission vorgestellt.

Die geplante ePrivacy-Verordnung soll europaweit einheitliche Datenschutzregeln im Bereich der elektronischen Kommunikation schaffen. Sie ist als Spezialgesetzgebung zur DSGVO angelegt und soll deren Regeln im Hinblick auf elektronische Kommunikationsdaten präzisieren und ergänzen. Deshalb soll sie sich nach Absicht der Europäischen Kommission primär an die Anbieter elektronischer Kommunikationsdienste richten. Der von der Kommission vorgelegte Entwurf der ePrivacy-Verordnung würde durch die fortschreitende Digitalisierung und Konvergenz jedoch auch schwerwiegende, mutmaßlich nicht beabsichtigte Konsequenzen für die europäische Wirtschaft als Ganzes haben. Voraussichtlich wird der LIBE in seiner Sitzung am 11. und 12. Oktober 2017 den Berichtsentwurf diskutieren und verabschieden, sodass das Plenum noch im Oktober über die vorgeschlagene Verordnung beraten kann. Parallel dazu diskutieren die EU-Mitgliedstaaten derzeit im Rat den Kommissionsvorschlag und versuchen, eine gemeinsame Position zu finden. Ob eine Einigung im Rat noch in 2017 oder erst 2018 erzielt wird, ist heute noch nicht absehbar. Die Verordnung kann erst dann erlassen werden, wenn sich Parlament, Rat und Kommission im Trilog auf einen Kompromiss über den Kommissionsvorschlag geeinigt haben. Danach soll es nach Absicht der Kommission jedoch schnell gehen: Schon am 25. Mai 2018 soll die ePrivacy-Verordnung ohne Übergangsfrist in Kraft treten. Es ist deshalb höchste Zeit, einen genauen Blick auf die Auswirkungen der geplanten ePrivacy-Verordnung auf die europäische Wirtschaft und auf die Wettbewerbsfähigkeit datengetriebener Geschäftsmodelle *made in Europe* zu werfen.

Die konkreten Auswirkungen der geplanten ePrivacy-Verordnung sind mit großer Ungewissheit behaftet.

1 Verordnung über die Achtung des Privatlebens und den Schutz personenbezogener Daten in der elektronischen Kommunikation (ePrivacy-Verordnung)
2 Richtlinie 2002/58/EG über die Verarbeitung personenbezogener Daten und den Schutz der Privatsphäre in der elektronischen Kommunikation (Datenschutzrichtlinie für elektronische Kommunikation)

Anstatt einer falsch verstandenen Datensparsamkeit sollten die europäischen Datenschutzregeln dem Zielbild der Datensouveränität folgen.

Denn erstens weichen viele Regeln im Entwurf der ePrivacy-Verordnung von der DSGVO ab und sorgen damit für erhebliche rechtliche Unsicherheit. Zweitens befindet sich der Entwurf der Verordnung noch im Gesetzgebungsverfahren, in dessen Zuge mit zahlreichen Änderungen zu rechnen ist. Die große Bedeutung personenbezogener Daten für die europäische Wirtschaft und die vielfach geäußerte Kritik am Entwurf der ePrivacy-Verordnung erfordern eine umfassende Prüfung der beabsichtigten und mutmaßlich unbeabsichtigten Auswirkungen des Kommissionsvorschlags.

Die Annahme, dass die ePrivacy-Verordnung in der jetzigen Form negative Auswirkungen auf die europäische Wirtschaft hätte, basiert auf zwei Hauptargumenten: Erstens geht der Entwurf der ePrivacy-Verordnung über die Regeln der DSGVO hinaus und legt Unternehmen zusätzliche Hürden für die Verarbeitung personenbezogener Daten in den Weg. Zweitens ist der Anwendungsbereich im Entwurf der ePrivacy-Verordnung so weit gefasst, dass nahezu alle europäischen Unternehmen davon betroffen wären.

Die ePrivacy-Verordnung droht deshalb die digitale Wertschöpfung in ganz Europa auszubremsen. Gleichzeitig würde der aktuelle Entwurf der ePrivacy-Verordnung zu einer weiteren Stärkung der dominanten Internetplattformen führen. Sie können in ihren großen digitalen Ökosystemen zahlreiche digitale Dienstleistungen anbieten und notwendige Nutzereinwilligungen kundenfreundlich bündeln. So könnte die geplante ePrivacy-Verordnung eine weitere Konzentration personenbezogener Daten in den Händen einer kleinen Zahl marktbeherrschender Unternehmen verursachen und letztlich – und paradoxerweise – den Datenschutz in Europa schwächen. Dies widerspräche dem erklärten Ziel der Europäischen Kommission, auf Grundlage eines digitalen Binnenmarkts und fairer Wettbewerbsbedingungen digitale Innovationen zu fördern und Europa zur führenden Region in der weltweiten Internetwirtschaft zu machen.

Damit die europäische Wirtschaft nicht ins digitale Hintertreffen gerät, muss die geplante ePrivacy-Verordnung daher einschließlich ihrer teils unbeabsichtigten negativen Auswirkungen einer gründlichen Prüfung unterzogen werden. Anstatt einer falsch verstandenen Datensparsamkeit sollten die europäischen Datenschutzregeln dem Zielbild der Datensouveränität folgen. Die Bürger sollen eine informierte Entscheidung darüber treffen können, welche Dienste und Funktionen sie nutzen möchten und welcher Art der Datenverarbeitung sie deshalb zustimmen. Diese Sichtweise vermeidet den Dualismus zwischen den Interessen der Nutzer auf der einen Seite und den Interessen der Unternehmen auf der anderen Seite. Stattdessen trägt sie der Tatsache Rechnung, dass datengetriebene Produkte einen hohen Kundennutzen generieren und die Datenverarbeitung der Unternehmen deshalb auch im Sinne der Nutzer ist.

2 WAS AUF DEM SPIEL STEHT:

Daten als Grundlage einer zukunftsfähigen Wirtschaft

Daten kommt im Zuge der Digitalisierung eine zentrale Rolle in allen Gesellschaftsbereichen und Wirtschaftssektoren zu. Die Bedeutung von Daten für das Funktionieren moderner Gesellschaften wird häufig mit der Rolle des Öls im 20. Jahrhundert verglichen. Denn zum einen sind Daten genauso wie Öl aus zahlreichen Produkten nicht mehr wegzudenken. Zum anderen benötigen die Unternehmen Daten, um ihr Produkt zum Kunden zu bringen. Es ist mittlerweile einfacher, ein Produkt ohne die Verwendung fossiler Treibstoffe zu liefern als ohne die Verwendung von Daten. Digitale Geschäftsmodelle basieren auf der Verknüpfung ausgewählter Datenpunkte und können so zusätzlichen Kundennutzen generieren. Die Geschwindigkeit und das Ausmaß der digitalen Transformation der Wirtschaft zeigt ein Blick auf die Sektoren, in denen die zehn wertvollsten Unternehmen der Welt aktiv sind. →A

Im Jahr 2006 entfielen 64% des Börsenwerts der zehn wertvollsten Unternehmen weltweit auf Industrie- oder Rohstoff-Unternehmen.[3] Mit Microsoft war nur ein Technologieunternehmen unter den zehn wertvollsten Unternehmen der Welt vertreten. Dieses Verhältnis hat sich zehn Jahre später fast umgekehrt: Nur noch ein Viertel der Marktkapitalisierung der weltweit zehn wertvollsten Unternehmen entfällt auf die Industrie[4] – 59% hingegen auf Technologieunternehmen.[5]

Der Blick auf die Spitze darf nicht darüber hinwegtäuschen, dass Daten zu einem zentralen Produktionsfaktor beinahe aller Unternehmen werden. Sie müssen ihre Kunden über eine digitale Schnittstelle erreichen und Lösungen anbieten, die konsequent vom Kunden her gedacht sind. Ansonsten drohen die großen Internetplattformen mit ihren digitalen Ökosystemen die Kundenschnittstelle zu besetzen und herkömmliche Geschäftsmodelle obsolet zu machen. Als Musterbeispiel für diese Vertikalisierung gilt das Vordringen von Alphabet (Google) in unterschiedlichste digitale und industrielle Sektoren (Betriebssystem, Browser, Messaging, Logistik, Smart Metering und mehr).

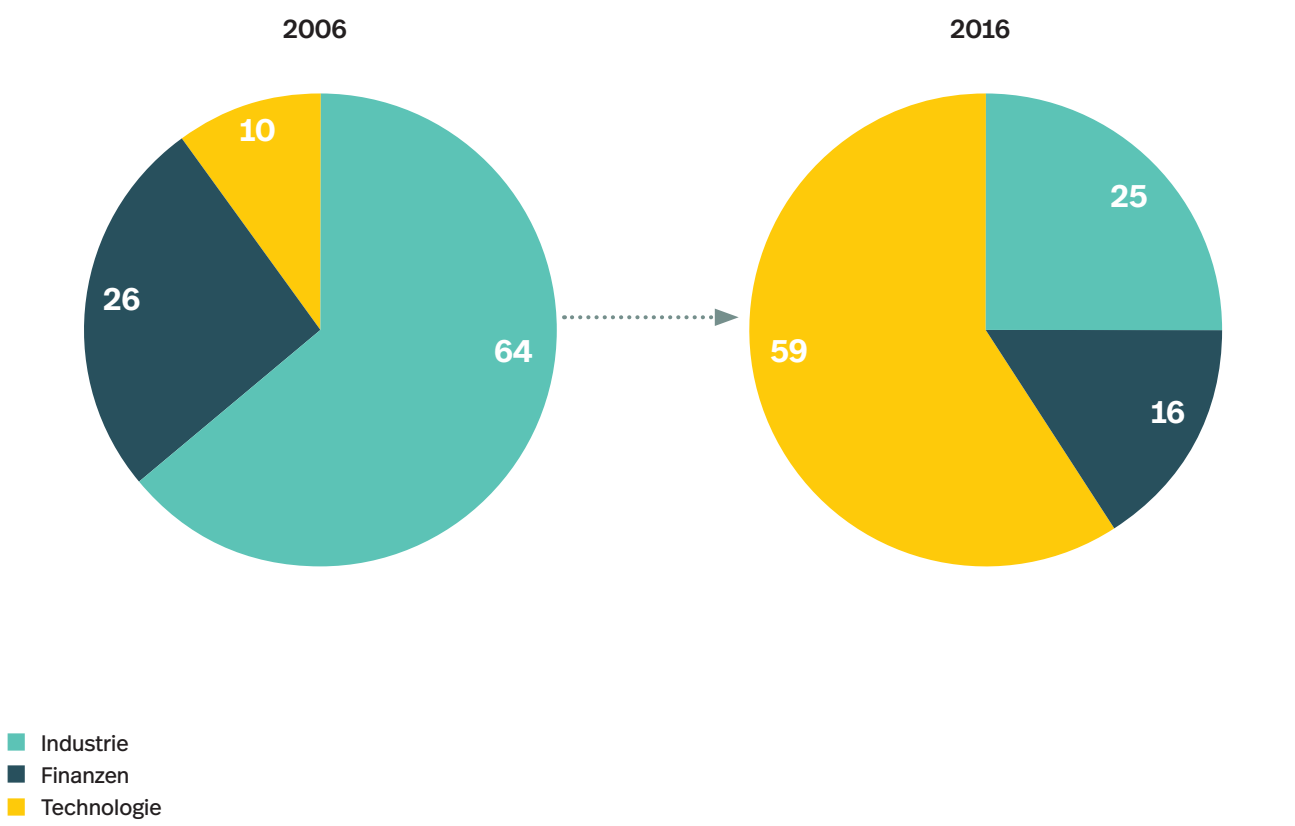
Damit die europäische Wirtschaft angesichts der Vorstöße digitaler Plattformen in etablierte Dienstleistungs- und Industriesektoren wettbewerbsfähig bleiben kann, müssen moderne Datenverarbeitung und innovative Analysen zentrale Bestandteile ihrer Geschäftsmodelle werden. Der Aufbau und die intelligente Nutzung umfassender Datenbanken werden zum entscheidenden Wettbewerbsfaktor. Durch die gezielte Verknüpfung einzelner Datenpunkte können zeitgemäße Geschäftsmodelle und maßgeschneiderte Angebote für Kunden entwickelt werden. Diese personalisierten Angebote treffen auf eine große Nachfrage, weil sie einen hohen Kundennutzen generieren.

Personenbezogene Daten stellen zwar nur einen Teil der von Unternehmen verarbeiteten Daten dar und elektronische Kommunikationsdaten im Sinne der geplanten ePrivacy-Verordnung wiederum sind nur eine Unterkategorie personenbezogener Daten. Allerdings nehmen elektronische Kommunikationsdaten eine zentrale

3 ExxonMobil, General Electric, Gazprom, BP, Royal Dutch Shell, Toyota
4 ExxonMobil, Johnson & Johnson, General Electric
5 Apple, Alphabet (Google), Microsoft, Facebook, Amazon

A Neue Welt: Innerhalb von zehn Jahren hat sich der Hauptanteil des Börsenwerts der weltweit zehn wertvollsten Unternehmen von der Industrie- zur Technologiebranche verschoben

Jahresdurchschnitte [%]



Quelle: Bloomberg; Roland Berger

Stellung im Rahmen datengetriebener Geschäftsmodelle ein. Diese ist vergleichbar mit der Lenkung eines Fahrzeugs: Sie ist nur eines von vielen Elementen eines Fahrzeugs, ist aber für eine sinnvolle und zielgerichtete Fortbewegung unverzichtbar. Deshalb sind die europäischen Unternehmen auf einen verlässlichen gesetzlichen Rahmen angewiesen, der es ihnen ermöglicht, elektronische Kommunikationsdaten so zu nutzen, wie es unsere digitale Welt heute erfordert. Wenn der Gesetzgeber die Hürden für die Verarbeitung dieser Daten zu hoch ansetzt, verliert die Wirtschaft Zugang zum wichtigsten Rohstoff der digitalen Welt – zum Schaden der Unternehmen, Arbeitnehmer und Verbraucher.

Die europäische Wirtschaft droht den Zugang zum wichtigsten Rohstoff der digitalen Welt zu verlieren.

Was auf dem Spiel steht, lässt sich anhand einer von der Europäischen Kommission in Auftrag gegebenen Studie[6] erkennen. Die im Februar 2017 veröffentlichte Analyse untersucht unter anderem, wie sich die europäische Datenwirtschaft bis 2020 entwickelt. Im Mittelpunkt der Analyse steht der makroökonomische Effekt, den der Markt für datenbezogene Dienstleistungen und Produkte auf die Gesamtwirtschaft hat. Dabei werden direkte, indirekte und sekundäre Effekte berücksichtigt.[7] Für das Jahr 2016 schätzt die Studie so den Wert der europäischen Datenwirtschaft auf 300 Milliarden Euro – das entspricht etwa 2% der gesamten europäischen Wirtschaftsleistung (BIP). Sollten sich die Rahmenbedingungen für den europäischen Datenmarkt verbessern, könnte der Wert der gesamten europäischen Datenwirtschaft bis 2020 auf 739 Milliarden Euro oder fast 5% des BIP[8] steigen. Das entspräche einer jährlichen Steigerung um 25%. Ob die europäische Wirtschaft dieses Wachstumspotenzial realisieren kann, hängt auch von der konkreten Ausgestaltung der geplanten ePrivacy-Verordnung ab.

6 European Data Market – Final Report, Februar 2017. Die Studie wurde von IDC und Open Evidence im Auftrag der Europäischen Kommission, Generaldirektion Kommunikationsnetze, Inhalte und Technologien (DG CONNECT), erstellt.

7 Direkte Effekte resultieren aus den Umsätzen mit datenbezogenen Dienstleistungen und Produkten. Indirekte Effekte umfassen die zusätzlichen Umsätze der Zuliefer- und Anwenderindustrien. Die Vorteile eines auf Grundlage von Daten optimierten Produktionsprozesses wären dementsprechend ein indirekter Effekt des Datenmarkts auf die Gesamtwirtschaft. Sekundäre Effekte schließlich berücksichtigen den Konsum, der aus den zusätzlichen Gehältern der Angestellten des Datenmarkts und der direkten Zulieferindustrie erwächst.

8 Für die Schätzung des Anteils wurde die Prognose des BIP (real, Preise und Wechselkurse von 2010) der EU im Jahr 2020 von Oxford Economics herangezogen.

3
DIGITALER HÜRDENLAUF:
Die wirtschaftlichen Auswirkungen der geplanten ePrivacy-Verordnung

Die geplante ePrivacy-Verordnung ist als Spezialgesetzgebung (lex specialis) zur DSGVO angelegt. Das heißt, dass die ePrivacy-Verordnung die DSGVO hinsichtlich elektronischer Kommunikationsdaten präzisieren und ergänzen soll, sofern diese als personenbezogene Daten einzustufen sind.

Im Gegensatz zur bislang gültigen Datenschutzrichtlinie für elektronische Kommunikation aus dem Jahr 2002 soll die neue Regelung als Verordnung umgesetzt werden, die nach ihrem Inkrafttreten unmittelbar in allen EU-Mitgliedsländern gilt. Dies ist ein konsequenter und sinnvoller Schritt, da die Umsetzung als Verordnung einheitliche Regeln für alle Konsumenten und Unternehmen schaffen würde. Auch die geplante Einführung des Marktortprinzips analog zur Regelung der DSGVO – also die Geltung der Verordnung für alle Endnutzer in der EU, unabhängig vom Standort oder Sitz des Datenverarbeiters – ist ein wichtiger Schritt zur Schaffung gleicher Wettbewerbsbedingungen für europäische und nichteuropäische Unternehmen.

Anders als die Vorgänger-Richtlinie soll die ePrivacy-Verordnung auch für sogenannte *Over-the-Top*-Kommunikationsdienste („OTT-Dienste“) gelten. Dabei handelt es sich um Internetdienste wie WhatsApp, Facebook Messenger oder Skype, die elektronische Kommunikationsdienste als Online-Anwendung anbieten. Künftig soll für diese OTT-Dienste der gleiche Rechtsrahmen wie für klassische Telekommunikationsanbieter gelten. Damit würde die ePrivacy-Verordnung sowohl den modernen technischen Rahmenbedingungen als auch dem geänderten Verhalten der Nutzer gerecht werden. Das gilt auch für die neuen Möglichkeiten datenbasierter Wertschöpfung, die Telekommunikationsanbieter nach expliziter Zustimmung der Endnutzer erhalten können. →B

Neben diesen positiven Aspekten enthält der Entwurf der ePrivacy-Verordnung jedoch auch zahlreiche Elemente, die sich negativ auf den europäischen Digitalstandort auswirken würden. So soll die ePrivacy-Verordnung zeitlich mit der DSGVO am 25. Mai 2018 in Kraft treten. Im Gegensatz zur DSGVO ist die verbindliche Fassung der ePrivacy-Verordnung jedoch noch gar nicht bekannt. Aufgrund des komplexen Gesetzgebungsvorgangs wird diese erst kurz vor Inkrafttreten der Verordnung vorliegen. Das stellt die europäische Wirtschaft vor kaum lösbare Probleme, weil sie sich unmöglich auf ein Regelwerk vorbereiten kann, dessen Inhalt noch gar nicht feststeht.

Überdies umfasst der Anwendungsbereich der geplanten ePrivacy-Verordnung nicht nur elektronische Kommunikationsdienste, sondern fast alle digitalen Dienstleistungen sowie zahlreiche Anwendungen im Bereich des Internet of Things. Dies ist deshalb problematisch, weil der Entwurf der ePrivacy-Verordnung noch höhere Barrieren für die Datenverarbeitung vorsieht als die DSGVO.

3.1 Breiter Anwendungsbereich

In Hinsicht auf den Anwendungsbereich erinnert der Kommissionsvorschlag der ePrivacy-Verordnung an ein Puzzle. Auf den ersten Blick handelt es sich bei der geplanten Verordnung um eine Spezialgesetzgebung,

B Neue Regeln: Die wichtigsten Neuerungen der geplanten ePrivacy-Verordnung gegenüber der bislang gültigen Datenschutzrichtlinie für elektronische Kommunikation

Verordnung statt Richtlinie
Die Umsetzung der geplanten Regelung in Form einer Verordnung statt einer Richtline soll einheitliche Regeln in der ganzen EU schaffen.

Marktortprinzip
Die geplante Verordnung soll für alle Endnutzer in der EU gelten, unabhängig vom Standort oder Sitz des Datenverarbeiters.

Einwilligung für Datenverarbeitung
Die Verarbeitung von Kommunikationsdaten soll zukünftig in fast allen Fällen eine explizite Einwilligung der Endnutzer erfordern, auch bei Pseudonymisierung der Nutzerdaten.

Zentrale Privatsphäre-Einstellung
Nutzer sollen Einstellungen zur Privatsphäre wie die Einwilligung zur Datenverarbeitung zentral vornehmen können, zum Beispiel im Browser.

OTT-Dienste
Die Datenschutzregeln sollen auch für Over-the-Top-Dienste wie WhatsApp gelten, um sie klassischen Telekommunikationsanbietern gleichzustellen.

M2M-Kommunikation
Die geplante Verordnung soll auch für die Kommunikation zwischen Maschinen gelten.

Quelle: Roland Berger

die elektronische Kommunikationsdienste betrifft. Je näher man sich jedoch mit dem Text befasst, desto mehr Anwendungsbereiche der Verordnung tauchen auf. Setzt man diese einzelnen Bereiche richtig zusammen, ergibt sich ein überraschendes Bild: Der aktuelle Entwurf der ePrivacy-Verordnung regelt einen so breiten Anwendungsbereich, dass kaum ein digitales Geschäftsmodell denkbar ist, das nicht von der Verordnung betroffen wäre.

So fände die ePrivacy-Verordnung nicht nur auf Apps der OTT-Dienste, sondern wegen ihrer zugrunde liegenden Funktionalität auf alle Apps Anwendung. Alle App-Entwickler, die ihre Produkte auf dem europäischen Markt anbieten möchten, müssten also die Regeln der ePrivacy-Verordnung einhalten. Die starke Zunahme innovativer Apps in den letzten Jahren wurde von der Möglichkeit getragen, das Produkt mithilfe persönlicher Nutzungsdaten analysieren, verbessern, bewerben und finanzieren zu können. →CASE 1 Deshalb würde die ePrivacy-Verordnung mit der gesamten europäischen App-Economy das wichtigste Wachstumsfeld der Digitalwirtschaft betreffen. Zusätzlich wären viele digitale Angebote von der Anwendung der geplanten Verordnung auf Kommunikationsdienste, die lediglich eine untergeordnete Nebenfunktion eines Dienstes darstellen, berührt. Dabei handelt es sich beispielsweise um Chat-Funktionen, die der Vereinfachung spezifischer Transaktionen auf digitalen Plattformen dienen. →CASE 2

Überdies führt der Einschluss sogenannter M2M-Kommunikation in den Anwendungsbereich der geplanten ePrivacy-Verordnung dazu, dass zahlreiche Anwendungen im Bereich des Internet of Things (IoT) betroffen wären. Neben schon bekannten Anwendungen wie vernetztem Fahren oder Smart Homes würde die ePrivacy-Verordnung auch für gänzlich neue, noch nicht entwickelte IoT-Technologien gelten. →CASE 3

Schließlich würde die geplante ePrivacy-Verordnung zahlreiche europäische Unternehmen betreffen, die gerade digitale Geschäftsmodelle entwickeln. Aufgrund der zentralen Stellung, die Daten insgesamt und personenbezogene Kommunikationsdaten im Besonderen für digitale Innovationen und neue Geschäftsmodelle innehaben, droht die geplante ePrivacy-Verordnung so zu einem Bremsklotz für die Digitalisierung in Europa zu werden.

3.2 Neue Hürden für die Datenverarbeitung

Neben dem sehr breiten Anwendungsbereich der ePrivacy-Verordnung sind vor allem die darin vorgesehenen Hürden für die Verarbeitung personenbezogener Daten kritisch zu hinterfragen. Denn zum einen sind manche Bestimmungen im Entwurf der ePrivacy-Verordnung nicht konsistent mit den Regeln der DSGVO. Dies bedeutet eine erhebliche Rechtsunsicherheit für alle Unternehmen, die momentan in die Umsetzung der in der DSGVO festgelegten Normen investieren. Und zum anderen sieht der Entwurf der ePrivacy-Verordnung höhere Hürden für die Verarbeitung personenbezogener Daten vor als die DSGVO. Überdies lässt der Berichtsentwurf

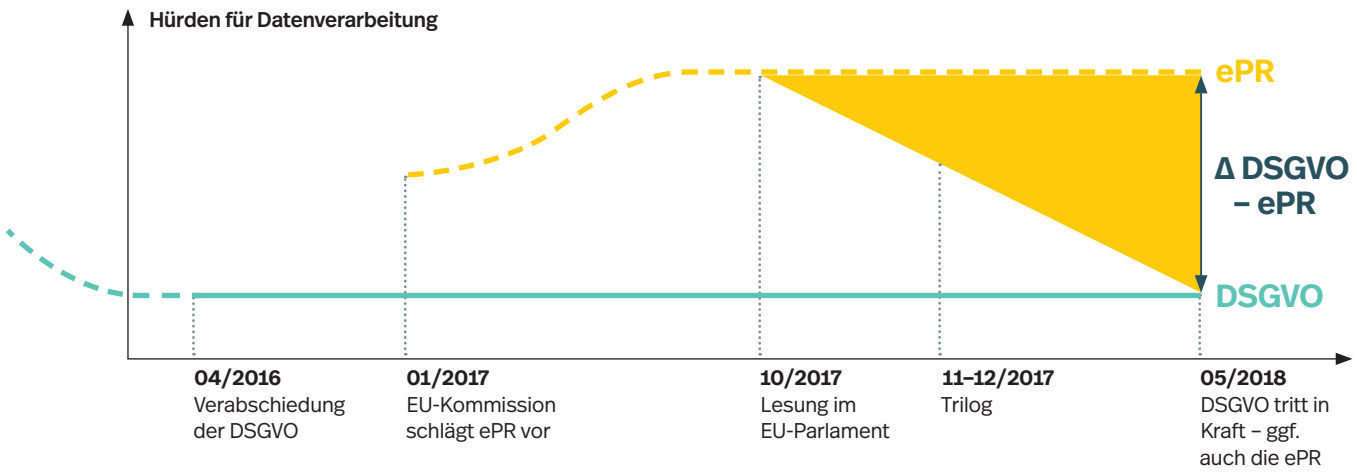
des Parlamentsausschusses befürchten, dass die Hürden für die Datenverarbeitung im Rahmen des parlamentarischen Prozesses noch erhöht werden könnten. →C

So ist im Entwurf der ePrivacy-Verordnung im Gegensatz zur DSGVO[9] keine Datenverarbeitung auf Grundlage eines berechtigten Interesses des Datenverarbeiters oder Dritter vorgesehen. Das bedeutet, dass Kommunikationsdaten zum Beispiel nicht ohne Einwilligung des Nutzers zur Verhinderung des Missbrauchs des Dienstes eingesetzt werden dürfen. Je nach Auslegung der geplanten ePrivacy-Verordnung könnte dies sogar dazu führen, dass für den Einsatz von Spamfiltern die explizite Einwilligung des Absenders notwendig ist.

Im Gegensatz zur DSGVO[10] sieht die ePrivacy-Verordnung keine Berücksichtigung technischer Datenschutzmaßnahmen, insbesondere durch die Verarbeitung pseudonymisierter Daten oder Verschlüsselungen, vor. Mithilfe der Pseudonymisierung wird die Identität der

C Digitale Hürden: Die geplante ePrivacy-Verordnung würde die Hürden für die Verarbeitung personenbezogener Daten gegenüber der Datenschutzgrundverordnung deutlich erhöhen

Zeitplan und Datenschutzhürden der geplanten ePrivacy-Verordnung



Quelle: Roland Berger

9 Siehe Verordnung (EU) 2016/679 Art. 6 (1) lit. f
10 Siehe Verordnung (EU) 2016/679 Art. 6 (4) lit. e

CASE 1

Wie Cookies digitale Angebote verbessern

Cookies sind Identifizierungscodes – meist in Form einer Textdatei –, die Websites und Apps auf dem Endgerät der Nutzer speichern. Wenn der Nutzer die entsprechende Website erneut aufsucht, wird dieser Identifizierungscode an den Web Server der Seite geschickt. Auf diesem Wege können die Anbieter digitaler Dienste verschiedene Informationen erfassen. Dazu gehören zum Beispiel Meldungen über Störungen oder Probleme bei der Nutzung des Dienstes. Auch Formulareinträge können so hinterlegt und dem Nutzer bei Bedarf vorgeschlagen werden, wenn er das Formularfeld erneut nutzt. Diese Technologie wird auch eingesetzt, um Dienste zu personalisieren. Davon profitieren die Nutzer, indem sie beispielsweise zu ihrem Aufenthaltsort passende Angebote wie lokale Wetterdaten, Lokalnachrichten oder zielgerichtete Werbung angezeigt bekommen. Mithilfe von Cookies kann auch die Effektivität einer Werbekampagne überprüft und die Relevanz der Anzeigen gesteigert werden. So kann sich ein digitaler Dienst mit einer geringeren Zahl an Werbeeinblendungen finanzieren. Insgesamt sind Cookies zentral sowohl für die Funktionalität als auch für die Finanzierung digitaler Angebote.

Die Artikel 8 bis 10 der geplanten ePrivacy-Verordnung zielen darauf ab, das Platzieren von Cookies in den meisten Fällen an die explizite Einwilligung des Nutzers zu knüpfen (Erwägungsgründe 20 bis 24 des Vorschlags der Kommission). Andere Erlaubnisgründe, wie etwa die Abwägung berechtigter Interessen und technische Maßnahmen wie Pseudonymisierung, spielen dabei bisher keine Rolle. Der Entwurf misst zudem der zentralen Einstellung in der Zugangssoftware zum Internet – also dem Browser – eine wesentliche Rolle dabei zu. Bei Inbetriebnahme der Software müsste der Kunde eine allgemeine Entscheidung über den Umgang mit Cookies treffen. Man kann davon ausgehen, dass selbst Nutzer, die im konkreten Fall das auf Cookies basierende Angebot schätzen und nutzen möchten, bei einer allgemeinen Entscheidung keine Cookies zulassen würden. Die Konsequenzen dieser Entscheidung könnten vielen Nutzern nicht klar sein, da die spezifischen Vorteile von Cookies vielfältig und technischer Natur sind. Unklar bleibt dabei jedoch, wie einzelne Anbieter trotz der zentralen Browser-Einstellung eine Einwilligung zum Setzen von Cookies einholen können, wenn der vom Kunden gewünschte Dienst solche erfordert.

Es steht deshalb zu befürchten, dass zahlreiche Dienste keine Cookies mehr setzen dürften. Dies würde zum einen die Qualität des Kundenangebots mindern, weil Cookies eine wichtige Funktion bei der Qualitätssicherung des Angebots innehaben. Zum anderen würde die geplante ePrivacy-Verordnung der Finanzierung zahlreicher kostenloser, von Kunden gerne in Anspruch genommener Dienstleistungen im Internet die Grundlage entziehen. Dies trifft unter anderem die Anbieter von Nachrichtenseiten, die zur Finanzierung ihres Angebots auf Cookies angewiesen sind. Auch kleine Unternehmen können mithilfe von Cookies günstig zielgerichtete Werbung im Internet platzieren. Die ePrivacy-Verordnung würde deshalb vor allem diese kleinen Unternehmen treffen und damit die Vielfalt digitaler Angebote untergraben.

CASE 2

Warum digitale Produkte auf Kommunikationsdienste als Nebenfunktion angewiesen sind

Laut Artikel 4(2) im Entwurf der ePrivacy-Verordnung sind auch solche Dienste als interpersoneller Kommunikationsdienst einzustufen, „die eine interpersonelle und interaktive Kommunikation lediglich als untrennbar mit einem anderen Dienst verbundene untergeordnete Nebenfunktion ermöglichen“ (siehe auch Erwägungsgrund 11 im Entwurf der ePrivacy-Verordnung). Das bedeutet, dass auch die interpersonelle Kommunikation in Form einer Chatfunktion innerhalb einer Spiele-App oder einer E-Commerce-Plattform in den Anwendungsbereich der geplanten ePrivacy-Verordnung fallen würde.

Zahlreiche digitale Dienste verwenden solche Chat-Funktionen, um ihr Angebot nutzerfreundlicher zu gestalten. So können Nutzer einer E-Commerce-Seite solche Funktionen beispielsweise verwenden, um bei Fragen oder Beschwerden direkt mit dem Verkäufer in Kontakt treten zu können. Damit ermöglicht die Kommunikationsfunktion eine unkomplizierte und meist schnelle Abstimmung zwischen Kunde und Verkäufer, ohne dass eine Einmischung des Diensteanbieters nötig ist. Auch Anbieter von Plattformen, auf denen Mitfahrgelegenheiten angeboten und gesucht werden können, nutzen in der Regel eine solche Chat-Funktion. Darüber können Fahrer und Mitfahrer vor der Fahrt Kontakt zueinander aufnehmen und Details wie zum Beispiel den genauen Abfahrtsort besprechen. Bei Online-Spielen erleichtert die Kommunikationsfunktion das Zusammenarbeiten mehrerer Spieler in einem Team.

In allen Fällen hat der Diensteanbieter ein berechtigtes Interesse daran, die Kommunikation in dem von ihm angebotenen Kanal nach unangemessenen Inhalten zu filtern. Dazu gehören beispielsweise Beleidigungen oder sexuelle Belästigung. Auch die missbräuchliche Nutzung des Dienstes und illegale Inhalte muss der Betreiber filtern können, um seinen Kunden eine sichere und vertrauensvolle Nutzung des Angebots garantieren zu können. Sollte die ePrivacy-Verordnung wie geplant in Kraft treten, müssten die Diensteanbieter auf entsprechende Filter verzichten. Der Leidtragende wäre damit der Kunde, der auf einen nützlichen und geschützten Kommunikationskanal verzichten müsste.

CASE 3

Wie Smart Homes die Lebensqualität verbessern

Von der Anwendung der ePrivacy-Verordnung auf M2M-Kommunikation wären nicht nur Anwendungen im Bereich der Mobilität, sondern auch des Wohnens

betroffen. Unter dem Stichwort Smart Home wird die Vernetzung verschiedener Geräte im Haushalt zusammengefasst, um beispielsweise Energie zu sparen, die Sicherheit zu erhöhen, die Funktionen im Haus an einzelne Bewohner anzupassen sowie das Leben angenehmer und bequemer zu gestalten.

So kann zum Beispiel die Heizung hochgefahren werden, wenn das Smartphone eines Bewohners die Information übermittelt, dass der Bewohner bald zu Hause sein wird. Mithilfe von Sensoren und Kameras kann die Sicherheit der eigenen vier Wände erhöht werden. Und ein intelligenter Kühlschrank kann beispielsweise erkennen, ob noch genug Milch vorrätig ist, und eine entsprechende Lieferung beim Lebensmittelhändler veranlassen.

Allen diesen Anwendungen ist gemeinsam, dass sie auf personenbezogenen Kommunikationsdaten basieren. Ihren Zweck erfüllen diese Anwendungen jedoch nur dann, wenn sie ohne Zutun des Nutzers tätig werden. Der vernetzte Kühlschrank soll die Milch bestellen, ohne dass der Nutzer die Einwilligung geben muss, dass diese Information an den Lebensmittelhändler übermittelt werden darf. Ebenso verhält es sich mit der Heizung: Der Nutzer möchte eine angenehme Raumtemperatur vorfinden, wenn er nach Hause kommt. Wenn er der Übermittlung seiner Ankunftszeit jedes Mal erst explizit zustimmen muss, mindert das den Nutzen der Anwendung.

Smart Homes benötigen auch personenbezogene Kommunikationsdaten, um Kundennutzen zu generieren.

CASE 4

M2M-Kommunikation als Basis für die Mobilität der Zukunft

Erwägungsgrund 12 im Entwurf der ePrivacy-Verordnung hält fest, dass auch die Kommunikation zwischen Maschinen in den Anwendungsbereich der Verordnung fallen soll. Diese sogenannte M2M-Kommunikation stellt die Basis für IoT-Anwendungen dar und ist das wichtigste Zukunftsfeld industrieller Wertschöpfung.

Ein Beispiel für die Bedeutung von M2M-Kommunikation ist das bereits jetzt verbreitete vernetzte Fahren. Schon heute senden Millionen von Fahrzeugen Informationen zu Verkehr, Straßenverhältnissen und Wetter. So kann der Fahrer eines vernetzten Fahrzeugs beispielsweise rechtzeitig auf ein Stauende hinter einer Kurve oder eine Nebelbank hingewiesen werden. Dazu ist es notwendig, dass möglichst viele Fahrzeugführer der Übermittlung und anonymisierten Auswertung ihrer Fahrzeugdaten zustimmen. Wenn einzelne Fahrzeuge die Übertragung dieser sicherheitsrelevanten Informationen nicht vornehmen, wäre dies ein Rückschritt für die Verkehrssicherheit, ohne dass der Datenschutz verbessert würde.

Noch größer ist die Bedeutung von M2M-Kommunikation beim autonomen Fahren. Autonome Fahrzeuge können nur dann sicher navigieren, wenn sie

regelmäßige Updates mit aktuellen Navigations- und Verkehrsinformationen erhalten. Der Hersteller muss deshalb die Möglichkeit haben, ohne explizite Einwilligung des Nutzers Daten auf dem „Endgerät“ (dem Auto) zu speichern. Nur wenn die Informationen aller autonomen Fahrzeuge aktuell sind, kann autonomes Fahren sicher und zuverlässig ermöglicht werden.

CASE 5

Vom Zugangstor zum Gatekeeper

Internet-Browser sind neben Apps auf Smartphones weiterhin die zentrale Benutzeroberfläche, mit der Internetnutzer die Seiten von E-Commerce-, Informations- oder Unterhaltungsangeboten im Internet nutzen. Um dem Nutzer ein möglichst attraktives Nutzungserlebnis (insbesondere durch Personalisierung und Lokalisierung) bieten zu können, sind diese Anbieter – anders als reichweitenstarke Social-Media-Plattformen – in der Regel auf das Setzen von Cookies angewiesen.

Nach dem Vorschlag der ePrivacy-Verordnung würde Internet-Browsern künftig eine noch größere Rolle bei der Ausgestaltung zukommen, welche Internetangebote Informationen auf das Gerät des Nutzers (zum Beispiel Cookies) schreiben dürfen und welche nicht. Die entsprechenden Entscheidungen sollen vom Nutzer zentral in den Einstellungen des Browsers getroffen werden. Bei der künftigen Nutzung von Internetangeboten im Browser würde daher nicht allein die entsprechende Einwilligung per Klick auf der Seite des Anbieters ausreichen. Der Browser würde weiterhin durch die entgegenstehenden zentralen Einstellungen das Schreiben von Cookies verhindern. Der Nutzer müsste also im (regelmäßig komplexen) Einstellungsmenü des Browsers die entsprechenden Ausnahmen zusätzlich bestätigen, was erfahrungsgemäß die wenigsten Nutzer auf sich nehmen. Eine technische Schnittstelle, die Einzelausnahmen direkt und für den Nutzer bequem in die zentralen Einstellungen überträgt, ist nach dem Verordnungsvorschlag nicht vorgesehen. Die Anbieter wären daher vom Wohlwollen der Browser-Hersteller abhängig und der Ausgestaltung der Schnittstellendefinitionen des Browser-Herstellers ausgeliefert, so dieser überhaupt welche vorsieht.

Dadurch würde innerhalb der Internetanbieter die starke Position der Social-Media-Dienste weiter steigen, die auf eine Identifikation der Nutzer durch Cookies verzichten können, weil diese eingeloggt sind. Außerdem birgt die damit verbundene Gatekeeper-Rolle der Browser-Hersteller, die einen Markt mit nur wenigen starken Teilnehmern bilden und ihrerseits oftmals Teil vertikal integrierter Ökosysteme sind, eine zusätzliche Missbrauchsgefahr, die neue wettbewerbliche Probleme heraufbeschwört.

Die Browser-Hersteller drohen im Zuge der geplanten ePrivacy-Verordnung zu mächtigen Gatekeepern der digitalen Welt zu werden.

Nutzer von ihren Daten getrennt, um ein hohes Datenschutzniveau zu gewährleisten und gleichzeitig die Verarbeitung der Daten zu ermöglichen. Die DSGVO trägt dem Umstand Rechnung, dass pseudonymisierte Daten eine geringere Schutzbedürftigkeit haben als personenbezogene Daten und ermöglicht deshalb unter bestimmten Umständen die Datenverarbeitung ohne explizite Einwilligung. Die ePrivacy-Verordnung hingegen nimmt diese Unterscheidung nicht vor. Vielmehr fokussiert sich der Entwurf der ePrivacy-Verordnung allein auf die explizite Einwilligung des Nutzers als Grundlage für die Verarbeitung personenbezogener Daten und nimmt damit eine strengere Wertung vor als die DSGVO.

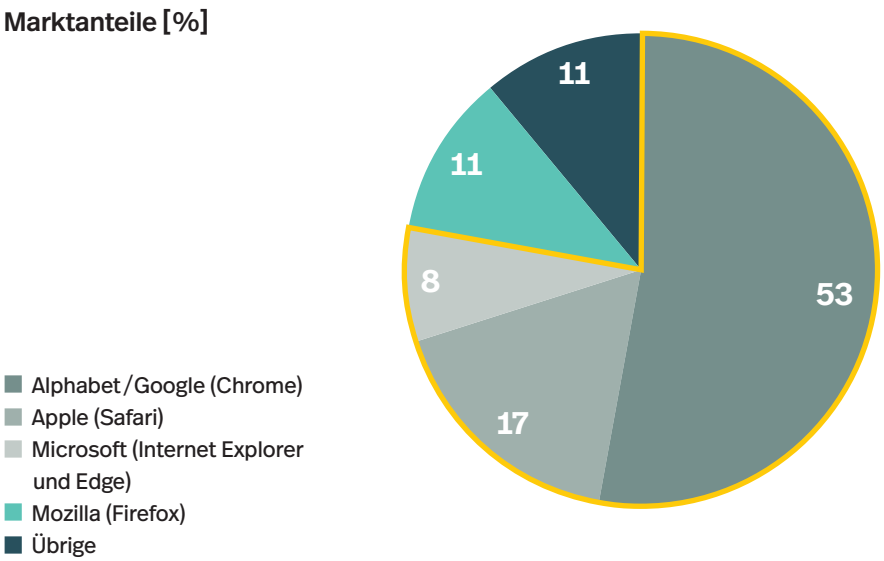
Die Überwindung der im Vergleich zur DSGVO noch höheren Barrieren zur Datenverarbeitung wird großen Internetplattformen leichter fallen als kleinen Unternehmen. Der Kommissionsvorschlag der ePrivacy-Verordnung wird vor allem singuläre Online-Dienste gegenüber den großen Internetplattformen benachteiligen. Plattformen wie Alphabet (Google), Apple, Facebook, Amazon oder Microsoft[11] haben digitale Ökosysteme geschaffen, in denen Kunden eine Vielzahl vertikaler Dienstleistungen wie zum Beispiel Browser, E-Mail, Messaging und Cloudspeicher aus einer Hand erhalten. Ihre dominante Marktstellung in Verbindung mit einer breiten vertikalen Integration ermöglicht diesen digitalen Plattformen die umfassende Verknüpfung personenbezogener Kundendaten und die Erstellung detaillierter Nutzerprofile. Strenge Einwilligungsvorbehalte für das Verarbeiten personenbezogener Daten haben auf die Geschäftsmodelle der großen Internetplattformen nur geringen Einfluss, da sie ihren Nutzern ein bequemes Universal-Opt-in für die gesamte Palette ihrer digitalen Dienstleistungen bieten können. In Kombination mit den aufgrund ihrer starken Vertikalisierung generierten Lock-in-Effekten werden digitale Plattformen sehr einfach an die Einwilligung zum Verarbeiten personenbezogener Daten gelangen. Somit würde einer Konzentration der Nutzerdaten in den Händen weniger dominanter Internetkonzerne Vorschub geleistet.

Weiter verschärft wird die Fokussierung auf die explizite Einwilligung als zentrale Bedingung für die Verarbeitung personenbezogener Daten durch die Schaffung neuer Gatekeeper. So sollen die Nutzer künftig über eine zentrale Einstellung in der Zugangssoftware zum Internet festlegen, ob sie der Verarbeitung ihrer personenbezogenen Daten zustimmen. Dabei sind Ausnahmen für einzelne Dienste vorgesehen – die Nutzer könnten also spezifische Dienste festlegen, denen sie die Einwilligung für die Datenverarbeitung erteilen. Wie digitale Dienste diese Ausnahmen erlangen und wie diese mit gegebenenfalls abweichenden Zentraleinstellungen in Einklang gebracht werden, ist noch unklar. Insgesamt würden die Browser zu mächtigen Gatekeepern für digitale Dienste gemacht. →CASE 5 Dies ist vor allem vor dem Hintergrund der Machtverhältnisse unter den Browser-Anbietern bedenklich: Die Browser der großen Internetplattformen besitzen in Europa einen Marktanteil von 78%. →D

11 Auch bei den chinesischen Unternehmen Tencent und Alibaba handelt es sich um Internetplattformen; diese sind bislang nur in geringem Umfang in Europa aktiv, ein Vordringen auf den europäischen Markt ist jedoch nur eine Frage der Zeit.

Die ePrivacy-Verordnung würde wie ein Schraubstock von zwei Seiten Druck auf die europäische Wirtschaft ausüben: →E Aufgrund des sehr breiten Anwendungsbereichs wären die gesamte App-Economy, zahlreiche Anwendungen im Bereich des IoT sowie alle Unternehmen betroffen, die im Zuge der Digitalisierung auf die Verarbeitung von Kommunikationsdaten angewiesen sind. Für sich allein genommen würde der breite Anwendungsbereich der Verordnung nicht zwangsläufig negative Auswirkungen nach sich ziehen. Allerdings sieht der Entwurf der ePrivacy-Verordnung gleichzeitig sehr hohe Barrieren für die Verarbeitung von Nutzerdaten vor. Durch die Fokussierung auf die explizite Einwilligung würden die Regeln der ePrivacy-Verordnung von denen der DSGVO abweichen und eine strengere Wertung vornehmen. Bleiben die zusätzlichen Hürden für die Verarbeitung von Nutzerdaten so bestehen, wie sie im Entwurf der ePrivacy-Verordnung vorgesehen sind, wird die europäische Datenwirtschaft ihr Wachstumspotenzial nicht verwirklichen können. Die Digita-

D Dominanz im Netz: Die Browser der großen Internetplattformen besitzen in Europa einen Marktanteil von 78%



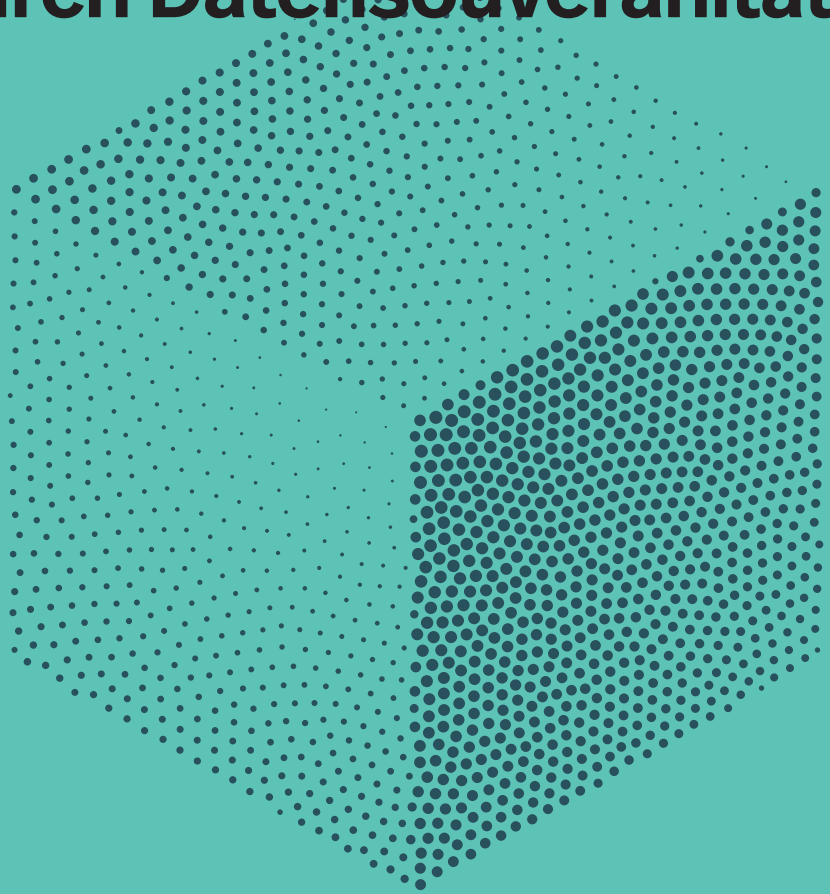
Quelle: Statcounter (Daten vom August 2017); Roland Berger

lisierung schreitet weltweit voran, doch Europa bremst sich selbst aus. Insbesondere die Entwicklung innovativer, datengetriebener Geschäftsmodelle und der Ausbau von IoT-Zukunftsfeldern wie Smart Homes und autonomes Fahren würden von der Verordnung verlangsamt. Zudem könnte die ePrivacy-Verordnung zu einer Machtverschiebung im Internet führen: Wenn die großen Plattformkonzerne ihr digitales Ökosystem zum Einholen von Opt-ins nutzen, werden sie personenbezogene Daten zukünftig einfacher erheben und verarbeiten können als kleinere Anbieter einzelner Online-Dienste. Das heute schon vorhandene Gefälle zwischen dominanten Plattformen und kleineren Internetunternehmen würde sich weiter ausweiten. Insgesamt würde die überzogene Datensparsamkeit der geplanten ePrivacy-Verordnung deshalb nicht nur die Wachstumschancen der europäischen Wirtschaft verringern, sondern aufgrund der Bevorteilung großer Plattformen auch den Datenschutz in Europa langfristig schwächen.

E Wirtschaft im Schraubstock: Die geplante ePrivacy-Verordnung betrifft alle Wirtschaftssektoren und legt Unternehmen hohe Hürden für die Verarbeitung personenbezogener Daten in den Weg

Quelle: Roland Berger

4
WAS JETZT ZU TUN IST:
Wirksamer Datenschutz durch Datensouveränität



In wirtschaftlicher Hinsicht blicken viele Länder Europas auf ein verlorenes Jahrzehnt zurück. Europas Wirtschaft wächst heute jedoch wieder und der Arbeitsmarkt bietet den Bürgern wieder bessere Perspektiven. Damit der wirtschaftliche Aufschwung in Europa weiter an Fahrt gewinnt und die europäische Wirtschaft global wettbewerbsfähig bleibt, müssen wir die richtigen Rahmenbedingungen setzen. Die Digitalisierung bietet das größte Potenzial für höhere Produktivität, bessere Arbeitsplätze und eine gerechtere Gesellschaft. Die Nutzung dieses Potenzials darf nicht durch eine fehlgeleitete Regulierung ausgebremst werden. Die von der Europäischen Kommission vorgeschlagene ePrivacy-Verordnung könnte in der jetzigen Form jedoch genau dies tun.

Die grundlegenden Probleme der geplanten ePrivacy-Verordnung resultieren aus einer überzogenen Datensparsamkeit, die auf eine größtmögliche Einschränkung der Verarbeitung von Kommunikationsdaten abzielt. Dieser Grundsatz schränkt Chancen für Innovationen bewusst ein und untergräbt die Datensouveränität der Bürger. Das Zielbild der ePrivacy-Verordnung sollte nicht die rigide Datensparsamkeit des aktuellen Entwurfs, sondern ein datensouveräner Bürger sein. Zur Stärkung der individuellen Datensouveränität sollte die geplante Verordnung deshalb allen Bürgern einen informierten und selbstbestimmten Umgang mit ihren personenbezogenen Daten ermöglichen. So würde die digitale Mündigkeit der Bürger gestärkt und gleichzeitig eine Grundlage für einen zukunftsfähigen digitalen Binnenmarkt geschaffen.

Die ePrivacy-Verordnung würde zu einer Schwächung des europäischen Wirtschaftsstandorts führen.

Im jetzigen Entwurf würde die Kombination aus dem sehr breiten Anwendungsbereich und den vor allem im Vergleich zur DSGVO noch größeren Hürden für die Verarbeitung personenbezogener Daten zu einer Schwächung des europäischen Wirtschaftsstandorts führen. Zudem würde die vorgeschlagene ePrivacy-Verordnung insbesondere die europäische Datenwirtschaft gegenüber den großen digitalen Ökosystemen der US-amerikanischen Plattformen benachteiligen. Dies könnte zu einer weiteren Marktkonzentration und damit zu einer noch stärkeren Konzentration personenbezogener Daten in den Händen einiger weniger Unternehmen führen. In diesem Fall hätte die ePrivacy-Verordnung den Datenschutz geschwächt anstatt ihn zu stärken.

Um dieses Szenario zu verhindern, sollte die ePrivacy-Verordnung hinsichtlich dreier wesentlicher Punkte angepasst werden:

1. Die ePrivacy-Verordnung sollte die Verarbeitung elektronischer Kommunikationsdaten analog zu den in der DSGVO festgelegten Bedingungen ermöglichen. Dazu gehört die Verarbeitung auf Grundlage eines berechtigten Interesses ebenso wie die Berücksichtigung datenschutzfreundlicher Technologien wie Pseudonymisierung.

2. Überdies sollte die ePrivacy-Verordnung keine neuen Gatekeeper in Form der Zugangssoftware zum Internet schaffen. Es muss sichergestellt werden, dass kein Online-Anbieter durch die zentralen Privatsphäre-Einstellungen noch weiter behindert wird und in noch größere Abhängigkeit zu den dominanten Internetplattformen und den von ihnen betriebenen Browsern gerät.

3. Schließlich sollte auch der ambitionierte Zeitplan der EU-Kommission angepasst und eine Übergangsfrist vorgesehen werden, damit die europäischen Unternehmen ausreichend Zeit für die Umsetzung der geplanten Verordnung haben.

Ein europaweit einheitlicher Rechtsrahmen zum Schutz personenbezogener Daten stellt einen wichtigen Schritt zur Verwirklichung des digitalen Binnenmarkts dar. Gleichzeitig dürfen digitale Innovationen im Rahmen einer falsch verstandenen Datensparsamkeit nicht sehenden Auges verhindert werden. Die Interessen der Nutzer dürfen nicht gegen die Interessen der Unternehmen ausgespielt werden. Stattdessen sollten die Interessen der Konsumenten und der datenverarbeitenden Unternehmen auf Grundlage individueller Datensouveränität in Einklang gebracht werden. Nur dann kann der europäische Internetstandort an Wettbewerbsfähigkeit gewinnen, zu unserem Wohlstand beitragen und weiter Angebote mit hohem Kundennutzen entwickeln.

Die Interessen der Konsumenten und der datenverarbeitenden Unternehmen sollten auf Grundlage individueller Datensouveränität in Einklang gebracht werden.

Impressum

Herausgeber

Internet Economy Foundation (IE.F)
Uhlandstraße 175
10719 Berlin
www.ie.foundation

Prof. Dr. Friedbert Pflüger
Vorsitzender

Roland Berger GmbH
Sederanger 1
80538 München
www.rolandberger.com

Stefan Schaible
CEO Germany & Central Europe

Autoren

Clark Parsons
c.parsons@ie.foundation

Felix Styma
f.styma@ie.foundation

Klaus Fuest
klaus.fuest@rolandberger.com

Dr. David Born
david.born@rolandberger.com

Kontakt

Clark Parsons
Geschäftsführer
Internet Economy Foundation (IE.F)
c.parsons@ie.foundation
+49 30 8877 429-400

Claudia Russo
Pressereferentin
Roland Berger GmbH
claudia.russo@rolandberger.com
+49 89 9230-8190

Bildnachweise

Seite 1: chaluk/iStock **Seite 2:** sanchesnet1/iStock **Seite 6:** amgun/iStock **Seite 10 und 14:** RGAP/iStock
Seite 19–22: Olga Korshunova/iStock **Seite 26:** Samolevsky/iStock **Seite 31**: Ludmila_m/iStock