EDPS

DER EUROPÄISCHE DATENSCHUTZBEAUFTRAGTE

Antwort des EDSB zu der öffentlichen Konsultation der Kommission zum Regelungsumfeld für Plattformen, Online-Vermittler, Daten, Cloud-Computing und die partizipative Wirtschaft

Am 24. September 2015 startete die Europäische Kommission eine öffentliche Konsultation zu Online-Plattformen (und getrennt zu Geo-Blocking) als Teil ihrer Strategie für den digitalen Binnenmarkt.

Die Fragen der Konsultation überspannen einen recht breiten Bereich, was auf einen relativ umfassenden Ansatz der Kommission beim Umgang mit den Themen im Zusammenhang mit Online-Plattformen schließen lässt. Insbesondere bezieht sich die Konsultation auf die soziale und wirtschaftliche Bedeutung von Online-Plattformen, Transparenz (z. B. Suchergebnisse), Nutzungsbedingungen, Bewertungen und Rezensionen, die Nutzung von Informationen durch Plattformen, die Beziehung zwischen Plattformen und ihren Anbietern, die Bedingungen für einen Wechsel zwischen vergleichbaren Leistungen, die von Plattformen angeboten werden, sowie die Bedeutung von Online-Vermittlern, einschließlich von Verfahren zum Umgang mit unzulässigem Inhalt im Internet.

Der EDSB, als Berater der EU-Organe im Bereich des Schutzes der Privatsphäre und des Datenschutzes, befasst sich schon seit längerem mit der unkontrollierten Nutzung von personenbezogenen Daten zur Förderung der Funktion von Geschäftsmodellen, die von Online-Plattformen betrieben werden (oder mit ihnen verbunden sind) (z. B. die Stellungnahme des EDSB *„Bewältigung der Herausforderungen in Verbindung mit Big Data“*, siehe Fußnote 5).

Im Rahmen dieser öffentlichen Konsultation möchten wir unsere Kommentare auf Bereiche der Konsultation beschränken, die für das Recht auf den Schutz der Privatsphäre und den Datenschutz relevant sind oder sich auf diese auswirken. Dazu haben wir die Fragen geprüft und jene ausgewählt, die unserer Ansicht nach für die Rechte des Einzelnen auf den Schutz der Privatsphäre und den Datenschutz, die gemäß Artikel 7 und 8 der EU-Charta der Grundrechte, Artikel 16 des Vertrags über die Arbeitsweise der Europäischen Union und gemäß der Richtlinie 95/46/EG (die „Datenschutzrichtlinie“) geschützt sind, am relevantesten sind.

Einleitende Bemerkungen

Wir hegen allgemein Bedenken, dass bei der Formulierung vieler Fragen der öffentlichen Konsultation nicht angemessen darauf eingegangen wird, dass die meisten (wenn nicht sogar alle) Online-Plattformen aus der Verarbeitung von personenbezogenen Daten großen Gewinn ziehen. Stattdessen finden wir im ganzen Text Verweise auf „nicht personenbezogene“ Daten, wodurch die Ansichten der Befragten über die Art der Verarbeitung *personenbezogener Daten* auf Plattformen von vornherein ausgeschlossen werden. Dies stellen wir beispielsweise in der ersten Frage auf S. 16[1] fest, bei der lediglich nicht personenbezogene Daten erwähnt werden, während das zentrale Problem die Übermittlung

von personenbezogenen Daten zwischen Online-Diensten betrifft. Leider enthält der Text noch weitere Beispiele. Auch auf S. 24 lautet die Frage: *„Zur Gewährleistung eines freien Datenverkehrs innerhalb der Europäischen Union ist die Regulierung des Zugangs zu, die Übermittlung von und die Nutzung von nicht personenbezogenen Daten auf europäischer Ebene Ihrer Ansicht nach...“*. Bei dieser Frage wird die Tatsache überhaupt nicht berücksichtigt, dass es sich im Zusammenhang mit Online-Plattformen bei personenbezogenen Daten um die wertvollsten, gemeinsam genutzten Informationen handelt.

Die Fragen auf S. 26 betreffen *„Zugriff auf und Wiederverwendung von (NICHT PERSONENBEZOGENEN) wissenschaftlichen Daten“*, und auch hier haben die Befragten keine Gelegenheit, sich zu dem Wert zu äußern, den personenbezogene Daten im Zusammenhang mit wissenschaftlicher Forschung haben, oder zum kommerziellen Wert, den sie für pharmazeutische Unternehmen darstellen.

Wir räumen zwar ein, dass es sich nicht bei allen Daten, die auf Online-Plattformen gespeichert sind oder verkehren, um personenbezogene Daten handelt, müssen jedoch feststellen, dass dies auf einen großen Teil zutrifft, der auch sehr wertvoll ist. Die Aufnahme von Fragen, wie sie in den Beispielen erwähnt werden, bewirkt, dass wichtige Datenschutzthemen völlig übergangen werden. Darüber hinaus ist es möglich, dass die Antworten der Befragten dadurch verzerrt werden könnten, dass die Befragten zwar auf die Verarbeitung von personenbezogenen Daten eingehen möchten, aber nicht können; die Folge davon ist, dass die Schlussfolgerung der Kommission aus dieser Konsultation im Wesentlichen mangelhaft sein könnte.

1. ***Definition von Online-Plattformen***

In der öffentlichen Konsultation wird zwar eingeräumt, dass eine umfassende Definition von Online-Plattform angesichts der Vielfalt von Geschäftsmodellen keine einfache Aufgabe ist, aber es wird dennoch eine vorläufige Definition vorgeschlagen, die geprüft werden soll.

Wir empfehlen, in die Definition aufzunehmen, dass mit Online-Plattformen die Verarbeitung personenbezogener Daten verbunden ist - also einen zweckgerichteten Ansatz, bei dem die zentrale Rolle personenbezogener Daten für Plattformen hervorgehoben wird.

Falls sich die Kommission für die Regulierung von Plattformen entscheidet, würde eine solche Definition die Aufmerksamkeit des Gesetzgebers auf Datenschutzthemen wie *eingebauten Datenschutz*, Rechenschaftspflicht, Transparenz, Kontrolle der Nutzer über ihre Daten (einschließlich Datenübertragbarkeit), Sicherheitsmaßnahmen und andere Risikominderungsmethoden wie Datenminimierung lenken.

Schließlich stellen wir fest, dass Internet-Zugangsanbieter (IAP) als Kategorie im Geltungsbereich der Definition nicht enthalten sind. Eine generelle Ausnahmeregelung würde unserer Ansicht nach in dieser Hinsicht nicht greifen, da es durchaus möglich sein kann, dass IAP Online-Werbung auf ihren Websites hosten und so als Plattform fungieren, über die sie ihre Kunden mit externen Werbetreibenden in Kontakt bringen. Diese Geschäftsmodalität war zwar in der Vergangenheit häufiger anzutreffen - als viele IAP auch als Web-Portale mit kostenlosen Diensten (E-Mail, Wetterbericht, Aktienkurse) und Online-Werbung fungierten - , wird heute aber möglicherweise immer noch genutzt.[2]

2. Transparenz für Nutzer von Online-Plattformen: Verbraucher und Bürgerschutz

Online-Plattformen haben Geschäftsmodelle eingerichtet, bei denen (in den meisten Fällen) das zunehmende Volumen an personenbezogenen Daten, die sie durch die Bereitstellung von kostenlosen Diensten erheben, zu Geld gemacht wird. Die Komplexität derartiger Geschäftsmodelle verstärkt die Informationsasymmetrie zwischen Diensteanbietern und Kunden. Letztere können oft nicht in vollem Ausmaß und klar verstehen, wie sich Plattformen auf ihr Leben und ihre wirtschaftliche Lage auswirken.

Transparenz ist ein Grundprinzip sowohl des Verbraucherschutz- als auch des Datenschutzrechts (siehe insbesondere Artikel 8 der EU-Charta der Grundrechte). Im Verbraucherschutzrecht trägt Transparenz dazu bei, Gleichgewicht und Fairness zwischen den Vertragsparteien (dem Anbieter und den Kunden) sicherzustellen. Im Datenschutzrecht sorgt Transparenz dafür, dass betroffene Personen die Kontrolle über ihre personenbezogenen Daten und ihre Verwendung behalten. Gemäß dem Datenschutzrecht der EU sollten Plattformen klare Informationen über alle Bedingungen der mit den Kunden eingegangenen Vertragsvereinbarungen bereitstellen. Des Weiteren sollten sie klare und transparente Informationen über die Erhebung von personenbezogenen Daten und ihre Verarbeitung bereitstellen. Insbesondere ergibt sich eine derartige Verpflichtung aus dem Grunderfordernis der Verarbeitung nach Treu und Glauben, und sie beeinflusst, wie der Einzelne sein Recht auf Auskunft, Berichtigung und Widerspruch ausübt.[3]

Wir hegen Bedenken, dass der gegenwärtige Grad an Transparenz bei der Verarbeitung von personenbezogenen Daten häufig unzureichend ist und dem Kunden weder die Verarbeitung seiner Daten verständlich macht noch ihn in die Lage versetzt, fundierte Entscheidungen zu treffen. Transparenz kann dazu beitragen, sicherzustellen, dass Verbraucher, wenn sie sich über den Datenverabeitungs- und Monetisierungsvorgang vollkommen im Klaren sind, eine gerechtere Verarbeitung ihrer Daten verlangen oder zu Plattformen wechseln, die ihre Daten gerechter und effizienter nutzen.

Transparenz und die Möglichkeit für den Verbraucher, zwischen Plattformen zu wechseln, sind aus politischer Sicht äußerst wünschenswert, da sie u. U. einen positiven Wettbewerb beleben und Unternehmen dazu anregen können, sich gegenseitig bei den Datenschutzmaßstäben, die sie ihren Kunden anbieten, zu überbieten.

Online-Plattformen sollten Datenschutzrichtlinien klar ersichtlich anzeigen, und es soll darin erläutert werden, wie, von wem und zu welchem Zweck personenbezogene Daten verarbeitet und geschützt und wie lange sie aufbewahrt werden. Da Kunden unter Umständen keine langen Datenschutzrichtlinien lesen wollen, sollten diese verständlich und zugänglich formuliert werden.

3. Nutzung personenbezogener Daten für rechtmäßige und unrechtmäßige Zwecke

Gemäß Artikel 6 Buchstabe b der Richtlinie 95/46/EG werden personenbezogene Daten für festgelegte eindeutige und rechtmäßige Zwecke erhoben und verwendet und nicht in einer mit diesen Zweckbestimmungen nicht zu vereinbarenden Weise weiterverarbeitet. In dieser Hinsicht bestehen die größten politischen Bedenken darin, dass es für Online-Plattformen wirtschaftlich von Nutzen ist, Daten für Zwecke zu verwenden, die sich entweder von denen unterscheiden, zu denen sie ursprünglich erhoben wurden, oder mit diesen möglicherweise unvereinbar sind.

Online-Plattformen erleichtern auch Partnerschaften zwischen Unternehmen, die sich ansonsten nicht miteinander verbinden würden. Dies stellt zwar eine wichtige wirtschaftliche Funktion dar, kann aber die Aufklärung des Einzelnen darüber, wie seine Daten verwendet werden, erschweren.

In dieser Hinsicht ist es wichtig, dass Plattformen Kunden/Nutzern klare Vorabinformationen über ihr Geschäftsmodell und die Rolle, die personenbezogenen Daten in diesem Kontext zukommt, zur Verfügung stellen. Ist ein Element der Datenverarbeitung nicht bekannt (z. B. weil sich auf der Plattform neue, unvorhersehbare Geschäftspartnerschaften herausbilden), muss die Plattform über die geeignete Technologie verfügen, mit der sie Nutzer rechtzeitig *vor* dem Beginn einer etwaigen neuen Verarbeitung ihrer Daten informiert (z. B. Meldemechanismen auf intelligenten Endgeräten) und sie in die Lage versetzt, zu reagieren, wenn sie dies möchten. Auch in diesem Zusammenhang können sich Unternehmen mittels eingebauten Datenschutzes und standardmäßiger Datenschutzeinstellungen im Voraus auf die Erfüllung gesetzlicher Anforderungen vorbereiten.

4. Umgang mit rechtswidrigem Inhalt im Internet

Als einleitende Bemerkung stellen wir fest, dass Diensteanbieter (*z. B.* Online-Plattformen), die Inhalte „hosten" (oder speichern), die ihnen von einem ihrer Nutzer zur Verfügung gestellt wurden, gemäß der Richtlinie über den elektronischen Geschäftsverkehr von einer Ausnahmeregelung der „reinen Durchleitung" profitieren. Eine solche Ausnahme setzt jedoch voraus, dass sich der Anbieter der Unrechtmäßigkeit des Inhalts nicht bewusst ist, oder dass er Maßnahmen ergreift, um den Inhalt zu entfernen oder den Zugang zum Inhalt zu sperren, sobald er von der Unrechtmäßigkeit Kenntnis erlangt. Folglich sollte die Ausnahme nicht gelten, wenn ein Verstoß gegen Datenschutzbestimmungen für den Plattformbetreiber offensichtlich ist oder wird (z. B. personenbezogene Informationen werden verwendet, um jemanden zu belästigen).

Der Schwerpunkt der Konsultation der Kommission liegt zu Recht auf dem Inhalt als dem Hauptfaktor für den Erfolg einer Plattform. Während die für den Betrieb einer Plattform notwendigen Technologieinfrastrukturen reglementiert sind und darüber hinaus allgemeinen Wettbewerbsbestimmungen unterliegen, unterliegt der Inhalt weitgehend der Vertragsverhandlungsdynamik zwischen privaten Parteien. Daher muss also festgelegt werden, wann Inhalt rechtmäßig und somit verhandelbar ist und wann nicht.

Es besteht zwar kein (oder kaum) Zweifel, dass Inhalt, dessen Verwendung Urheberrechte verletzt, rechtswidrig ist und Mechanismen zur „Ahndung" von Urheberrechtsverletzungen auf Plattformen vorhanden sind, wir möchten jedoch Plattformen darin bestärken, von sich aus ähnlich wirksame Schutzmaßnahmen vorzusehen (z. B. Mechanismen für wirksame Forderungen zur Entfernung rechtswidriger Inhalte[4]), wenn die Verarbeitung von personenbezogenen Daten nicht im Einklang mit den Datenschutzbestimmungen steht. Mit dieser Thematik ist die Frage verbunden, ob Plattformbetreiber den in ihrer Online-Umgebung gespeicherten Inhalt aktiv überwachen sollten.

5. ***Wettbewerb zwischen Plattformen und Hindernisse, die Nutzern das Wechseln erschweren***

Die Fähigkeit der Verbraucher, von Plattform zu Plattform zu wechseln, spielt eine entscheidende Rolle bei der Förderung von Wettbewerb und Innovation, einschließlich auf dem Gebiet der Datenschutzmaßnahmen.

Ein Hindernis in dieser Hinsicht könnte unseres Erachtens die fehlende Datenübertragbarkeit sein; in diesem Fall müssten alle personenbezogenen Daten der betroffenen Person vollständig auf einer neuen Plattform bereitgestellt werden. Datenübertragbarkeit ist ein Konzept, das wir schon wiederholt befürwortet haben.[5] Wie es in der öffentlichen Konsultation erwähnt, ist die Datenübertragbarkeit immer dann eingeschränkt, wenn personenbezogene Daten nicht vollständig zugänglich sind oder in einem unzugänglichen Format bereitgestellt werden. Wenn die Übertragung der personenbezogenen Daten online nicht zur Verfügung steht, technisch schwierig oder teuer ist, besteht die Wahrscheinlichkeit, dass die Nutzer ihre anfängliche Wahl bestätigen. Die Gewährleistung von Datenübertragbarkeit, die außerdem für die Nutzerkontrolle wesentlich ist, ist daher ein Schlüsselfaktor für die Sicherstellung eines fairen Wettbewerbs zwischen Plattformen. Durch Gesetze gestützte Normierungsaktivitäten oder wirksame Selbstregulierung sind für die Unterstützung der Datenübertragbarkeit von ausschlaggebender Bedeutung und müssen gefördert werden. Gleichzeitig sollte die Implementierung der Datenübertragbarkeit nicht durch ausstehende Ergebnisse künftiger Normierungs- und Selbstregulierungsprozesse, die lange dauern können, behindert oder aufgeschoben werden.

6. ***Das Internet der Dinge: Funktion, Sicherungsmaßnahmen und Haftungszuweisung***

Fast alle Online-Plattformen (z. B. Amazon, Google, Facebook, Ebay) entwickeln Softwareanwendungen, die auf intelligenten Endgeräten (z. B. Handys, Tablets, Smart-TVs, Smartuhren) laufen und sich auf dem Markt weithin durchgesetzt haben. Produkte und Objekte, die durch diese Plattformen angebotene Dienste unterstützen, sind außerdem in zunehmendem Maße verbunden und können direkt untereinander kommunizieren und Feedback an die Plattform selbst liefern. All dies trägt zum Internet der Dinge („Internet of Things - IoT")[6] bei, das in Verbindung mit einer zunehmenden Rechnerleistung dazu führt, dass in großem Umfang personenbezogenen Daten „geerntet" werden können („Big Data").[7]

Die Wechselwirkung zwischen dem IoT und Big Data stellt möglicherweise u. a. eine Gefahr für den Datenschutz dar, weil sie die Herstellung von Verbindungen zwischen scheinbar getrennten und zusammenhanglosen Informationen ermöglicht. Darüber hinaus wird die Gewinnung von Erkenntnissen aus unbedeutenden oder gar Daten, die zuvor als „anonym" galten, durch die Verbreitung von Sensoren erleichtert und es werden bestimmte Aspekte von Gewohnheiten, Verhaltensmustern und Vorlieben einer Person offenbart.[8]

Dieses Szenario erscheint sogar noch komplexer, wenn man bedenkt, dass verbundene Objekte in der Regel von verschiedenen Herstellern produziert werden, die wiederum die Datenverarbeitung entweder unabhängig durchführen oder Dritten übertragen. Auf dem Markt gibt es oder kann es daher zahllose für die Verarbeitung Mitverantwortliche und Verarbeiter geben, was die Zuweisung von Verantwortung und Haftung erschwert und ein Hindernis für die betroffenen Personen bei der Ausübung sowohl ihrer Rechte als auch der Kontrolle über ihre Daten und bei der Inanspruchnahme von Rechtsmitteln darstellen kann.

Die in dieser Hinsicht wirksamste Regulierungsmaßnahme ist die kohärente Anwendung der Datenschutzrichtlinie, in der der für die Verarbeitung Verantwortliche wie folgt definiert wird: „*die natürliche oder juristische Person, Behörde, Einrichtung oder jede andere Stelle, die allein oder gemeinsam mit anderen über die Zwecke und Mittel der Verarbeitung von personenbezogenen Daten entscheidet*", und durch die ihm eine Reihe von Pflichten auferlegt wird, die dem Schutz des Rechts des Einzelnen auf Privatsphäre und Datenschutz dienen. Daher sollten sich Plattformbetreiber und andere Diensteanbieter vor einer Datenverarbeitung in den Informationen für Nutzer, deren Daten sie verarbeiten, als für die Verarbeitung Verantwortliche (oder Mitverantwortliche) identifizieren. Sie können ihre Position als für die Verarbeitung Verantwortliche ausschließlich auf der Grundlage identifizieren, dass sie personenbezogene Daten zu ihren eigenen Zwecken verarbeiten. Durch diesen Ansatz wird gewährleistet, dass Unternehmen verantwortungsvoll und im Einklang mit der Richtlinie handeln und dass die Haftungszuweisung effizient erfolgt.

Abschließend möchten wir darauf hinweisen, dass das Gericht im *Google Spain*-Urteil den Versuch der Suchmaschine, sich der Haftung für die Nichterfüllung der Datenschutzpflichten zu entziehen, da die Verarbeitung personenbezogener Daten (zu ihren Zwecken) auf Websites von Dritten stattgefunden habe, zurückgewiesen hat.[9]

7. ***Personenbezogene Daten und Cloud-Computing***

Da die meisten Online-Plattformen cloudbasiert sind, sehen sie sich alle denselben Herausforderungen in Bezug auf personenbezogene Daten durch Cloud-Computing gegenüber.

Trotz der Bedeutung, die Cloud-Dienstleistungen beim Einsatz von Online-Diensten zukommt, scheinen die Verbraucher in der EU cloudbasierten Diensten immer noch nicht völlig zu vertrauen, und zwar aus mehreren Gründen: Ungewissheit über effektive Datenspeicherlokalisierung und geltendes Recht, mangelnde Transparenz bei dem vom Cloud-Anbieter gewährleisteten Sicherheitsniveau und nicht zuletzt die unkalkulierbare Risikoverteilung zwischen Cloud-Anbieter und Nutzer bei Datenschutzverletzungen und nachfolgender Haftung.[10]

Die Bereitstellung datenschutzfreundlicher Lösungen für Cloud-Computing-Dienste ist daher eine der wichtigsten Herausforderungen für Online-Plattformen. Der EDSB als solcher und als Mitglied der Artikel 29-Datenschutzgruppe hat sich in der Vergangenheit dazu bereits geäußert[11] und wird auch weiterhin einschlägige Unterstützung und Beratung anbieten.

Die Förderung von Forschung und Vermarktung von Lösungen, die die Transparenz erhöhen und dem Nutzer mehr Kontrolle über seine Daten verleihen (wie „Managementsysteme für personenbezogene Daten"), ist unabdingbar, wenn ein höheres Schutzniveau angeboten und somit das Vertrauen des Nutzers erhöht werden soll.

Cloudbasierte Plattformen können Daten auch in Drittländer übertragen, wodurch es notwendig wird, für ein angemessenes Datenschutzniveau im Sinne der Richtlinie zu sorgen. Besonders das Empfängerland muss über Datenschutzmaßnahmen verfügen, die den im Rahmen der Europäischen Union gewährleisteten im Wesentlichen entsprechen, wie dies in der jüngsten Rechtsprechung des EuGH bestätigt wurde.[12]

Schlussfolgerung

Unsere wichtigste Bemerkung im Hinblick auf die öffentliche Konsultation der Kommission betrifft die Notwendigkeit (wenn nicht sogar Dringlichkeit, angesichts der Geschwindigkeit, mit der sich Plattformen entwickeln) einer angemessenen Definition der relevanten Fragen über die Nutzung personenbezogener Daten auf Online-Plattformen. Durch die Einschränkung von Fragen auf „nicht personenbezogene" Daten werden Probleme lediglich umgangen und aufgeschoben, was dazu führt, dass politische Maßnahmen auf fehlerhaften (oder zumindest unvollständiger) Erwägungen aufbauen. Bei jedem künftigen Instrument muss davon ausgegangen werden, dass eine Verarbeitung personenbezogener Daten mit hoher Wahrscheinlichkeit stattfindet. Zur Gewährleistung von Rechtssicherheit ist ein einfacher Verweis auf die Datenschutz-Grundverordnung möglicherweise nicht ausreichend, weshalb gründlich darüber nachgedacht werden muss, wie Datenschutzanforderungen in die EU-Politik zu Online-Plattformen genau zu integrieren sind.

Was den Regulierungsansatz zu Datenschutzfragen betrifft, sind wir der Ansicht, dass die bestehenden Datenschutzprinzipien und -vorschriften (zu Notwendigkeit, Verhältnismäßigkeit, Datenminimierung, Beschränkung auf den jeweiligen Zweck und Transparenz), ergänzt durch neue Prinzipien (wie Rechenschaftspflicht sowie eingebauter Datenschutz und standardmäßige Datenschutzeinstellungen) als Folge der Datenschutzreform eine stabile Grundlage für die Sicherung der Rechte des Einzelnen auf den Schutz der Privatsphäre und Datenschutz bieten werden. Erhöhte Transparenz, angemessene Auskunftsrechte und Datenübertragbarkeit sowie effektive Opt-out-Mechanismen können Nutzern nicht nur mehr Kontrolle über ihre Daten verleihen, sondern auch zu effizienteren Märkten für personenbezogene Daten beitragen, sowohl zugunsten von Verbrauchern als auch von Unternehmen. Eine verstärkte Einflechtung von Datenschutzprinzipien in die sektorspezifischen Rechtsvorschriften wird ebenfalls notwendig sein.

Eine gute Reglementierung ist zwar wesentlich, aber nicht ausreichend. Unternehmen und andere Organisationen, die intensive Anstrengungen unternehmen, um innovative Möglichkeiten für die Nutzung personenbezogener Daten zu finden, sollten bei der Umsetzung von Datenschutzprinzipien das gleiche innovative Denken zeigen. Nach wie vor notwendig sind die kontinuierliche Anwendung von Lösungen, die den Schutz der Privatsphäre erhöhen und auf dem Markt konkurrieren können, eine transparente und wirksame Selbstregulierung durch die Wirtschaft auf der Grundlage von Rechtsprinzipien und technischen Standards sowie eine bessere Aufklärung und Sensibilisierung von Nutzern und Anbietern.

Geschehen zu Brüssel am 15. Dezember 2015

[1] Die Frage lautet: „*Sollte ein zwingendes Erfordernis vorliegen, das ein leichtes Extrahieren von nicht personenbezogenen Daten und ihre problemlose Übermittlung zwischen vergleichbaren Online-Diensten gestattet?*"

[2] Siehe beispielsweise die Website tiscali.it

[3] Siehe Urteil des EuGH vom 1.10.2015 in der Rechtssache C-201/14, *Smaranda Bara u. a. gegen Președintele Casei Naționale de Asigurări de Sănătate u. a.*, Randnr. 33-34.

[4] Siehe Urteil des EuGH vom 13.5.2014 in der Rechtssache C-131/12, *Google Spain gegen AEPD*, in dem der Gerichtshof befand, dass der Suchmaschinenbetreiber Informationen, die für die Zwecke der Verarbeitung nicht mehr erheblich sind oder darüber hinausgehen, löschen muss (Randnr. 94).

[5] Siehe EDSB-Stellungnahme 7/2015, „*Bewältigung der Herausforderungen in Verbindung mit Big Data*", abrufbar unter https://secure.edps.europa.eu/EDPSWEB/webdav/site/mySite/shared/Documents/Consultation/Opinions/2015/15-11-19_Big_Data_DE.pdf; Stellungnahme 4/2015, „*Der Weg zu einem neuen digitalen Ethos: Daten, Würde und Technologie*", abrufbar unter https://secure.edps.europa.eu/EDPSWEB/webdav/site/mySite/shared/Documents/Consultation/Opinions/2015/15-09-11_Data_Ethics_DE.pdf und Stellungnahme vom 26. März 2014, „*Privatsphäre und Wettbewerbsfähigkeit im Zeitalter von Big Data*", abrufbar unter https://secure.edps.europa.eu/EDPSWEB/webdav/site/mySite/shared/Documents/Consultation/Opinions/2014/14-03-26_competitition_law_big_data_DE.pdf.

[6] Siehe Stellungnahme der Artikel 29-Datenschutzgruppe zum Internet der Dinge („Stellungnahme 8/2014 zu den jüngsten Entwicklungen im Internet der Dinge"). „*Unter dem Begriff „Internet der Dinge" versteht man eine Infrastruktur, in der Milliarden von in gewöhnlichen, alltäglichen Geräten („Dinge" als solche oder Dinge, die mit anderen Objekten oder Personen verbunden sind) eingebetteten Sensoren Daten erheben, verarbeiten, speichern, weiterleiten und - da ihnen eindeutige Kennungen zugeordnet sind - sich über Netzwerkfunktionen mit anderen Geräten oder Systemen verbinden und austauschen können*."

[7] Diesbezüglich besonders relevant sind so genannte „wearable computing devices" (also tragbare Vorrichtungen wie z. B. Armbanduhren, Brillen, Armbänder, Musikabspielgeräte, T-Shirts), in denen zahlreiche miteinander verbundene Sensoren integriert sind, die das Verhalten, Körperfunktionen und Informationen über Lebensweise des Nutzers aufzeichnen können.

[8] Siehe Artikel 29-Datenschutzgruppe, Stellungnahme zum Internet der Dinge, S. 8. Plattformen, Anbieter von Apps und intelligenten Endgeräten können ausreichende Mengen an Daten sammeln, sodass sie in der Lage sind, für sich selbst oder ihre Partner (z. B. Unternehmen oder Regierungen) gruppenspezifische Statistiken (unternehmensweite Profile oder regionale Profile) über jegliche Nutzerparameter zu erstellen. Dadurch kann für Plattformen, Diensteanbieter und andere Marktteilnehmer mit Datenzugriff ein Anreiz dafür geschaffen werden, von der Unterstützung der Nutzer bei ihrer Selbst-Quantifizierung (z. B. üblicherweise kostenlose, den Nutzern angebotene Möglichkeit, ihre Gesundheitsparameter zu messen) bis zum freiwilligen Smart-Coaching (Nutzern wird z. B. ermöglicht, mit Beratung durch Dritte einen gesunden Lebensstil zu pflegen) zu einer Phase zu wechseln, in der sie sich auf Verhaltensforscher stützen, um den Nutzern die „richtige" Botschaft zum „richtigen" Zeitpunkt „aufzudrängen".

[9] Siehe Urteil des EuGH vom 13.5.2014 in der Rechtssache C-131/12, *Google Spain gegen AEPD*, Randnr. 22 und Randnr. 28 ff.

[10] Siehe EDSB-Stellungnahme vom 26.11.2012 zu der Mitteilung der Kommission über „*Freisetzung des Cloud-Computing-Potenzials in Europa*", abrufbar unter https://secure.edps.europa.eu/EDPSWEB/webdav/shared/Documents/Consultation/Opinions/2012/12-11-16_Cloud_Computing_EN.pdf

[11] Siehe die Stellungnahme der Artikel 29-Datenschutzgruppe vom 22.9.2015 über den Verhaltenskodex zu Cloud-Computing, abrufbar unter http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2015/wp232_en.pdf und die Stellungnahme vom 1.7.2012 zu Cloud-Computing, abrufbar unter http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2012/wp196_en.pdf

[12] Siehe Urteil des EuGH vom 6.10.2015 in der Rechtssache C-362/14 *Maximillian Schrems gegen Data Protection Commissioner*, Randnr. 73-74.