Deutscher Bundestag
Ausschuss Digitale Agenda

Ausschussdrucksache
18(24)91

Stellungnahme zum Fachgespräch „Europäische Datenschutzgrundverordnung“
Karlsruhe, 19. Februar 2016

Vorbemerkung:

Die Generierung von Daten hat in den letzten Jahren dramatisch zugenommen, 90% des weltweiten Datenvolumens stammen aus den letzten zwei Jahren. Wie nicht zuletzt die Enthüllungen rund um Edward Snowden gezeigt haben, ist der vertrauensvolle Umgang mit Daten essentiell wichtig für das digitale Zeitalter. Daten spielen aber auch bei der Refinanzierung für den Nutzer kostenfreier Angebote eine wichtige Rolle und schaffen dabei für beide Seiten einen Mehrwert: je besser Inhalte und Werbung auf den Kunden zugeschnitten sind, desto interessanter ist ein Angebot und desto weniger Werbung ist erforderlich, um das kostenlose Angebot zu refinanzieren. Dabei stehen deutsche und europäische Unternehmen im Wettbewerb zu marktstarken Plattformen nicht zuletzt aus den USA, die sich ohne klares Marktortprinzip auf andere Datenschutzregeln berufen können. Die Umsetzung der Datenschutzgrundverordnung in die Praxis muss daher vor allem zwei Ziele ins Gleichgewicht bringen: sie muss praxisgerechte Lösungen entwickeln, die eine Datennutzung nicht unnötig behindern und damit innovative Geschäftsmodelle ausbremsen. Gleichzeitig muss sie eine europaweit einheitliche Rechtslage für alle Anbieter auf dem europäischen Markt und vor allem auch die Durchsetzungsmöglichkeiten für alle Anbieter gewährleisten, damit eine durch unterschiedliche Datenschutzniveaus bestehende Schieflage beseitigt wird. Insofern wird es insbesondere darauf ankommen, dass sich die EU-Datenschutzbehörden auf ein gemeinsames, praktikables Verständnis der Datenschutzgrundverordnung, ihrer unbestimmten Rechtsbegriffe und auch Spielräume für nationale Öffnungsklauseln verständigen und dieses gemeinsam erarbeitete Datenschutzniveau auch gleichmäßig durchsetzen, damit innerhalb Europas nicht erneut ein Gefälle zwischen den Schutzniveaus einzelner Mitgliedsstaaten entsteht.

1) *Wie sind die Ergebnisse des Trilogs zur Datenschutzgrundverordnung aus Ihrer Sicht grundsätzlich zu bewerten? Im Zusammenhang mit der Datenschutzgrundverordnung sind Big Data, Ubiquitous Computing, Cloud Computing und andere datenzentrierte Geschäftsmodelle diskutiert worden. Sind diese Möglichkeiten der modernen Datenverarbeitung - vor dem Hintergrund der getroffenen Regelungen zur Weiterverarbeitung und Pseudonymisierung - aus Ihrer Sicht weiterhin möglich? Welche Auswirkun-*

United Internet AG

Vorstand:
Ralph Dommermuth (Vorsitzender),
Robert Hoffmann, Frank Krause,
Jan Oetjen, Martin Witt

Vorsitzender des Aufsichtsrats:
Kurt Dobitsch

Commerzbank AG, Frankfurt am Main
IBAN DE71500400000574622700
BIC COBADEFFXXX

Elgendorfer Straße 57
D-56410 Montabaur
HRB Montabaur 5762

Fon +49 2602/96-1100
Fax +49 2602/96-1011
www.united-internet.de

gen auf den internationalen Wettbewerb sind für europäische Anbieter zu erwarten? Inwiefern wird die Datenschutzgrundverordnung den gestiegenen Herausforderungen hinsichtlich eines effektiven Grundrechtschutzes angesichts neuer Arten der Datenerfassung, Speicherung, Verarbeitung und Weitergabe an Dritte insgesamt gerecht?

Grundsätzlich ist es zu begrüßen, dass mit der Datenschutzgrundverordnung ab dem Inkrafttreten (voraussichtlich Mitte 2018) erstmals einheitliche Regelungen für alle Mitgliedsstaaten und vor allem für alle in der Europäischen Union tätigen Unternehmen gelten werden. Neben der Vereinheitlichung der Rechtslage für die Verbraucher als Datenschutzsubjekte ist es wichtig festzustellen, dass Daten zu einem wichtigen Bestandteil der Wertschöpfung in der digitalen Wirtschaft geworden sind und daher gleiche Regeln für alle Marktteilnehmer ein wichtiger Schritt zur Herstellung von Wettbewerbsgleichheit sind. Der Umfang, in dem Daten erhoben, gespeichert und miteinander verknüpft werden können und dürfen, hat in datenbasierten Geschäftsmodellen direkten Einfluss auf die Wertschöpfung und damit auch die Möglichkeiten, sich durch Innovation, neue Produkte und Marketing am Markt zu positionieren. Hierbei gibt es durch unterschiedliche Datenschutzniveaus zwischen Deutschland, anderen EU-Mitgliedsstaaten und den USA aktuell noch ein deutliches Gefälle, das sich durch die Datenschutzgrundverordnung nun hoffentlich auflöst.

Gerade vor dem Hintergrund moderner Technologien und datenbasierter Geschäftsmodelle bleibt die Verordnung auf ihrer materiellen Seite jedoch weit hinter dem Anspruch zurück, ein modernes Datenschutzrecht für die digitale Welt zu schaffen. Vielmehr schafft sie gerade keine Anreize, Daten in pseudonymisierter Form zu nutzen, sondern betont in Verkennung der potenziellen Auswirkungen für digitale Nutzungsszenarien die Einwilligung als zentrale Erlaubnisvorschrift. Der Zugang zu personenbezogenen Daten ist eine kritische Voraussetzung für eine erfolgreiche und wettbewerbsfähige digitale Transformation aller Wirtschaftszweige. Klassische Branchen, wie beispielsweise die Automobilindustrie, arbeiten an zahlreichen datenbasierten Anwendungen, die neue Wertschöpfungsmöglichkeiten und Innovationen ermöglichen werden. Dabei wird es nur durch die Nutzung personenbezogener Daten künftig möglich sein, die Kundenschnittstelle in Anwendungsfällen wie der Echtzeit-Routenplanung mit dynamischer Stauvermeidung, der Autovermietung, entsprechender Versicherungsleistungen oder der Koordination von Tankstopps zu besetzen.

Um international als Wirtschaftsstandort Geltung zu behalten, werden Unternehmen im Austausch mit den zuständigen Aufsichtsbehörden Lösungen finden müssen, um die datenbasierte Technologien und Wertschöpfungsmodelle auch in Deutschland und Europa zu ermöglichen. Die Vorgaben der Datenschutzgrundverordnung erlauben dafür eine gewisse Flexibilität, legen aber nicht unbedingt den besten Grundstein. Insofern gehen wir davon aus, dass insbesondere durch Öffnungsklauseln und nähere Bestimmung bislang unklarer Begriffe (s.u. Frage 3) auch künftig eine pseudonymisierte Nutzung ermöglicht werden kann und setzen insoweit auf die Unterstützung der Datenschutzbehörden.

2) *Wird mit der Datenschutzgrundverordnung der erhoffte einheitliche und europaweite Rechtsrahmen für den Datenschutz erreicht, der europaweit einen hohen Datenschutzstandard garantiert, und kann hierdurch insbesondere auch das Marktortprinzip Wettbewerbsgleichheit für alle Anbieter, die in Europa ihre Dienste anbieten, sichergestellt werden? Wird die Umsetzung der Datenschutzgrundverordnung gleiche und faire Wettbewerbsbedingungen für deutsche und europäische Unternehmen sowie US-amerikanische Unternehmen herstellen?*

Im Wege der Verordnung wird ein einheitliches Regelwerk geschaffen, das in allen Mitgliedsstaaten gilt. Insofern gelten – zunächst auf dem Papier – europaweit die gleichen Regeln. Für grenzüberschreitend tätige Unternehmen bietet das den Vorteil, dass sie ihre Angebote nicht mehr an 28 unterschiedlichen Datenschutzgesetzen ausrichten müssen, sondern sich an einer zentralen Regelung orientieren können.

Wichtig ist jedoch, dass diese einheitlichen Regeln in den einzelnen Mitgliedsstaaten und Rechtsordnungen nun auch einheitlich verstanden, ausgelegt und vor allem umgesetzt werden. Das Marktortprinzip muss gelebt werden. Die Wahl einer direkt anwendbaren Verordnung als Regelungswerkzeug erscheint dafür zumindest vielversprechender als die bisherige Richtlinie. Worum es jetzt jedoch gehen muss, ist aber die Durchsetzung auch einheitlich zu gestalten. In der konkreten Auslegung der Datenschutzgrundverordnung muss das Ziel sein, Spielräume für digitale Geschäftsmodelle zu erhalten. Es darf jedoch nicht erneut ein Standortwettbewerb in Europa entbrennen, durch den sich einzelne Mitgliedsstaaten mit maximaler Ausnutzung des Spielraums und niedriger Kontrolldichte gegenüber anderen mit restriktiverem Ansatz profilieren und damit erneut ungleiche Wettbewerbsbedingungen schaffen. Hier muss zwingend ein nah an der Praxis moderner Nutzungsformen orientierter Konsens zwischen den verschiedenen Aufsichtsbehörden hergestellt werden.

Die Datenschutzgrundverordnung bietet also die Grundlage für die Erreichung gleicher Wettbewerbsbedingungen. Eine Garantie dafür, ist sie alleine allerdings nicht. Die starke Fokussierung der Datenschutzgrundverordnung auf die Einwilligung der Nutzer stellt sogar ein Risiko für den Wettbewerb dar: Die großen und dominierenden Internetplattformen verfügen bereits über eine unmittelbare Nähe zum Nutzer (z.B. über das Betriebssystem) und werden daher keine Schwierigkeiten haben, zukünftig erforderliche Einwilligungen für die Datenverarbeitung zu erhalten. Kleinere Unternehmen oder Startups – insbesondere in Bereichen jenseits der klassischen Internetdienste – haben jedoch deutlich reduzierte Chancen, entsprechende Einwilligungen zu erhalten. In der Folge verschlechtert sich deren Wettbewerbssituation. Es ist daher essentiell, dass in Hinblick auf die Wettbewerbsbedingungen des europäischen Digitalstandorts parallel zur Datenschutzgrundverordnung auch das regulative Umfeld großer Plattformen in den Blick genommen wird (Fragen der Neutralität, Interoperabilität, vertikalen Integration eigener Dienste etc.).

3) *Welcher Änderungsbedarf ergibt sich aus der Verabschiedung der Datenschutzgrundverordnung für das deutsche Datenschutzrecht und die zahlreichen bereichsspezifischen Vorgaben? Von welchen Öffnungsklauseln sollte der nationale Gesetzgeber zwingend Gebrauch machen, um über die Vorgaben der Datenschutzgrundverordnung hinausgehende Regelungen zu schaffen? In welchen Bereichen besteht zukünftig kein Spielraum mehr für den nationalen Gesetzgeber? Wo sehen Sie für den nationalen Gesetzgeber nach der Verabschiedung der Datenschutzgrundverordnung noch Möglichkeiten, Regelungen im nicht-öffentlichen Bereich zu schaffen? Sehen Sie insbesondere Handlungsbedarf seitens des Gesetzgebers im Bereich der Beschäftigtendaten? Und wenn ja, in welcher Form? Was kann man außerhalb der Gesetzgebung tun, um den Datenschutz in Umsetzung der Datenschutzgrundverordnung in Deutschland zu fördern?*

Welcher Änderungsbedarf sich ergibt, können wir derzeit noch nicht quantifizieren. Zahlreiche nationale Vorschriften werden bis zum Inkrafttreten geändert werden müssen und viele weitere werden nicht mehr bestehen bleiben können. Nach unserer Information arbeitet das zuständige Bundesministerium des Innern aktuell mit Hochdruck an der Beantwortung dieser Frage. Diese Situation wird in ähnlicher Form auch in den anderen europäischen Mitgliedsstaaten bestehen. Es wird dabei essentiell für den Erfolg der Datenschutzgrundverordnung sein, dass bestehende nationale Unterschiede in der datenschutzrechtlichen Bewertung innerhalb der europäischen Mitgliedsstaaten aufgehoben werden.

Aus unternehmerischer Sicht sollte der nationale Gesetzgeber nun denkbaren Öffnungsklauseln prüfen, die eine weitere Feinsteuerung erlauben, um aktuelle und zukünftige datenbasierte Wertschöpfung weiterhin zu ermöglichen. Inhaltlich geht es dabei vor allem um die bereits angesprochene pseudonyme Verarbeitung personenbezogener Daten, die in der bisherigen Form der Datenschutzgrundverordnung nicht ohne Eingreifen eines weiteren Erlaubnistatbestandes möglich ist. Die pseudonyme Verarbeitung erlaubt keinen Rückschluss auf die Identität einer Person, ohne dass gleichzeitiger Zugriff auf separate Datensätze erfolgt. Das Schutzniveau dieser Daten ist somit deutlich höher als das von sonstigen personenbezogenen Daten. Dies sollte in der Auslegung des Erlaubnistatbestands des legitimen Interesses Berücksichtigung finden (s. Frage 9). Weiterhin sollte die Praxis der Profilbildung, die aktuell in Deutschland spezialgesetzlich geregelt ist (insbesondere § 15 Abs. 3 Telemediengesetz) in den Blick genommen werden: es handelt sich hierbei um eine der wesentlichen Grundlagen für werbefinanzierte Geschäftsmodelle, die auch zukünftig für Unternehmen und Nutzer praktikabel bleiben muss. Die Datenschutzgrundverordnung erlaubt explizit (Art. 20 Abs. 1a lit. (b)) die Nutzung oder Schaffung nationalstaatlicher Regelungen, die im Kontext automatisierter Einzelauskünfte mögliche Aktivitäten legitimieren.

Von zentraler Bedeutung ist bei den Überlegungen zum Thema Öffnungsklauseln jedoch, dass die Arbeit der nationale Gesetzgeber und Datenschutzbehörden keine nationalen Sonderwege zur Folge haben darf. Das vorrangige Ziel muss die Schaffung eines einheitlichen Rechtsrahmens für alle Mitgliedsstaaten bleiben, in dem kein Gefälle hinsichtlich der Rechtsdurchsetzung herrscht. Daher ist eine enge Zusammenarbeit zwischen den Nationalstaaten und ihren Behörden von Beginn an erforderlich.

4) *Lässt die Datenschutzgrundverordnung ausreichend Spielraum für Innovation? Leistet sie einen Beitrag dazu, dass Datenschutz sich als Wettbewerbsvorteil für europäische Unternehmen etablieren kann? Wo und warum sehen Sie in dem neuen Regelungswerk positive und wo negative Effekte für die deutsche und europäische Wirtschaft?*

Wie bereits angemerkt, fällt die Datenschutzgrundverordnung weit hinter dem Anspruch zurück, ein modernes, innovationsförderndes Datenschutzrecht für eine zunehmend digitalisierte Welt zu schaffen.

Gerade die häufig kritisierten fehlenden Anreize für eine Pseudonymisierung sind hier hervorzuheben. Insbesondere dort, wo eine Vielzahl von Daten erhoben, gespeichert und verknüpft wird (Stichwort Big Data) geschieht dies in der Regel pseudonym, also ohne die Möglichkeit einer Zuordnung zu einzelnen Personen. Bei gleichzeitigem Schutz der Persönlichkeitsrechte wird also eine Verwertung ermöglicht. Diese Form der Datennutzung wird nicht explizit mit einem Anreiz versehen, sodass ein Szenario darin besteht, dass künftig so oder so eine Einwilligung des Nutzers notwendig ist und das Unternehmen in der Folge auf eine pseudonymisierte und damit deutlich datenschutzsensitivere Datennutzung verzichten wird. Insofern hätte sich die Wirtschaft eine eindeutige Klarstellung und positive Rechtsklarheit gewünscht, die jetzt erst im Rahmen der Auslegungsmöglichkeiten, unbestimmten Rechtsbegriffe und Öffnungsklauseln gemeinsam mit den Datenschutzbehörden erarbeitet werden muss. Durch die Bezugnahme auf die Pseudonmyisierung und Verschlüsselung im Rahmen der Anforderungen an mögliche Zweckänderungen gibt es hier Ansatzpunkte, die aber weit hinter dem zurückbleiben, was sich die Wirtschaft gewünscht hätte. In der konkreten Praxis werden Gespräche mit den Aufsichtsbehörden notwendig, wie die Vorschrift auszulegen ist bzw. ob sie nicht durch Zusatzgesetze spezifiziert werden sollte.

Die Einwilligung (und ihr Widerruf) werden als Erlaubnisnorm noch zentraler und unterliegen gleichzeitig strengeren Voraussetzungen (Unmissverständlichkeit durch eindeutige Handlung, freie Widerrufbarkeit, gesonderte Einwilligungen für verschiedene Verarbeitungsvorgänge). Dies spiegelt die allgegenwärtige Nutzung von Daten in den verschiedensten Kontexten nicht wider: Bereits heute werden zeitgemäße Geschäftsmodelle und maßgeschneiderte Angebote auf Basis komplexer Kundenprofile und einer Vielzahl weiterer Informationen

entwickelt. Die Entwicklung komplexer und flexibel nutzbarer Datenpools wird zum entscheidenden Wettbewerbsfaktor und es muss berücksichtigt werden, dass sich Anwendungsfelder dieser Daten nach der Erhebung ändern oder erst ergeben. Es bleibt daher abzuwarten, inwiefern dies vor dem Hintergrund der kommenden Regelverschärfungen weiterhin praktikabel durch die Wirtschaft umgesetzt werden kann.

Die Datenschutzgrundverordnung beinhaltet zahlreiche neue Dokumentations-, Melde- und Genehmigungspflichten (beispielsweise detaillierte Informationen zum Verarbeitungsvorgang und dem Zweck der Verarbeitung) und führt damit zu einem gesteigerten bürokratischen Aufwand. Auch an dieser Stelle sollte das zur Zeit in Europa bestehende Durchsetzungsgefälle berücksichtigt und beseitigt werden, um gleiche Wettbewerbsbedingungen herzustellen.

Auf der positiven Seite, kann neben dem bereits erwähnten Marktortprinzip, das eine große Chance für gleiche Wettbewerbsbedingungen darstellt, eine erhöhte Transparenz seitens der Unternehmen zu mehr Vertrauen beim Verbraucher führen. Es bleibt allerdings zu befürchten, dass sich in der Umsetzung ein spürbares Gefälle innerhalb Europas etablieren wird und sich dominierende Plattformen dies weiterhin zunutze machen werden. Eine enge Abstimmung zwischen den europäischen Aufsichtsbehörden wird daher von Beginn an entscheidend sein, um dieser Gefahr entgegenzuwirken. Bereits jetzt erfolgte im Rahmen der Article 29 Working Party eine grundlegende Abstimmung. Mit dem neuen Europäischen Datenschutzausschuss wird es ein Nachfolgegremium geben, dessen Aufgaben von entscheidender Wichtigkeit für das Ziel der einheitlichen Rechtsdurchsetzung sein werden. Insbesondere die Zusammenarbeit zwischen den nationalen Aufsichtsbehörden sollte bereits in den kommenden Monaten intensiviert werden, damit die bestehenden Regelungen geprüft und entsprechend der Datenschutzgrundverordnung angepasst werden können. Weiterhin bedarf es einer einheitlichen Auslegung der neuen Regeln.

Die Bestimmungen des Datenschutzes sind, wie eingangs erläutert, bereits jetzt von essentieller Bedeutung für Unternehmen und sollten daher europaweit einheitlich und nicht lokal ausgelegt werden. Eine vertiefte Zusammenarbeit und Ressourcenbündelung der Behörden, wie sie mit dem Europäischen Datenschutzausschuss geplant ist, ist aus unternehmerischer Perspektive absolut zu begrüßen: Im Bereich der Regulierungsbehörden für Telekommunikationsnetze besteht mit BEREC eine positive Vergleichsstruktur, die als Bezugsgröße genutzt werden kann. Insbesondere hinsichtlich einer einheitlichen Auslegung der Datenschutzgrundverordnung wird dem Ausschuss eine zentrale Rolle zukommen.

Jenseits der eigentlichen datenschutzrechtlichen Regulierung muss jedoch auch das Problembewusstsein der Nutzer berücksichtig werden, wenn Fragen des Wettbewerbsvorteils diskutiert werden sollen: Insbesondere die Enthüllungen von Edward Snowden zum systematischen Zugriff von Nachrichtendiensten auf Internetdienste und internetbasierte Kommunikation haben zu einem spürbaren Vertrauensverlust der Nutzer geführt. Initiativen der Wirtschaft, z.B. E-Mail made in Germany (GMX, Web.de, Deutsche Telekom, Freenet, Strato)

arbeiten mit einem dedizierten Datenschutzversprechen, Transparenz über den Speicherort der Daten und Möglichkeiten zur Verschlüsselung aktiv an einer erneuten Stärkung dieses Vertrauens. Wie die bisherige Erfahrung zeigt, eignet sich Datenschutz als zentraler Wettbewerbsvorteil zumindest im Endkundensegment nur eingeschränkt: Ein besonders hohes Maß an Datenschutz steigert die Nutzungs- und Zahlungsbereitschaft allein nur bedingt und verbleibt somit ausschließlich ein Baustein für einen attraktiven und wettbewerbsfähigen Service.

5) *Wie kann man eine flächendeckende Datenschutzaufsicht und -kontrolle im Hinblick auf das in der Verordnung verankerte „one-stop-shop"-Verfahren gewährleisten und dabei dem deutschen Föderalismus mit seinen Länderdatenschutzbeauftragten ausreichend Rechnung tragen? Welche Möglichkeiten sehen Sie, das innerstaatliche Kooperationsverfahren auszugestalten? Wie kann die Vertretung der deutschen Datenschutzaufsicht in Brüssel gewährleistet werden, ohne dass eine Doppelvertretung von Bundes- und Landesdatenschutzaufsichtsbehörden erfolgt, und wie könnte das Verfahren konkret ausgestaltet werden?*

Grundlage für ein europaweit einheitliches Verständnis ist es in der Tat, dass die deutschen Landesdatenschutzbeauftragten, die Bundesbeauftragte für den Datenschutz und weitere Behörden wie die Bundesnetzagentur ein gemeinsames Verständnis entwickeln. Dafür erscheinen ein verstärkter Kooperationsmechanismus und eine noch stärke Vereinheitlichung der Entscheidungen aller Aufsichtsbehörden notwendig. Dies demonstriert eindrücklich die aktuelle Debatte um die Folgen der EuGH-Entscheidung zu Safe Harbor und die unterschiedliche Bewertung der Standardvertragsklauseln zwischen verschiedenen Landesdatenschutzbeauftragten. Sollten sich tatsächlich unterschiedliche Bewertungen auf Landesebene manifestieren, entstünden schlimmstenfalls sogar unterschiedliche Rechtsfolgen innerhalb Deutschlands. Dies würde dem Ansatz europaweit einheitlicher Regelungen eindeutig zuwiderlaufen und das derzeit existente Binnengefälle weiter verschärfen. Idealerweise sollte es, wie in anderen europäischen Ländern üblich, auch in Deutschland nur eine Datenschutzinstanz geben. Selbstverständlich muss dabei der bewährten föderalen Struktur Rechnung getragen werden. Ein Gedanke hierzu wäre die Schaffung einer koordinierenden Geschäftsstelle, die eine einheitliche und verbindliche Regelung ermöglichte. Wie zuvor bereits erläutert, muss eine entsprechende, schrittweise Intensivierung der Zusammenarbeit der Aufsichtsbehörden natürlich gleichzeitig auch auf europäischer Ebene stattfinden.

6) *Wie bewerten Sie die Datenschutzgrundverordnung vor dem Hintergrund des Safe-Harbor-Urteils des EuGH von Oktober 2015 sowie des sogenannten „EU-US Privacy Shield" mit von der Europäischen Kommission ausgehandelten Kontrollbefugnissen*

und Rechten für europäische Bürger gegenüber amerikanischen Datenverarbeitern, das Anfang des Monats von der Europäischen Kommission vorgestellt wurde?

Zunächst ist zu konstatieren, dass sich materiellrechtlich in der Datenschutzgrundverordnung in Bezug auf die Möglichkeit der Übermittlung in Drittstaaten kaum Änderungen festzustellen sind: eine Übermittlung kann insbesondere auf Basis der bewährten Rechtsgrundlagen Einwilligung, Vertrag, Standardvertragsklauseln und Binding Corporate Rules erfolgen. Neue Auffangklauseln wie beispielsweise die des „berechtigten Interesses“ sind positiv hervorzuheben. Aktuell besteht in der Praxis aufgrund der Safe-Harbor-Entscheidung des Europäischen Gerichtshofs Unklarheit, ob diese Rechtsgrundlagen von den Datenschutzbehörden in Gänze (s. oben) weiterhin akzeptiert werden.

Es ist wichtig, dass eine Nachfolgeregelung von Safe Harbor, die zur Zeit unter dem Schlagwort „Privacy Shield“ diskutiert wird, verschiedene Anforderungen erfüllt. Es muss sichergestellt sein, dass ein Abkommen, unter welchem Namen es auch immer firmiert, keinen Freifahrtschein zur Aushöhlung deutschen und europäischen Datenschutzes ausstellt. Eine tatsächliche Kontrolle und Durchsetzung in der Praxis ist daher entscheidend. Die EU-Kommission hat angekündigt, dass die EU-Aufsichtsbehörden künftig intensiver mit der amerikanischen FTC zusammenarbeiten werden. Gleichzeitig wird die Kontrolle der Regeleinhaltung durch das amerikanische Handelsministerium erfolgen und die Kommission nur durch einen jährlichen Bericht informiert. Effektive Kontrolle wird jedoch letztendlich entscheidend sein und darf nicht nur Lippenbekenntnis bleiben. Ebenso muss sichergestellt sein, dass sich datenschutzrechtliche Bewertungen in den USA nicht nachträglich ändern und diesbezüglich verlässliche Planbarkeit besteht.

Klares Ziel muss in Anbetracht der neuen einheitlichen Datenschutzstandards vollkommene Transparenz für jeden europäischen Nutzer über die Speicherung und Verarbeitung seiner sensiblen personenbezogenen Daten sein, um den Nutzern daran anknüpfend weitergehende Wahlmöglichkeiten zur Datenverarbeitung anbieten zu können.

Was Unternehmen – und mittelbar natürlich auch Verbraucher – beiderseits des Atlantiks zur Zeit vor allem benötigen ist Rechtsklarheit. Ob diese im Lichte der Entscheidung des EuGH tatsächlich besteht, werden wohl erst die noch zu veröffentlichenden Details des „Privacy Shields“ und dessen Bewertung durch die Datenschutzbehörden und ggf. Gerichte zeigen.

7) *Kann Großbritannien tatsächlich eine Ausnahmeregelung in Anspruch nehmen, der zufolge die Sperrklausel des Art. 43 a Datenschutzgrundverordnung bei der Datenübermittlung an Drittstaaten keine Anwendung findet? Falls ja, wie bewerten Sie diesen Sachverhalt und welche Konsequenzen hätte dies für den Datenaustausch innerhalb von Europa und für britische Unternehmen?*

Sollten solche Ausnahmen in der Praxis tatsächlich relevant werden, ist das ein nicht zu unterschätzender Riss im Marktortprinzip, der Tür und Tor für ein erneutes Ungleichgewicht zwischen den verschiedenen europäischen Wirtschaftsstandorten öffnet. Das angestrebte einheitliche Schutzniveau in der Europäischen Union droht damit schon vor Inkrafttreten in einem gerade für den Verbraucher wichtigen Punkt zu scheitern. Wenn es wie in dieser Ausnahme nämlich um die Zulässigkeit der Datenübermittlung an ausländische Behörden geht, droht vor allem erneut ein Vertrauensverlust der Nutzer in die Sicherheit und Vertraulichkeit der Internetdienste.

8) *In Erwägungsgrund 40 wird die Weiterverarbeitung von personenbezogenen Daten erlaubt, wenn es sich dabei um eine aufgrund einer Rechtsvorschrift (seitens der Europäischen Kommission oder der Mitgliedsstaaten) „notwendige und verhältnismäßige Maßnahme zum Schutz insbesondere wichtiger Ziele des allgemeinen öffentlichen Interesses" handelt. Steht diese Passage vor dem Hintergrund, dass fraglich ist, ob eine einheitliche Rechtsauslegung dieser Begriffe in den Mitgliedsstaaten stattfindet, im Widerspruch zu einem einheitlichen Handeln innerhalb der EU-Mitgliedsstaaten?*

Wie alle Öffnungsklauseln und unbestimmten Rechtsbegriffe birgt auch diese Vorschrift die Gefahr unterschiedlicher Auslegungen, die schlussendlich einer einheitlichen Rechtsauslegung zuwiderläuft. Der Gefahr eines entstehenden Binnengefälles hinsichtlich der Rechtsauslegung wird zwar dadurch begegnet, dass sich das datenverarbeitende Unternehmen nur auf diejenige Rechtsordnung berufen kann, der sie selbst direkt unterworfen ist. Prinzipiell sollten jedoch unbedingt klare Definition und eine inhaltlich einheitliche Auslegung entsprechender Rechtsbegriffe sichergestellt werden, um das Ziel der einheitlichen Rechtsdurchsetzung nicht zu verwässern.

9) *Wie bewerten Sie die Ausnahmen der Datenschutzgrundverordnung zur Rechtmäßigkeit von Datenverarbeitung ohne Einwilligung zu Zwecken von berechtigtem Interesse?*

Ein alleiniges Abstellen auf die Einwilligung ist in der Praxis vielfach nicht umsetzbar. Die Datenschutzgrundverordnung umfasst daher auch zahlreiche weitere Erlaubnistatbestände, wie beispielsweise die Erfüllung rechtlicher Verpflichtungen oder öffentlicher Interessen (Beispiel: Datenaustausch mit Steuer- und Zollverwaltungen). Der Erlaubnistatbestand der „berechtigten Interesses" eröffnet insofern einen Spielraum, der grundsätzlich positiv zu bewerten ist und spezifische Abwägungen möglich macht. Es handelt sich hierbei um das bereits

aus dem aktuellen Bundesdatenschutzgesetz bekannte Abwägungsprinzip (siehe § 28 Abs. 1 Nr. 2 BDSG), das einen Ausgleich der Interessen des Betroffenen und des datenverarbeitenden Unternehmens vorsieht. Eine Datenverarbeitung ist also nicht automatisch unzulässig, wenn Interessen der Betroffenen berührt werden, sondern erst dann, wenn die Interessen der Betroffenen auch überwiegen. Damit hat das datenverarbeitende Unternehmen die Möglichkeit, den Effekt auf den Betroffenen zu minimieren bzw. die Positionen im Einzelfall in Ausgleich zu bringen. Denkbare Anwendungsfälle für diesen Erlaubnistatbestand sind beispielsweise Aspekte der internen Prozessoptimierung oder der Erkennung von Betrugsfällen. Insgesamt ist die Beibehaltung dieser Abwägungsvorschrift wichtig und zu begrüßen: Die Einholung einer Einwilligung in jeder Form der Datenverarbeitung wäre nicht umsetzbar und würde zudem die Nutzbarkeit für Verbraucher enorm einschränken. Die Nutzung technischer Maßnahmen wie vor allem der Pseudonymisierung sollte sich daher explizit positiv auf die erläuterte Interessensabwägung auswirken, allerdings wäre hier eine Klarstellung durch den Gesetzgeber wünschenswert, um Interpretationsspielräume und Schlupflöcher zu vermeiden.

Über United Internet

Die United Internet AG ist mit 15,43 Mio. kostenpflichtigen Kundenverträgen und 32,61 Mio. werbefinanzierten Free-Accounts der führende europäische Internet-Spezialist. Kern von United Internet ist eine leistungsfähige „Internet-Fabrik“ mit über 8.200 Mitarbeitern, ca. 2.700 davon in Produkt-Management, Entwicklung und Rechenzentren. Neben einer hohen Vertriebskraft über die etablierten Marken 1&1, GMX, WEB.DE, united-domains, Fasthosts, Arsys, home.pl, InterNetX, Sedo, affilinet und Versatel steht United Internet für herausragende Operational Excellence bei weltweit rund 48 Mio. Kunden-Accounts.

Ansprechpartner: Jan Oetjen, Vorstand Consumer Applications

Dr. Mario Rehse
mario.rehse@1und1.de | 030 8103152-8820 | Neustädtische Kirchstr. 8, 10117 Berlin