Stellungnahme

Zum Dokument des Rates der Europäischen Union - Interinstitutional File: 2017/0003 (COD)

06.12.2017

Bitkom vertritt mehr als 2.500 Unternehmen der digitalen Wirtschaft, davon gut 1.700 Direktmitglieder. Sie erzielen mit 700.000 Beschäftigten jährlich Inlands-umsätze von 140 Milliarden Euro und stehen für Exporte von weiteren 50 Milliarden Euro. Zu den Mitgliedern zählen 1.000 Mittelständler, 400 Start-ups und nahezu alle Global Player. Sie bieten Software, IT-Services, Telekommunikations- oder Internetdienste an, stellen Hardware oder Consumer Electronics her, sind im Bereich der digitalen Medien oder der Netzwirtschaft tätig oder in anderer Weise Teil der digitalen Wirtschaft. 78 Prozent der Unternehmen haben ihren Hauptsitz in Deutschland, 8 Prozent kommen aus Europa, 8 Prozent aus den USA und 4 Prozent aus anderen Regionen. Bitkom setzt sich insbesondere für eine innovative Wirtschaftspolitik, eine Modernisierung des Bildungssystems und eine zukunftsorientierte Netzpolitik ein.

Bundesverband
Informationswirtschaft,
Telekommunikation
und Neue Medien e.V.

Susanne Dehmel
Mitglied der Geschäftsleitung
T +49 30 27576-223
s.dehmel@bitkom.org

Rebekka Weiß, LL.M.
Referentin Datenschutz & Verbraucherrecht
T +49 30 27576 161
r.weiss@bitkom.org

Albrechtstraße 10
10117 Berlin

Präsident
Achim Berg

Hauptgeschäftsführer
Dr. Bernhard Rohleder

Zusammenfassung

Mit der Datenschutz-Grundverordnung (DS-GVO) wurden bereits EU-weit einheitliche strenge datenschutzrechtliche Vorschriften für alle Sektoren festgelegt, die ein flächendeckend hohes Datenschutzniveau garantieren. Der Gesetzentwurf der EU-Kommission zur e-Privacy Verordnung und auch der Parlamentsentwurf hierzu drohen jedoch die im langjährigen und mühsamen Prozess gefundene Balance zwischen dem Schutz der Privatsphäre und neuen Technologien wieder zu zerschlagen, indem in weiten Bereichen Datenverarbeitungen, die unter der DS-GVO zulässig wären, entweder unter den Vorbehalt einer strengeren Form der Einwilligung gestellt oder gänzlich untersagt werden.

Zudem werden durch den Entwurf auch Vorgänge erfasst, bei denen keine personenbezogenen Daten verarbeitet werden, indem er strenge Regeln für die Kommunikation zwischen Unternehmen und Maschinen vorsieht, die heute gängige Abläufe in der europäischen Wirtschaft in Frage stellen und Spielräume für Innovationen im Bereich Industrie 4.0 und dem Internet der Dinge sowie in anderen neuen Geschäftsfeldern stark verengt. Die Wettbewerbsfähigkeit der Wirtschaft in Europa wird damit über alle

Wirtschaftszweige hinweg bedroht.

Am 5. Dezember 2017 hat nun der Rat der Europäischen Union das Dokument 2017/0003 (COD) in Vorbereitung auf die WP TELE Zusammenkunft am 11. Dezember 2017 veröffentlicht und setzt sich darin erneut mit den Artikeln 6 bis 8 und 10 der Fassung des EU-Ratspräsidenten von September auseinander.

Bitkom bedankt sich für die Möglichkeit der Stellungnahme und möchte wie folgt auf einige der Änderungsvorschläge eingehen:

1. Artikel 6

Bitkom begrüßt zunächst, dass in Artikel 6(2)(b) die Verarbeitung für Zwecke der Vertragserfüllung eingeflossen ist und Artikel 6(2)(e) nun den Erlaubnistatbestand für wissenschaftliche Forschung und statistische Zwecke aufgenommen ist. Dies und auch die Änderung der Fassung für Artikel 6(2)(d) („vital interest") stellen notwendige Änderungen dar.

Die darüber hinaus wichtige und insbesondere für viele zukunftstragende Geschäftsmodelle notwendige Möglichkeit der Weiterverarbeitung von Metadaten fehlt bisher weiterhin. Im Rahmen des Artikel 6(2)(e) wird für die Verarbeitung von Metadaten zudem die Voraussetzung aufgestellt, dass die Verarbeitung für wissenschaftliche Forschung oder statistische Zwecke eine Rechtsgrundlage im EU-Recht oder nationalen Recht findet („Without prejudice to paragraph 1, providers of electronic communications networks and services may shall be permitted to process electronic communications metadata only i fit is necessary for scientific research or statistical purposes provided it is based on Union or Member State law (...)"). Eine solche Regelung läuft dem Zweck des e-Privacy VO-E entgegen, da durch die Inbezugnahme der jeweiligen nationalen Rechtslage bezüglich dieser Verarbeitung keine Harmonisierung erreicht werden kann.

Anhand einiger Beispiele lässt sich zudem verdeutlichen, dass die Verwendung statistischer Daten oft nicht ausreichend ist, um wichtige und nützliche Geschäftsmodelle zu ermöglichen:

(1) Parkleitsysteme

Reisenden kann in Innenstadtbereichen (erkannt über die zugehörigen Funkzellen) ein Verkehrs- und Parkplatzleitsystem angeboten werden, das über Empfehlungen an das jeweilige Endgerät arbeitet. Dabei werden lediglich Pseudonyme verwendet, die sich in dem betreffenden Bereich bewegen. Bei anonymen Informationen wäre die Einzelzuordnung nicht möglich. Eine Einwilligung unter Verwendung von Klardaten ist für diesen Dienst nicht erforderlich. Umgekehrt muss für ein verlässliches Verkehrsbild eine größt-

mögliche Menge teilnehmen, was mit einer Einwilligung statt einer opt-out Lösung kaum möglich ist. Zudem kann mit einem solchen System der CO2 Ausstoß und die Feinstaubbelastung in Innenstädten wegen der effizienteren Verkehrsführung erheblich reduziert werden.

(2) Verbindungsplanung im öffentlichen Nah-und Fernverkehr

Derzeit wissen Anbieter der öffentlichen Nah- und Fernverkehrsstrecken wie z.B. die Deutsche Bahn nicht, wie viele Fahrgäste sich in jedem (Regional-)Zug befinden. Im Falle einer Verspätung kann es vorkommen, dass ein Zug voller Fahrgäste eine Verbindung zum anderen Zug/Bus verpasst, der pünktlich abfährt. Mit pseudonymen Echtzeitdaten könnte die Bahn den Anschlusszug / Bus zurückhalten, um den meisten Fahrgästen auch im Falle einer Verspätung die beste Verbindung zu bieten. Anonyme Informationen sind in diesem Zusammenhang zu ungenau, da sie nur auf aggregierte Datensätze von mindesten 30 bzw. 50 Personen im Cluster zugreifen können.

(3) Gesundheitsbereich und Telemonitoring

Gesundheitsbereich gibt es zunehmend Dienste, bei denen Patienten ihre Gesundheitswerte in Echtzeit durch mobile Verbindungen überwachen lassen (müssen). In diesen Fällen ist eine hohe Verfügbarkeit der Verbindungen unerlässlich. Die Verfügbarkeit kann durch eine regelmäßige Überprüfung mit pseudonymen Daten überwacht und sichergestellt werden. Klardaten sind dazu nicht erforderlich. Anonyme Daten sind naturgemäß nicht ausreichend, weil eine Zuordnung nicht erfolgen kann.

(4) Netzstörungsanalyse und -information

Netzanbieter könnten die Standortmetadaten von Kunden verarbeiten, die sich in einem Gebiet befinden, in dem ein Netzausfall aufgetreten ist. Die Kunden erhalten eine nicht individualisierte Information, in der sie über den Netzausfall informiert werden, einschließlich weiterer Informationen über die Dauer usw. und wann das Netz wieder funktionsfähig ist.

(5) Unfallvermeidung

Die Zusammenführung von Standortdaten aus Fahrzeugen könnte zur Prognostizierung von Gefahrensituation verwendet werden, die aus der Kombination Autofahrer / Fußgänger / Fahrradfahrer entstehen könnten. Von Autosensoren erfasste Straßenschäden i.v.m. Mobilfunk Standortdaten können zur Unfallvermeidung genutzt werden. Klardaten sind in diesen Fällen nicht erforderlich, aber Pseudonyme.

(6) Situationsbezogene Warnungen

Die Benachrichtigung von Endkunden wäre möglich, wenn z.B. in räumlicher Nähe ihres Aufenthaltsbereichs ein besonderes Ereignis auftritt. Bei Besuchern von z.B. Nationalparks

z.B. in den Alpen kann es vorkommen, dass sie über eine gefährliche Situation im Park aufmerksam gemacht werden sollen, wie z.B. eine Lawinenwarnung. Dann kann eine Warnung an alle im Bereich des Parks befindlichen Besucher gesendet werden, basierend auf deren Standortdaten. Klardaten sind dafür nicht erforderlich, es genügt ein Pseudonym.

(7) Zusammenfassung

Im Rahmen des Artikels 6 sollte insgesamt die Privilegierung pseudonymer Datenverarbeitung aufgenommen werden. Bei der Verarbeitung großer Datenmengen, oftmals in Echtzeit, wird es künftig nur schwer möglich sein, mit den bisher vorgesehenen engen Tatbeständen belastbare und damit verwertbare Ergebnisse zu erhalten – zumal sich der Zweck einer Datenverarbeitung gerade bei Big Data Analytics ständig im Hinblick auf neue Korrelationen und Erkenntnisse ändert. Umso wichtiger werden deshalb Pseudonymisierungslösungen, die eine geeignete Grundlage und Flexibilität für kommerzielle Datenweiterverarbeitungen schaffen können und gleichzeitig die Interessen der Einzelnen angemessen schützen.

Art. 6 sollte daher an Art. 6 Abs.4 DS-GVO angepasst werden: demnach besteht die Möglichkeit der Weiterverarbeitung ohne erneuten Erlaubnistatbestand, soweit der neue Verarbeitungszweck „kompatibel“ und damit mit dem urspr. erhobenen Zweck vereinbar ist. Dabei spielen insbesondere Schutzmechanismen wie Pseudonymisierung und Verschlüsselung zum Schutz der Daten eine hervorgehobene Rolle (Art. 6 Abs.4 lit. e DS-GVO). Die Pseudonymisierung als anerkannte Schutzmaßnahme in der DS-GVO hat insofern den Vorteil gegenüber anonymisierten Daten, als der für Big Data Anwendungen so wichtige „identifier“, erhalten bleibt, unter gleichzeitiger Wahrung des Schutzes personenbezogener Daten.

Eine Anpassung an Art. 6 Abs. 4 DS-GVO würde den Anbietern die nötige Flexibilität geben, Metadaten zu anderen Zwecken nach Maßgabe der bereits in der DS-GVO festgelegten Kriterien zu verarbeiten. Damit würde ein gangbarer Weg für die Praxis aufgezeigt, der neben der Gewährleistung eines angemessenen Datenschutzniveaus dennoch Raum für Innovation lässt.

Dies hätte zudem den Vorteil, dass der so wichtige Gleichlauf mit der DS-GVO hier erreicht werden kann und sowohl die Interessen und der Datenschutz der Betroffenen gewahrt würden, ohne wichtige Geschäftszweige zu gefährden.

2. Artikel 7

In Artikel 7 fehlt derzeit noch die vollständige Inbezugnahme des Artikel 6(2)(b) („detecting or stopping fraudulent, or abusive use of, or subscription to, electronic communications services").

3. Kongruenz mit DS-GVO

Bitkom begrüßt zunächst, dass die Änderungsvorschläge eine Annäherung des e-Privacy VO-E an die Datenschutzgrundverordnung vornimmt. Hier müssen jedoch im Sinne der Kongruenz dann stringent die Anforderungen und Begrifflichkeiten der DS-GVO in dem e-Privacy VO-E eingearbeitet werden.

Diese Notwendigkeit zeigt sich zum Beispiel im Änderungsvorschlag zu Artikel 6(4) und Artikel 8(1)(d), in dem von „third party" statt von „processor" wie in dem in Bezug genommenen Artikel 28 DS-GVO die Rede ist. Hier sollte im Interesse der Rechtssicherheit unbedingt eine einheitliche Begriffsverwendung eingearbeitet werden.

Insgesamt sollte sich der Gesetzgeber daher bei den Verhandlungen zur e-Privacy Verordnung im Sinne der weiteren Harmonisierung für eine inhaltlich schlanke, an der DS-GVO orientierte Verordnung einsetzen, in der neue unbestimmte Rechtsbegriffe sowie zusätzliche Öffnungsklauseln vermieden werden. Alle Begrifflichkeiten, die in der e-Privacy Verordnung benutzt werden, sollten deshalb anwenderfreundlicher in den Begriffsbestimmungen zu finden sein. Es müsste außerdem eine klare Abgrenzung zwischen der Vertraulichkeit der Kommunikation (Telekommunikations-/Fernmeldegeheimnis) und der Verarbeitung von Daten (Datenschutz) geben. Regelungsbereiche, die bereits von der DS-GVO oder anderen Rechtsakten abgedeckt sind, sollten nicht parallel in der e-Privacy Verordnung wieder aufgegriffen werden.