Stellungnahme

Zur Abstimmung der Änderungsanträge zum Vorschlag einer Datenschutz-Grundverordnung im Ausschuss für bürgerliche Freiheiten, Justiz und Inneres (LIBE)
3. Juli 2013

Der Bundesverband Informationswirtschaft, Telekommunikation und neue Medien e.V. vertritt mehr als 1.700 Unternehmen, davon über 1.100 Direktmitglieder mit etwa 135 Milliarden Euro Umsatz und 700.000 Beschäftigten. Hierzu zählen Anbieter von Software & IT-Services, Telekommunikations- und Internetdiensten, Hersteller von Hardware und Consumer Electronics sowie Unternehmen der digitalen Medien. Der BITKOM setzt sich insbesondere für eine Modernisierung des Bildungssystems, eine innovative Wirtschaftspolitik und eine zukunftsorientierte Netzpolitik ein.

Seit Beginn der Arbeiten an der Verordnung fordert der BITKOM, ein dem deutschen Recht entsprechendes hohes Datenschutzniveau auf europäischer Ebene zu verankern. Dafür sollten bewährte Instrumente aus dem deutschen Recht übernommen werden. Gleichzeitig sollten mit der Verordnung aber auch Vorschriften, die sich nicht bewährt haben, überarbeitet werden, um den Rechtsrahmen für die Herausforderungen der kommenden Jahre zu stärken. Hierfür gibt es viele sinnvolle Vorschläge aus den Reihen der Europaabgeordneten im LIBE-Ausschuss. Im Folgenden möchten wir daher auf einige der aus unserer Sicht wichtigsten Punkte hinweisen.

Zusammenfassung

- Ob Daten zukünftig vermehrt pseudonymisiert und anonymisiert verarbeitet werden, hängt von den Anreizen ab, die die Verordnung setzt. Die Definition dieser Begriffe ist auch Voraussetzung für die Realisierbarkeit nützlicher Anwendungen wie z.B. Verkehrsplanung, E-Health, E-Energy etc.
- Anhand der gesetzlichen Erlaubnistatbestände und der Einwilligung entscheidet sich in der Praxis, ob Daten legal verarbeitet werden können. Deren Praxistauglichkeit muss daher besonders sorgfältig geprüft werden.
- Auftragsdatenverarbeitung spielt praktisch überall eine Rolle, wo IT eingesetzt wird. Unklare Regelungen ziehen schwierige Vertragsverhandlungen und Rechtsunsicherheiten in Unternehmen sämtlicher Branchen nach sich.
- Der Datenaustausch zwischen verbunden Unternehmen ist für die effizienten Unternehmensführung unerlässlich und sollte daher schlank geregelt werden.
- Profilbildung ist notwendig für das Funktionieren vieler Dienste und nicht grundsätzlich problematisch, Einschränkungen sollten sich daher am Risiko und den drohenden Nachteilen für den Betroffenen orientieren.
- Das Recht auf Vergessen werden muss kollidierende Grundrechte und mögliche Konsequenzen seiner Umsetzung berücksichtigen.
- Nur ein echtes One-Stop-Shop Modell und ein effizientes Kohärenzverfahren gewährleisten die einheitliche Durchsetzung der neuen Regeln.
- Das Verhältnis zur e-Privacy Richtlinie sollte für Fälle, in denen es Überschneidungen gibt, im Sinne eines Vorrangs der Verordnung geklärt werden.
- Das deutsche Modell des betrieblichen Datenschutzbeauftragten mit direkter Berichtslinie zur Geschäftsleitung hat sich bewährt und sollte entsprechend umgesetzt werden.

Bundesverband
Informationswirtschaft,
Telekommunikation und
neue Medien e.V.

Albrechtstraße 10 A
10117 Berlin-Mitte
Tel.: +49.30.27576-0
Fax: +49.30.27576-400
bitkom@bitkom.org
www.bitkom.org

Ansprechpartner
Susanne Dehmel
Bereichsleiterin
Datenschutz
Tel.: +49.30.27576-223
Fax: +49.30.27576-51-223
s.dehmel@bitkom.org

Nils Hullen
Leiter Büro Brüssel
Rue de la Science 14
1040 Brüssel, Belgien
Tel.: +32.2.609 53 21
Fax: +32.2.609 53 39
n.hullen@bitkom.org

Präsident
Prof. Dieter Kempf

Hauptgeschäftsführer
Dr. Bernhard Rohleder

1 Anwendungsbereich: Definition personenbezogenes Datum, anonyme und pseudonyme Daten

Datenschutzrecht stellt die rechtmäßige Verarbeitung und Nutzung von Informationen, die sich auf eine individualisierbare Person beziehen, sicher. Aufgabe des Datenschutzes ist die Vermeidung der Beeinträchtigung des allgemeinen Persönlichkeitsrechts durch die Nutzung, Verarbeitung oder Verbreitung personenbezogener Daten.

Einige der zurzeit diskutierten Änderungsvorschläge entsprechen nicht dem Sinn und Zweck des Datenschutzes. Der Umstand, dass einige Informationen unter Bezugnahme von Zusatzwissen theoretisch auf eine bestimmbare Person schließen lassen, stellt noch keinen ungerechtfertigten Eingriff in das Recht auf Schutz personenbezogener Daten dar. Stattdessen muss – wie im deutschen Datenschutzrecht – in Betracht gezogen werden, wer, unter welchen Umständen und mit welchem Aufwand, Daten mit einer bestimmten Person verknüpfen kann. Solange der Datenverarbeiter einen Personenbezug nicht (selbst) oder nur unter unverhältnismäßig hohem Aufwand herstellen kann, ist das allgemeine Persönlichkeitsrecht des Betroffenen bzw. das Recht auf Schutz personenbezogener Daten nicht berührt. Dies folgt auch dem Ansatz der Richtlinie 95/46, welche die Anwendbarkeit des Prinzips der Verhältnismäßigkeit auf das Konzept des personenbezogenen Datums in einem ihrer Erwägungsgründe anerkennt. Würde man den Anwendungsbereich auf Daten ohne Personenbezug erweitern, hätte es Folgendes zur Konsequenz:

1. Eine Vielzahl neuer digitaler Produkte und Dienste würden verhindert werden. Unsere digitale Umgebung bietet mehr und mehr individuell abgestimmte Anwendungen und auf das Nutzerverhalten ausgerichtete Angebote. Hierzu ist die Nutzung bestimmter Daten notwendig, in den allermeisten Fällen reichen hierzu pseudonymisierte oder anonymisierte Daten aus. Weiterhin stellen viele moderne innovative Dienste, bspw. zur Verbesserung des Verkehrsflusses, so genannte Big-Data-Anwendungen dar. Hierbei geht es weniger um die Auswertung individueller Daten, sondern um solche, die pseudonymisiert oder anonymisiert werden. Falls anonyme oder pseudonyme Daten als personenbezogen Daten klassifiziert werden und somit in den Anwendungsbereich der Datenschutzverordnung fallen sollten, obwohl das Recht auf Schutz der personenbezogener Daten nicht beeinträchtigt werden kann, werden solche Dienste zukünftig nicht mehr zu entwickeln und anzubieten sein.

2. Weiterhin werden Nutzer zukünftig kaum mehr zwischen wichtigen Datenverarbeitungsvorgängen und solchen, bei denen eine Einwilligung nur aus formalen Gründen notwendig ist, unterscheiden können. Falls alle Daten und Verarbeitungsvorgänge gleicht behandelt werden sollten, würde dies zu einer „Anklick-Routine“ im Rahmen der Einwilligung zur Nutzung digitaler Dienste führen. Die Verordnung sollte vielmehr das Bewusstsein und die Möglichkeit zum Schutz der eigenen Daten fördern.

Vor diesem Hintergrund unterstützt BITKOM die LIBE-Änderungsanträge, die eine kontrollierte, zukunftsorientierte Anwendung des Datenschutzes im angemessenen und erforderlichen Umfang bezwecken:

Bezüglich der Definition der betroffenen Person und anonymen Daten empfehlen wir **Änderungsantrag (ÄA) 734** zusammen mit **ÄA 14** (die Definition in AM 14 sollte in Art. 4 Abs. 1 übernommen werden) sowie **ÄA 391, 405** und **716, 720**. Weiterhin sollte der Anwendungsbereich klar definiert werden, vgl. **ÄA 683, 686, 687 oder 696**.

2 Rechtmäßigkeit der Verarbeitung, Einwilligung

BITKOM unterstützt das Konzept der informierten Einwilligung und einen harmonisierten Datenschutz in Europa, der kontrollierte Rahmenbedingungen für das Wachstum der digitalen Wirtschaft bietet.

Rechtsgrundlagen für rechtmäßige Datenverarbeitungsvorgänge sollten sich an den bestehenden und künftigen Bedürfnissen von Nutzern und Datenverarbeitern orientieren. Flexible Regelungen sollten unter anderem auf einer Grundrechtsabwägung basieren, die auch die Interessen Dritter berücksichtigt (**ÄA 455, 873, 874, 878**). Rechtsgrundlagen der Datenverarbeitung sollten darüber hinaus die Pseudonymisierung und die Anwendung technologischer Maßnahmen zur Verbesserung des Schutzes der Privatsphäre fördern (**ÄA 887, 897, 898, 900, 904**). Auch die steigende Notwendigkeit von Maßnahmen zur Betrugsbekämpfung (**ÄA 894)** und zur Steigerung der Internet- und Netzwerksicherheit (**ÄA 886, 899**) sowie zu Compliance-Zwecken (**ÄA 857/859/862**) muss berücksichtigt werden. Tarifverträge sind als eine hergebrachte Rechtsgrundlage für eine rechtmäßige Datenverarbeitung anzuerkennen (**ÄA 856**).

Regelungen zur Einwilligung sollten auf Transparenz und Handhabbarkeit abzielen und Rechtssicherheit für betroffene Personen und Datenverarbeiter gleichermaßen bieten. Die Anforderungen, die an eine gültige Einwilligung zu stellen sind, sollten sich dabei am Risiko, das mit dem Verarbeitungsvorgang verbunden ist, orientieren (**ÄA 105, 428, 429**). Eine unzweideutige, aber implizierte Einwilligung in Kenntnis aller relevanten Verarbeitungsumstände sollte bei entsprechend niedrigem Risiko möglich sein (**ÄA 105, 757, 758, 762, 765**). Zudem ist Rechtssicherheit eine unverzichtbare Voraussetzung zur Entwicklung neuer Geschäftsmodelle, eines innovativen digitalen Binnenmarkts und zur damit einhergehenden Förderung von Jobangeboten und wirtschaftlichem Wachstum. Eine rechtswirksame Einwilligung, die freiwillig und in Kenntnis aller relevanten Umstände abgegeben wurde, muss ein verlässlicher und beständiger Rechtsgrund der Datenverarbeitung bleiben. Schwammige Begriffe, wie der des „erheblichen Ungleichgewichts“, welches eine rechtsgültige Einwilligung aufheben soll, bedürfen keiner Berücksichtigung in einer stringenten Verordnung (**ÄA 983, 984, 985, 986, 987, 988**). Vertragsbeziehungen sollten auch weiterhin als Grundlage einer rechtmäßigen Datenverarbeitung für Betroffene und Datenverarbeiter dienen. Der Widerruf der Einwilligung darf nicht zu einer beliebigen Beendigung bestehender, rechtsgültiger Verträge führen oder dazu, dass Daten, die in rechtmäßiger Weise verarbeitet werden dürfen, gelöscht werden müssen (**AM 438, 976, 977, 980**).

3 Verhältnis Auftraggeber und Auftragsverarbeiter

Die Verantwortlichkeiten zwischen den für die Verarbeitung Verantwortlichen und Auftragsverarbeitern müssen klarer abgegrenzt werden. Die alleinige Verantwortlichkeit des für die Verarbeitung Verantwortlichen (vgl. Art. 6 Abs. 2 und Art. 17 RL 95/46/EG) hat sich bewährt. Diese deutliche Trennung hinsichtlich der alleinigen Verantwortung des für die Verarbeitung Verantwortlichen wird in den **Änderungsanträgen 522, 523, 524** sowie in **746, 747, 748** fortgeführt. Die bisherige Privilegierung des Auftraggebers, dass aufgrund seiner alleinigen Verantwortlichkeit die Weitergabe von Daten an einen Dienstleister im Rahmen einer Auftragsverarbeitung nicht den Voraussetzungen des Art. 6 unterliegt, findet sich in **ÄA 525**. Auch die betroffene Person muss wissen, wer ihr alleiniger Ansprechpartner beispielsweise für ihre Ansprüche auf Information und Auskunft ist. Daher können auch die Dokumentationspflichten auf denjenigen reduziert werden, der Ansprechpartner der betroffenen Person und dieser gegenüber informationspflichtig nach Art. 14 EU-DSGVO ist. Die **ÄA 1825, 1826** berücksichtigen dies. Eine deutliche Trennung der Verantwortlichkeiten zwingt den Auftraggeber, seiner Verantwortung auch schon bei der Auswahl des Dienstleisters gerecht zu werden. Dementsprechend ist auch eine gemeinschaftliche Haftung des Auftragsverarbeiters mit dem für die Verarbeitung Verantwortlichen nicht sachgerecht, da der Dienstleister nur weisungsgebunden agieren darf und zudem auch keine Möglichkeit hat, seinen Auftraggeber dahingehend zu kontrollieren, ob dieser tatsächlich die Berechtigung zur Verarbeitung der Daten besitzt. Daher sind die **ÄA 2818, 2822 und 2823** sachgerecht und berücksichtigen sowohl die Interessen der betroffenen Person, wie auch die Verteilung der Entscheidungskompetenz zwischen den für die Verarbeitung Verantwortlichen und den Auftragsverarbeitern.

4 Datenaustausch zwischen verbundenen Unternehmen

Das besondere Verhältnis zwischen verbundenen Unternehmen bedingt auch Bedürfnisse für einen Datenaustausch. Wenn ein angemessenes Datenschutzniveau im Konzern sichergestellt ist (z.B. durch Binding Corporate Rules, eine ernstzunehmende Selbstverpflichtung oder innerhalb Europas durch einheitliche Rechtsvorgaben), sollten die bisher bei einem Datentransfer innerhalb des Konzerns erforderlichen Verträge zur Auftragsdatenverarbeitung obsolet werden, um unnötigen bürokratischer Aufwand durch redundante vertragliche Vereinbarungen zu vermeiden. Insbesondere sollte es möglich sein, Schlüsselfunktionen wie Kundenservice, Rechtsabteilung, Revision oder Human Resources auf eine Rechtseinheit des Konzerns zu übertragen, ohne umfangreiche Vertragswerke zum Datenschutz abschließen zu müssen. Die rechtlichen Regelungen müssen hier an die Bedürfnisse von Konzernen angepasst werden und diejenigen Unternehmen privilegieren, die verbindliche Binding Corporate Rules etablieren. Zusätzlich sollten Binding Corporate Rules sich auch auf Unterauftragnehmer erstrecken, damit auch den Erfordernissen im Cloud Computing Rechnung getragen werden kann. Daher sollten insbesondere die **ÄA 795, 860/864, 901, 2426, 2467 2348**, **2349** und **2350** angenommen werden. Außerdem sinnvoll sind ÄA **2415, 2421** (in Folge von 2349) und **2422**.

5 Profilbildung

Art. 20 sollte nur Profiling-Maßnahmen untersagen, die das Persönlichkeitsrecht des Betroffenen tatsächlich beeinträchtigen. Änderungen, die einen angemessenen und praktikablen Ausgleich der Interessen von Nutzern und Datenverarbeitern bieten, sollten berücksichtigt werden. Die Grenze ist bspw. bei unfairen oder diskriminierenden Profiling-Maßnahmen erreicht, bzw. bei solchen, die zu schwerwiegenden Nachteilen für den Betroffenen führen. Grundsätzlich sollten Profiling-Maßnahmen unterhalb der Erheblichkeitsschwelle erlaubt bleiben. Profiling-Maßnahmen, die auf sensiblen Daten i.S.v. Art. 9 beruhen, sollten untersagt werden. Die Bestimmungen zur Verarbeitung von Daten im Arbeitsverhältnis i.S.v. Art. 9 Abs. 2 sollten hiervon unberührt bleiben.

Wir unterstützen daher Änderungsanträge, die Profiling beschränken, welches den Betroffenen schädigen kann (**ÄA 1544, 1547, 1553**). Andere Profiling-Maßnahmen sind als Datenverarbeitungsvorgänge durch die Verordnung geregelt (**ÄA 1579, 1588, 1590**). Darüber hinaus unterstützen wir solche Änderungsanträge, die Profiling-Maßnahmen, die auf der Verwendung pseusdonymer Daten beruhen, erlauben (**ÄA 1556, 1568**). Dies beruht auf einem risikobasierten Ansatz der Datenverarbeitung, der in der praktischen Anwendung das allgemeine Persönlichkeitsrecht der Betroffenen schützt und gleichzeitig die Anwendung von Profiling-Techniken nicht unterbindet, die grundlegend für viele Geschäftsmodelle, Wettbewerbsfähigkeit und wirtschaftlichem Erfolg sind.

Profiling-Maßnahmen, die unverzichtbar oder gesetzlich vorgeschrieben sind, sollten ausdrücklich erlaubt werden (**ÄA 1574, 1584, 1585, 1586, 1589**). Darüber hinaus unterstützen wir **ÄA 511, 1594, 1600, 1604 und 1612-1616**.

6 Recht auf “vergessen werden”

In der Form, in der das “Recht vergessen zu werden” im Entwurf der Kommission und verschärft in einigen der LIBE Änderungsanträge ausgestaltet ist, schafft operative Umsetzungsprobleme und zeigt nicht im vollen Umfang die Auswirkungen dieser Anforderungen auf a) andere nach der EU Charta anerkannte Grundrechte und b) die Rolle der Intermediäre nach EU-Recht. Wir unterstützen daher die **ÄA 1380, 1381, 1385, 1390, 1391, 1399, 1400, 1403, 1410, 1412, 1414.**

7 One-Stop-Shop und Kohärenzmechanismus

Die Einführung eines One-Stop-Shop-Prinzip ist richtig und wichtig. Die Zuständigkeit der Aufsichtsbehörde richtet sich im jetzigen Entwurf jedoch nach der einzelnen (meist juristischen) Person. Besteht ein Unternehmensverbund (z.B. ein Konzern) aus mehreren rechtlich selbstständigen Gesellschaften, etwa zwei GmbHs in Deutschland, einer S.A. in Frankreich, einer Ltd. in UK und einer SpA in Italien, so sind dies fünf Verantwortliche und es bleibt bei einer Beaufsichtigung durch vier bis fünf Aufsichtsbehörden. Die Rolle der Aufsichtsbehörde der Hauptniederlassung ist tatsächlich beschränkt auf Genehmigungen und die Koordinierung von gemeinsamer Durchsetzung. Ein „One-Stop-Shop“ existiert für in ihrer gesellschaftsrechtlichen Struktur diversifizierte Unternehmen nicht. **ÄA 786** führt dagegen zu einem echten One-Stop-Shop durch klar definierbare, konsistente und nachvollziehbare Kriterien zur Festlegung der Hauptniederlassung eines Konzerns oder einer Unternehmensgruppe. Diese Kriterien werden bereits heute erfolgreich im Datenschutzrecht angewendet, um die zuständige

Datenschutzbehörde für Binding Corporate Rules zu bestimmen. Hiernach kann ebenfalls eine einheitlich zuständige Datenschutzbehörde im Verhältnis zwischen Auftraggeber und Auftragsdatenverarbeiter bestimmt werden. **ÄA 790, 791** stärkt das One-Stop-Shop-Konzept durch die klare Festlegung, dass die Datenschutzbehörde der Hauptniederlassung eines Unternehmens die ausschließliche Zuständigkeit für Überwachungs- und Durchsetzungsmaßnahmen besitzt. Hierdurch wird Rechtssicherheit für betroffene Personen und Unternehmen gleichermaßen gewährleistet. **ÄA 793/794** stellt sicher, dass Unternehmen, die nicht in der EU ansässig sind, aber einen entsprechenden Vertreter in der EU benannt haben, ebenfalls vom One-Stop-Shop profitieren können. Dies ist vor dem Hintergrund des Grundsatzes der Nichtdiskriminierung geboten. Mit der Klarstellung, dass die Aufsichtsbehörde des Landes, in dem der Vertreter ansässig ist, ausschließlich zuständig ist (**ÄA 2588 2589 / 2590**), wird das One-Stop-Shop Prinzip weiterhin gestärkt. **ÄA 2599, 2618 / 2619, 2627 / 2628, 2633 / 2634, 2635 / 2636, 2662 / 2664** stehen im Einklang mit konsistenten One-Stop-Shop-Prinzipien und schreiben fest, dass dort die Befugnisse von der zuständigen Behörde i.S.v. Art. 51 wahrgenommen werden können.

8 Verhältnis der Verordnung zur e-Privacy Richtlinie

Vermeidung von Doppelregulierung bei e-Privacy Richtlinie: In der gegenwärtigen Fassung von Art. 89 ist das Verhältnis der Verordnung zur e-Privacy Richtlinie unklar. Zwar wird ausgeführt, dass die e-Privacy Richtlinie Vorrang genießt, soweit die Regelung dasselbe Ziel verfolgt wie die Verordnung, was dies im Einzelnen bedeutet, ist jedoch fraglich. Bei Bestands-, Verkehrs und Lokalisierungsdaten müssen gesetzliche Sonderwege für Telekommunikationsanbieter vermieden werden. Um ein Level-Playing-Field zu schaffen, ist eine klarstellende, unzweideutige und damit rechtssichere Anpassung des Anwendungsbereichs der sektorspezifischen e-Privacy Richtlinie erforderlich. Wir setzen uns für einen Anwendungsvorrang der Datenschutzverordnung ein, soweit identische Sachverhalte auch im Anwendungsbereich der e-Privacy Richtlinie liegen. Dieser Anwendungsvorrang sollte in der Verordnung durch eine Löschung der entsprechenden Vorschriften in der e-Privacy Richtlinie klargestellt werden (**ÄA 3127, 3129**). Eine spätere Novellierung der e-Privacy Richtlinie mit dem Ziel der Anpassung an die Verordnung, schafft gerade nicht die notwendige Rechtssicherheit.

9 Der betriebliche Datenschutzbeauftragte

Der betriebliche Datenschutzbeauftragte ist in Deutschland sehr erfolgreich. Das Modell ist sowohl bei den Aufsichtsbehörden als auch bei den Unternehmen anerkannt. Mit seiner starken Stellung und direkten Berichtslinie zur Geschäftsführung ist der betriebliche Datenschutzbeauftragte eine effektive und unabhängige interne Kontrollinstanz im Unternehmen. Um die Position des Datenschutzbeauftragen zu stärken, müssen Fortbildung, Unabhängigkeit (**ÄA 2228**) und Verschwiegenheit gewährleistet werden (**ÄA 2271, 2276, 2277, 2282, 2283).** Das Vertrauen in die Institution des Datenschutzbeauftragten wird gefördert, wenn pro Mitgliedsstaat mindestens ein Datenschutzbeauftragter bestellt werden muss (**ÄA 2195**). Die Bestellung eines Datenschutzbeauftragten sollte den

Unternehmen Vorteile bieten, etwa indem Melde- und Konsultationsverpflichtungen - wie auch im bisherigen nationalen Datenschutzrecht – entfallen (**ÄA 2019, 2861**). Dies würde die Eigenkontrolle in der Wirtschaft stärken und zugleich helfen, unnötigen bürokratischen Aufwand zu vermeiden. Zudem sollte die Möglichkeit, auf einen externen Datenschutzbeauftragen zurückgreifen zu können, ausdrücklich in der Verordnung verankert werden (**ÄA 2219**).