EUROPEAN DATA PROTECTION SUPERVISOR

Stellungnahme 7/2015

Bewältigung der Herausforderungen in Verbindung mit Big Data

Ein Ruf nach Transparenz, Benutzerkontrolle, eingebautem Datenschutz und Rechenschaftspflicht

19. November 2015

Der Europäische Datenschutzbeauftragte (EDSB) ist eine unabhängige Einrichtung der EU. Der Datenschutzbeauftragte hat nach Artikel 41 Absatz 2 der Verordnung (EG) Nr. 45/2001 „[i]m Hinblick auf die Verarbeitung personenbezogener Daten [...] sicherzustellen, dass die Grundrechte und Grundfreiheiten natürlicher Personen, insbesondere ihr Recht auf Privatsphäre, von den Organen und Einrichtungen der Gemeinschaft geachtet werden" und ist „für die Beratung der Organe und Einrichtungen der Gemeinschaft und der betroffenen Personen in allen die Verarbeitung personenbezogener Daten betreffenden Angelegenheiten" zuständig.

Der Datenschutzbeauftragte und der Stellvertretende Datenschutzbeauftragte wurden im Dezember 2014 mit dem konkreten Auftrag ernannt, konstruktiver und proaktiver vorzugehen, und haben im März 2015 eine Fünfjahresstrategie veröffentlicht, in der sie darlegten, wie sie diesen Auftrag umzusetzen und darüber Rechenschaft abzulegen gedenken.

Diese Stellungnahme schließt sich an die vorherige Stellungnahme des EDSB zu einem digitalen Ethos an[1]. Auch in dieser Stellungnahme geht es um die Herausforderung, den Datenschutz an die digitale Welt anzupassen - dem ersten Ziel der EDSB-Strategie -, „um bestehende Datenschutzprinzipien für die globale digitale Arena anzupassen", auch im Lichte der Pläne der EU für einen digitalen Binnenmarkt. Sie stimmt mit dem Ansatz der Artikel-29-Datenschutzgruppe in Bezug auf Datenschutzaspekte der Verwendung neuer Technologien wie dem „Internet der Dinge", zu dem der EDSB als Vollmitglied der Gruppe beitrug, überein.

BIG DATA	BIG DATA
TRANSPARENCY	TRANSPARENZ
USER CONTROL	BENUTZERKONTROLLE
DIGNITY	WÜRDE
PRIVACY BY DESIGN	EINGEBAUTER DATENSCHUTZ
ACCOUNTABILITY	RECHENSCHAFTSPFLICHT
FREEDOM	FREIHEIT
PRIVACY	PRIVATSPHÄRE

„*The right to be let alone is indeed the beginning of all freedom*“ (Das Recht, in Ruhe gelassen zu werden, ist der Beginn jeder Freiheit)[2].

Big Data können - sofern sie verantwortungsbewusst verwaltet werden - mit erheblichen Vorteilen und einer signifikanten Effizienzsteigerung für die Gesellschaft und für Einzelpersonen verbunden sein, und zwar nicht nur in den Bereichen Gesundheit, wissenschaftliche Forschung, Umwelt und anderen konkreten Bereichen. Allerdings bestehen hinsichtlich der derzeitigen und potenziellen Auswirkungen der Verarbeitung gewaltiger Datenmengen auf die Rechte und Freiheiten des Einzelnen, einschließlich des Rechts auf Schutz seiner Privatsphäre, ernsthafte Bedenken. **Die Herausforderungen und Risiken von Big Data erfordern daher einen wirksameren Datenschutz.**

Die Technologie sollte uns unsere Werte und Rechte nicht vorschreiben, ebenso wenig, wie die Förderung von Innovation und die Wahrung der Grundrechte als unvereinbar angesehen werden sollten. Neue Geschäftsmodelle, bei denen neue Möglichkeiten für die massive Erhebung, die echtzeitnahe Übertragung, Verknüpfung und Wiederverwendung personenbezogener Daten für unvorhergesehene Zwecke genutzt werden, stellen eine neue Belastung für die Datenschutzgrundsätze dar; daher ist eine eingehende Auseinandersetzung mit der Frage erforderlich, wie diese angewandt werden sollen.

Das europäische Datenschutzrecht wurde entwickelt, um unsere Grundrechte und grundlegenden Werte, einschließlich unseres Rechts auf Privatsphäre, zu schützen. **Die Frage lautet nicht, *ob* das Datenschutzrecht, sondern vielmehr, *wie* es in innovativer Weise in neuen Umfeldern auf Big Data angewandt werden soll.** Unsere derzeitigen Datenschutzgrundsätze, einschließlich Transparenz, Verhältnismäßigkeit und Zweckbindung, bieten die Grundlage, die wir benötigen, um unsere Grundrechte in der Welt von Big Data noch dynamischer schützen zu können. Sie müssen allerdings durch „neue“ Grundsätze ergänzt werden, die sich im Laufe der Jahre herausgebildet haben, etwa Rechenschaftspflicht sowie eingebauter Datenschutz (privacy by design) und eine automatische, datenschutzfreundliche Voreinstellung (privacy by default). Das Datenschutzreformpaket der EU soll den rechtlichen Rahmen[3] stärken und modernisieren.

Die EU plant durch die Nutzung von Big Data die Maximierung von Wachstum und Wettbewerbsfähigkeit. Allerdings kann der digitale Binnenmarkt die datengesteuerten Technologien und Geschäftsmodelle, die in anderen Teilen der Welt zur wirtschaftlichen Normalität geworden sind**, nicht unkritisch importieren.** Stattdessen muss er bei der Entwicklung einer verantwortungsbewussten Verarbeitung personenbezogener Daten eine führende Rolle übernehmen. Das Internet hat sich so entwickelt, dass einige der erfolgreichsten Unternehmen die Überwachung, d. h. die Verfolgung des Verhaltens von Menschen, als ein unumgängliches Ertragsmodell sehen. Diese Entwicklung macht eine kritische Bewertung und die Suche nach praktikablen Alternativen erforderlich.

Auf jeden Fall müssen Organisationen, die gewaltige Mengen personenbezogener Daten verarbeiten, unabhängig vom Geschäftsmodell, für das sie sich entscheiden, das geltende Datenschutzrecht einhalten. Der Europäische Datenschutzbeauftragte (EDSB) ist der Auffassung, dass eine verantwortungsbewusste und nachhaltige Entwicklung von Big Data auf **vier wesentlichen Aspekten** beruhen muss. Organisationen müssen

- in der Frage, wie sie personenbezogene Daten verarbeiten, **transparenter** vorgehen;

- Nutzern ein höheres Maß an **Kontrolle** darüber gewähren, wie ihre Daten genutzt werden;
- einen benutzerfreundlichen Datenschutz **konzipieren** und in ihren Produkten und Dienstleistungen verankern; und
- für das, was sie tun, zu mehr **Rechenschaft** verpflichtet werden.

Im Hinblick auf **Transparenz** muss dem Einzelnen genau mitgeteilt werden, welche Daten verarbeitet werden, einschließlich solcher, die beobachtet oder hergeleitet werden; der Einzelne muss besser darüber informiert werden, wie und für welche Zwecke die ihn betreffenden Informationen genutzt werden, einschließlich der Logik, die von Algorithmen zur Bestimmung von Annahmen und Vorhersagen eingesetzt wird.

Mithilfe der **Benutzerkontrolle** sollen Menschen in die Lage versetzt werden, ungerechte Behandlung besser zu erkennen und sich über Fehler zu beschweren. Damit kann die Sekundärnutzung von Daten für Zwecke verhindert werden, die nicht ihren rechtmäßigen Erwartungen entsprechen: Mit einer neuen Generation der Benutzerkontrolle erhalten Menschen gegebenenfalls die Möglichkeit, eine echte, fundierte Entscheidung zu treffen, und haben mehr Möglichkeiten, ihre personenbezogenen Daten besser zu nutzen.

Starke **Rechte auf Datenzugriff und Datenübertragbarkeit und wirksame Rücktrittsoptionen *(opt-out*)** können als **Voraussetzung** dienen, **damit Benutzer eine stärkere Kontrolle über ihre Daten ausüben können,** und auch zur Entwicklung neuer Geschäftsmodelle und einer effizienteren und transparenteren Nutzung personenbezogener Daten beitragen.

Durch den **Einbau des Datenschutzes bei der Gestaltung ihrer Systeme und Prozesse** und die **Anpassung** des Datenschutzes **für mehr echte Transparenz und Benutzerkontrolle** werden **verantwortungsbewusste für die Verarbeitung Verantwortliche** auch in der Lage sein, die Vorteile von Big Data zu nutzen und zugleich dafür zu sorgen, dass die Würde und Freiheiten des Einzelnen geachtet werden.

Doch Datenschutz ist nur ein Teil der Antwort. Die EU muss die vorhandenen modernen Werkzeuge einheitlicher umsetzen, auch im Bereich **Verbraucherschutz, Kartellrecht, Forschung und Entwicklung**, um Garantien und Wahlmöglichkeiten auf einem Markt zu gewährleisten, auf dem datenschutzfreundliche Dienstleistungen florieren können.

Um den Herausforderungen von Big Data gerecht werden zu können, müssen wir **Innovation zulassen und zugleich die Grundrechte schützen.** Es ist jetzt Aufgabe von Unternehmen und anderen Organisationen, die viel Zeit und Mühe darin investieren, neuartige Möglichkeiten für die Nutzung personenbezogener Daten zu finden, auch bei der Umsetzung des Datenschutzrechts dasselbe innovative Denken an den Tag zu legen.

Auf der Grundlage früherer Beiträge der Wissenschaft und vieler Regulierungsbehörden und Interessengruppen **möchte der EDSB eine neue, offene und fundierte Diskussion in und außerhalb der EU** unter Beteiligung der Zivilgesellschaft, von Entwicklern, Unternehmen, Wissenschaftlern, Behörden und Regulierungsstellen zu der Frage **anregen**, wie das kreative Potenzial der Branche am besten für die Umsetzung von Rechtsvorschriften und den Schutz unserer Privatsphäre und anderer Grundrechte genutzt werden kann.

INHALTSVERZEICHNIS

1. Analyse von Big Data: Chancen, Risiken und Herausforderungen

1.1 „Big Data“ und „Analyse von Big Data“

Allgemein ausgedrückt bezieht sich der Begriff „Big Data“[4] als gemeinsamer Nenner unterschiedlicher Definitionen auf die Praxis des Kombinierens immenser Mengen von Informationen aus verschiedenen Quellen und ihre Analyse; dabei kommen komplexere Algorithmen als Grundlage der Entscheidungsfindung zur Anwendung. Big Data beruht nicht nur auf der zunehmenden Fähigkeit der Technologie, die Erhebung und Speicherung großer Datenmengen zu unterstützen, sondern auch auf ihrer Fähigkeit, den vollständigen Wert von Daten zu analysieren, zu verstehen und zu nutzen (insbesondere anhand von Analyseanwendungen).

Die Erwartungen an Big Data bestehen darin, dass sich daraus schließlich bessere und fundiertere Entscheidungen ergeben könnten. So könnten Big Data bessere Einblicke in die wissenschaftliche und medizinische Forschung, mehr Selbsterkenntnis für den Einzelnen sowie Produkte, Dienstleistungen und medizinische Behandlungen mit sich bringen, die besser auf die persönlichen Bedürfnisse zugeschnitten und damit besser für den Einzelnen geeignet sind, sowie bessere automatisierte Entscheidungen für Unternehmen und andere Organisationen, die Daten verarbeiten. Diese automatisierten Entscheidungen wiederum könnten zu einer besseren Effizienz führen, die vielfältige kommerzielle und andere Anwendungen in Aussicht stellt.

Die bei Big-Data-Anwendungen verarbeiteten Daten sind nicht immer personenbezogen: von Sensoren generierte Daten zur Überwachung von Phänomenen in der Natur oder der Atmosphäre wie Wetter oder Umweltverschmutzung oder zur Überwachung technischer Aspekte von Herstellungsverfahren beziehen sich nicht auf „*eine bestimmte oder bestimmbare Person*“. Einer der größten Vorteile von Big Data für Unternehmen und Behörden leitet sich jedoch aus der kollektiven und einzelpersonenbezogenen Überwachung von *menschlichem* Verhalten her und beruht auf deren Prognosepotenzial.

Ein Ergebnis ist die Entstehung eines Ertragsmodells für Internet-Firmen, das auf der Nachverfolgung von Online-Aktivitäten beruht. Derartige „Big Data“ sollten als personenbezogen eingestuft werden, selbst wenn Anonymisierungstechniken zur Anwendung gekommen sind: Der Rückschluss auf die Identität einer Person durch das Kombinieren von angeblich „anonymen“ Daten mit anderen öffentlich, beispielsweise auf sozialen Medien, zugänglichen Informationen, wird immer einfacher. Mit dem Einzug des „Internets der Dinge“ werden viele der von immer mehr persönlichen und anderen Geräten und Sensoren erhobenen und kommunizierten Daten personenbezogener Natur sein: die dabei gesammelten Daten lassen sich problemlos mit den Nutzern dieser Geräte in Verbindung bringen, deren Verhalten sie überwachen. Darunter fallen auch höchst sensible Daten wie Gesundheitsinformationen und Informationen über unsere Denkmuster und unsere psychologischen Anlagen.

Bei Big-Data-Anwendungen, bei denen personenbezogene Daten verarbeitet werden, werden oft auch bestimmte Aspekte von Einzelpersonen bewertet, einschließlich gesundheitlicher oder finanzieller Risiken. In anderen Fällen nutzen Unternehmen Big Data, um ihre Produkte oder Dienstleistungen effizienter und effektiver zu vermarkten bzw. eine stärker individuell zugeschnittene Dienstleistung zu erbringen. Auch bei einer wachsenden Zahl anderer Anwendungen werden Einzelpersonen zu unterschiedlichen Zwecken bewertet: so nutzt ein

Arbeitgeber Big Data zur Vorauswahl der aussichtsreichsten Bewerber für eine offene Stelle, und Reisende suchen mithilfe von Apps Taxiunternehmen oder Frühstückspensionen aus, die den besten Service anbieten. In anderen Fällen benötigen Unternehmen unsere Daten für verschiedene Untersuchungen: sie wollen allgemeine Entwicklungstrends und Zusammenhänge zwischen den Daten erkennen[5].

1.2 Welches sind heutzutage die größten Risiken und Herausforderungen in Verbindung mit Big Data?

Die Anwendung von Big Data ist mit erheblichen Vorteilen für den Einzelnen und für die Gesellschaft verbunden, wirft aber auch ernsthafte Bedenken hinsichtlich ihrer potenziellen Auswirkungen auf die Würde sowie die Rechte und Freiheiten des Einzelnen, einschließlich des Rechts auf Schutz der Privatsphäre, auf. Diese Risiken und Herausforderungen wurden bereits ausgiebig von Datenschutzexperten weltweit analysiert[6], und daher geht der EDSB lediglich auf einige der wichtigsten Bedenken ein.

Mangelnde Transparenz. Während die Datenverarbeitung immer komplexer wird, verlangen Unternehmen zur Wahrung von Geschäftsgeheimnissen häufig einen vertraulichen Umgang damit, „wie" Daten verarbeitet werden. In einem Bericht des Weißen Hauses aus dem Jahr 2014 heißt es: „*some of the most profound challenges revealed during this review concern how big data analytics may ... create such an opaque decision-making environment that individual autonomy is lost in an impenetrable set of algorithms*"[7] (bei einigen der größten Herausforderungen, die sich bei dieser Prüfung herausstellten, geht es darum, wie Big-Data-Analysetechniken eine derartig undurchsichtige Entscheidungsfindungsumgebung … erzeugen, dass sich die Autonomie des Einzelnen hoffnungslos in einem Algorithmen-Dschungel verstrickt). Einzelpersonen, die nicht über die geeigneten Informationen und Kontrolle verfügen, „*will be subject to decisions that they do not understand and have no control over*"[8] (sind Gegenstand von Entscheidungen, die sie nicht verstehen und über die sie keine Kontrolle haben). In Fällen in denen eine solche Einwilligung erforderlich ist, können Einzelpersonen die sie betreffenden Daten nicht wirksam kontrollieren und auch keine Einwilligung dazu erteilen, die auf einem echten Verständnis der Situation beruht und damit aussagekräftig ist. Dies gilt umso mehr, als die genauen künftigen Verwendungszwecke bei einer Sekundärnutzung der Daten zum Zeitpunkt ihrer Beschaffung möglicherweise noch nicht bekannt sind; in dieser Situation sind die für die Verarbeitung Verantwortlichen möglicherweise nicht in der Lage oder zögern, sich dazu zu äußern, was vermutlich mit den Daten geschieht, und bei Bedarf eine Einwilligung einzuholen.

Informationsgefälle zwischen den Organisationen, die die Daten verwalten, und den Einzelpersonen, deren von ihnen verarbeitete Daten mit der Bereitstellung von Big-Data-Anwendungen zunehmen[9].

Werden diese Probleme nicht bewältigt, besteht möglicherweise die Gefahr, dass die zentralen Grundsätze des Datenschutzes gefährdet werden. Die Chancen, die im Zusammenhang mit Big Data wahrgenommen werden, bieten Anreize, möglichst viele Daten zu erheben und diese möglichst lange für zukünftige, noch nicht näher bestimmte Zwecke aufzubewahren. Manche Befürworter von Big Data fordern Ausnahmen von den zentralen Grundsätzen, insbesondere von denjenigen der Zweckbindung und der Datensparsamkeit, und führen an, dass diese Grundsätze nicht (oder nicht vollständig) auf die Verarbeitung von Big Data angewandt werden sollten. Big Data stellt aber auch die Grundsätze der Genauigkeit und Relevanz von Daten in Frage. Big-Data-Anwendungen neigen typischerweise dazu, dass

Daten aus unterschiedlichen Quellen erhoben werden, ohne dass die Relevanz oder Genauigkeit der auf diese Weise erhobenen Daten sorgfältig überprüft wird.

Einer der potenziell schlagkräftigsten Einsatzbereiche von Big Data sind Vorhersagen dessen, was passieren könnte, jedoch noch nicht passiert ist, und was wir wahrscheinlich tun werden, jedoch noch nicht getan haben. So könnte Big Data beispielsweise zur Vorhersage der schulischen Leistungen von Kindern oder der Anfälligkeit von Erwachsenen für Krankheiten oder vorzeitigen Tod, von Kreditausfällen oder das Begehen von Straftaten verwendet werden. Trotz der potenziellen Vorteile wurden Daten von einem Kommentator als „*pollution problem of the information age*“[10] (Verschmutzungsproblem im Informationszeitalter) beschrieben, das mit dem Risiko einer „**Datendiktatur**“ einhergeht, bei der – einer Studie einer europäischen Datenschutzbehörde zufolge – „*we are no longer judged on the basis of our actions, but on the basis of what all the data about us indicate our probable actions may be*“[11] *(wir nicht mehr aufgrund unseres Handelns, sondern aufgrund aller Daten über uns, die auf unser mögliches Handeln hindeuten, beurteilt werden).*

Das übersteigerte Vertrauen in die Fähigkeiten von Big Data könnte aufgrund der erwarteten Vorteile von auf Statistiken beruhenden Vorhersagen noch weiter zunehmen. **Bei Big-Data-Anwendungen könnten falsche Zusammenhänge bei Daten gefunden werden,** und zwar auch in Fällen, in denen kein unmittelbarer Ursache-Wirkungs-Zusammenhang zwischen zwei Phänomenen besteht, die in einem engen Wirkungszusammenhang stehen. In diesen Fällen besteht das Risiko, dass ungenaue, jedoch auch - bei einer Anwendung auf individueller Ebene - **potenziell ungerechte und diskriminierende Schlussfolgerungen** gezogen werden.

Diese und weitere Merkmale von Big Data, die ausgiebige Nutzung automatisierter Entscheidungen und der Vorhersageanalyse könnten ferner zu weitreichenderen unerwünschten Veränderungen bei der Entwicklung unserer Gesellschaften führen. Wichtig ist, dass sie zu Diskriminierung, zur Verhärtung bereits vorhandener Stereotypen und zu **sozialer und kultureller Segregation und Ausgrenzung führen können**[12].

Die Anhäufung gewaltiger Datenreihen personenbezogener Daten, die in die Analyse von Big Data einfließen, ist aufgrund der ständigen, unsichtbaren Verfolgung von Online-Aktivitäten möglich. Diese Überwachung kann sich aber auch **abschreckend auf Kreativität und Innovation auswirken.**

Mithilfe der Analyse von Big Data werden Verhaltensmuster ermittelt, die statistisch gesehen kaum problematisch sind, um für die Organisationen, die die Daten verarbeiten, einen größeren Mehrwert zu schaffen. Es ist ein Trend dahingehend zu beobachten, dass versucht wird, Spontaneität, Experimentierfreude oder die Abweichung von der statistischen „Norm“ zu verhindern oder zu bestrafen und ein konformistisches Verhalten zu belohnen. So haben beispielsweise der Banken- und der Versicherungssektor ganz offenkundig ein Interesse daran, tiefe Einblicke in das Einzelpersonen anhaftende Risiko zu gewinnen, die sich aus Kombinationen von Datensätzen ergeben, die durch Aktivitäten in sozialen Netzwerken und durch angeschlossene Geräte zur Verfolgung des Standortes und anderen personenbezogenen Informationen sowie der steigenden Zahl angeschlossener Gegenstände generiert werden. Der Bedarf an einem Darlehen oder einer Versicherung könnte Menschen dazu bewegen oder zwingen, den Kontakt mit bestimmten Menschen oder Unternehmen zu meiden oder Bereiche mit einer hohen Kriminalitätsrate zu besuchen, ebenso wie sich Menschen dadurch veranlasst sehen, „Black Boxes“ zu installieren, damit sie von einem externen Kontrolleur beim Fahren überwacht werden können[13].

Allein die Tatsache, dass unser Verhalten ununterbrochen verfolgt und analysiert wird, könnte uns zur Vorsicht mahnen, damit wir beobachten, wie wir uns verhalten, und uns dazu anregen, uns bereits im Vorfeld an das anzupassen, was wir als die Norm ansehen. Diese Trends können sich aber auch abschreckend auf die freie Meinungsäußerung und andere Aktivitäten auswirken, die für den Erhalt einer demokratischen Gesellschaft erforderlich sind, etwa die Ausübung der Versammlungs- und Vereinigungsfreiheit.

Unter diesem Gesichtspunkt sind die Rechte auf Privatsphäre und den Schutz personenbezogener Daten eine Voraussetzung, damit der Einzelne seine Persönlichkeit entfalten und ein Leben als unabhängiger Mensch führen kann, sowie eine Voraussetzung für die Ausübung wertvoller Rechte und Freiheiten, aber auch eine **Voraussetzung für die Innovationstätigkeit Einzelner und der Gesellschaft insgesamt**.

Damit unsere Grundrechte und grundlegenden Werte, einschließlich unserer Fähigkeit, für uns als Gesellschaft und als Einzelne, auch künftig innovativ zu sein, geschützt und gewahrt werden, muss Big Data verantwortungsvoller und nachhaltiger eingesetzt werden. Wie bereits in unserer früheren Stellungnahme 4/2015 ausgeführt, muss dringend ein großes Datenschutz-Ökosystem angedacht werden, das besteht aus

- Organisationen, die in der Frage, wie sie personenbezogene Daten verarbeiten, transparenter vorgehen;
- Einzelnen, die ein höheres Maß an Kontrolle über die Art der Nutzung der sie betreffenden Daten besitzen;
- in Produkte und Dienstleistungen eingebautem Datenschutz; und
- für die Verarbeitung Verantwortlichen, die in höherem Maße rechenschaftspflichtig sind.

In dieser Stellungnahme soll auf jedes dieser vier Themen kurz eingegangen werden.

2. Transparenz: die verdeckte Profilerstellung muss ein Ende haben

2.1 Offenlegung der Logik der Analyse von Big Data

Mit dem Aufkommen der Analyse von Big Data kommt der Transparenz automatisierter Entscheidungen ein immer höherer Stellenwert zu. Durch Aufdeckung der Logik, die der Entscheidungsfindung zugrunde liegt, können Einzelne besser überprüfen, ob die Schlussfolgerungen von Organisationen, die die Daten verarbeiten, und die sich auf Einzelne auswirken, richtig und angemessen sind. Sie können die zugrunde gelegten Kriterien und die Faktoren, die die Entscheidung beeinflussen, besser verstehen und vielleicht berichtigen.

Als Gesellschaft müssen wir in der Lage sein, in die „Black Box“ der Big-Data-Analyse hineinzuschauen, damit gewährleistet ist, dass spezielle Analyseanwendungen sicher installiert werden können und uns allen zugutekommen[14]. Dementsprechend wird von Organisationen erwartet, dass sie die der Big-Data-Analyse zugrunde liegende Logik offen legen, sofern sich diese (direkt oder indirekt) auf den Einzelnen auswirkt. Dabei müssen sie

proaktiv vorgehen[15], ohne dass Einzelne aktiv Schritte unternehmen müssen, um eine Offenlegung zu beantragen[16].

Die im Zusammenhang mit Big Data verarbeiteten personenbezogenen Daten bestehen nicht mehr aus Informationen, die Einzelne Organisationen bewusst mitgeteilt haben. Die heutzutage verarbeiteten personenbezogenen Daten werden weitgehend beobachtet oder hergeleitet: die Erfassung von Online-Aktivitäten und Standorten von Smartphones und Tablets sowie die wachsenden Möglichkeiten, Aktivitäten in der „echten Welt" mithilfe von intelligenten Geräten und dem „Internet der Dinge" zu verfolgen, ergänzen den gewaltigen Datenberg, aus dem Rückschlüsse auf uns gezogen und Vorhersagen getroffen werden. Transparenz ist aber auch dann wichtig, wenn Daten aus öffentlich zugänglichen Quellen gewonnen werden.

Ob Daten freiwillig zur Verfügung gestellt, beobachtet oder hergeleitet werden[17] oder aus öffentlich zugänglichen Quellen stammen - der Einzelne ist in jedem Fall in vollem Umfang berechtigt zu erfahren, um welche Art von Daten es sich handelt und von wo/wem die für die Verarbeitung Verantwortlichen sie beschafft haben. Es wird immer notwendiger, Einzelnen proaktiver die Daten an sich *„in verständlicher Form"* sowie die Datenquelle mitzuteilen.

Durch die Wahrung von Geschäfts- oder Betriebsgeheimnissen können die Grundrechte des Einzelnen auf Privatsphäre und Datenschutz nicht generell außer Kraft gesetzt werden. Stattdessen ist ein sorgfältiges Ausbalancieren erforderlich, um beide miteinander in Einklang zu bringen[18]. Und auch die Entscheidung bezüglich der Offenlegung ist vielschichtig. Bei der Bewertung muss vielmehr geprüft werden, welche Informationen offen gelegt werden können und welche Offenlegungs- und Bewertungsverfahren es gibt. So können in manchen Fällen beispielsweise Vertrauenspersonen als Gutachter eingesetzt werden, anstatt dem Einzelnen oder der Öffentlichkeit sämtliche Einzelheiten preiszugeben[19].

Datenschutzbehörden (und andere Regulierungsbehörden wie zum Beispiel Verbraucherschutzbehörden, Wettbewerbsbehörden oder Finanz- und Versicherungsaufsichtsbehörden) sollten ebenfalls in der Lage sein, in die „Black Box" hineinzusehen.

Aus diesen Gründen empfehlen wir eine Stärkung der Bestimmungen der vorgeschlagenen EU-Datenschutzverordnung zur Transparenz sowie die konkrete Aufnahme der Offenlegung der „Logik der Entscheidungsfindung", der Daten selbst sowie der Datenquelle, damit gewährleistet ist, dass der verdeckten Profilerstellung ein Ende bereitet wird.

2.2 Bessere Instrumente zur Information des Einzelnen

Wichtig ist auch, dass Fortschritte dahingehend erzielt werden, wie Informationen gegenüber Einzelnen offen gelegt werden. Informationen über die Verarbeitung personenbezogener Daten müssen in einer klaren, verständlichen Sprache abgefasst werden und auf die entsprechende Zielgruppe zugeschnitten sein, damit sich dem Einzelnen komplexe Informationen sinnvoll erschließen und diese leicht zugänglich sind. Sobald die Verarbeitung komplexer wird, haben die für die Verarbeitung Verantwortlichen dafür Sorge zu tragen, dass Nutzer und Verbraucher besser informiert werden.

Mit diesen Maßnahmen soll wirksam dazu beitragen werden, dass die Interessen des von der Verarbeitung personenbezogener Daten Betroffenen gewahrt und nicht nur die für die Verarbeitung Verantwortlichen vor der Übernahme ihrer gesetzlichen Haftung geschützt werden. Wie auch im Fall des Verbraucherrechts sollten Unklarheiten in diesen Maßnahmen,

sofern vorhanden, zugunsten des Einzelnen und nicht zugunsten des Verantwortlichen ausgelegt werden. Sie sollten aber auch wahrheitsgemäß und ehrlich sein.

Die eher traditionellen Datenschutzrichtlinien sollten trotz ihrer Bedeutung für die Rechenschaftspflicht nicht die einzige oder sogar die wichtigste Informationsquelle für Einzelne sein. Datenschutzbehörden haben über lange Zeit hinweg eine „mehrschichtige Datenschutzerklärung“ [20] empfohlen, mit der die Betroffenen Schritt für Schritt über die sie betreffenden verarbeiteten Daten informiert werden. Dies bedeutet, dass dem Einzelnen die wesentlichen Informationen über die Verarbeitung zu dem Zeitpunkt mitgeteilt werden, an dem er aufgrund der Informationen eine Entscheidung treffen muss (etwa, wenn ein Einzelner wissen muss, ob eine heruntergeladene App auf seine Standortdaten zugreifen wird, bevor er sich überhaupt dazu entschließt, sie zu installieren), und dass weitere Informationen in anderen Formaten zur Verfügung gestellt werden, etwa über ausführlichere Informationen auf einer Website.

3. Jenseits von unverständlichen Datenschutzrichtlinien: Benutzerkontrolle und Teilhabe aller an den Vorteilen von Big Data

Global gesehen wird die derzeitige Debatte durch Missverständnisse bezüglich der Begriffe „Mitteilung“ und „Einwilligung“ beeinträchtigt. Im Sinne des europäischen Datenschutzrechts[21] hat der Begriff „Einwilligung“ niemals lange und undurchsichtige Datenschutzrichtlinien gemeint, die von Anwälten für Anwälte geschrieben waren und zu denen die Nutzer ihre „Einwilligung“ erteilen müssen, sofern sie die Inanspruchnahme des gewünschten Dienstes nicht völlig einstellen wollen. Stattdessen bedeutet er eine echte, freiwillig getroffene Entscheidung mit der Alternative, ohne jeden Nachteil „ja“ sagen zu können. Außerdem setzt er ein klares Verständnis dessen voraus, wozu man seine Zustimmung erteilt.

Für Organisationen ist eine Einwilligung zur Verarbeitung von Daten nicht immer Voraussetzung[22]. Doch wenn eine Einwilligung erforderlich ist, sollte diese tatsächlich erteilt werden: lediglich ein Kästchen anzukreuzen, ohne dass man versteht, wozu man seine Zustimmung erteilt hat, und ohne dass eine echte Wahlmöglichkeit besteht, reicht nicht aus, um unsere Einwilligung zu komplexen Big-Data-Anwendungen zu erteilen. Transparenz und Benutzerkontrolle müssen Wirklichkeit werden[23].

3.1 In Ermangelung einer Einwilligung: Widerspruchsrecht und Rücktrittsoption (*Opt-Out-Mechanisms*)

Das Recht, Widerspruch gegen die Verarbeitung einzulegen (das in der heutigen Praxis nicht sehr häufig ausgeübt wird), kann ein wirksames Instrument in der Hand von Einzelnen werden, wenn es als bedingungslose Rücktrittsoption „ohne Angabe von Gründen“ ausgeübt wird. Damit lässt sich unter bestimmten Umständen das richtige Gleichgewicht zwischen dem Recht des Einzelnen, ein gewisses Maß an Kontrolle über die ihn betreffenden Daten auszuüben, und der für Unternehmen für die Entwicklung, Innovation und bestmögliche Nutzung der online und offline erzeugten gewaltigen Datenmengen notwendigen Flexibilität erzielen[24].

Eine bedingungslose Rücktrittsoption bedeutet, dass ein Einzelner sich dessen bewusst ist, dass seine Daten verarbeitet werden, und dass er weiß, dass er - hätte er sich so entschieden - diese Einwilligung auch nicht geben kann. Er kann die Tatsache, dass seine Daten verarbeitet werden, uneingeschränkt anerkennen oder auch nicht, wobei er allerdings häufig dadurch nicht in ausreichendem Maße beeinträchtigt wird – bzw. sich dadurch ganz einfach nicht „gestört" fühlt –, als dass er die Voreinstellung tatsächlich ändert. Eine Rücktrittsoption beeinflusst einen Menschen subtil so, dass er seine Einwilligung erteilt, ohne ihm völlig sein Recht abzuerkennen, nicht zuzustimmen.

Insbesondere in Grenzfällen, in denen nur schwer ein Gleichgewicht zwischen den berechtigten Interessen des Verantwortlichen und den Rechten und Interessen der Betroffenen herzustellen ist, könnte eine gut durchdachte und funktionsfähige Rücktrittsoption, auch wenn sie den Betroffenen nicht unbedingt alle Informationen zur Verfügung stellt, die sie für eine gültige Einwilligung gemäß dem europäischen Datenschutzrecht benötigen[25], eine wichtige Rolle bei der Wahrung der Rechte und Interessen des Einzelnen spielen[26].

Als Gesellschaft müssen wir kluge Entscheidungen im Hinblick auf die Bedingungen treffen, zu denen die für die Verarbeitung Verantwortlichen eine echte Einwilligung einholen müssen, und im Hinblick darauf, wann wir uns mit einer einfachen Bewertung der Ausgewogenheit zwischen Interessen und Rücktrittsoption begnügen. Insbesondere müssen wir versuchen, zwischen Datenverarbeitungsvorgängen mit allgemeinen/gesellschaftlichen Vorteilen einerseits und solchen Vorgängen andererseits zu unterscheiden, die lediglich mit wirtschaftlichen Vorteilen für diejenigen verbunden sind, die die Daten verarbeiten. Wir müssen aber auch die potenziellen Auswirkungen auf die Betroffenen bewerten und diese sowie alle anderen maßgeblichen Faktoren gegeneinander abwägen[27].

Die Rücktrittsoption kann durch branchenweite Vereinbarungen erleichtert werden, solange diese wirksam und einfach umsetzbar sind. Es bedarf jedoch weiterer Anstrengungen, bevor einzelne Initiativen befürwortet werden können, da die bislang mit solchen Vereinbarungen gemachten Erfahrungen kaum konkrete Ergebnisse hervorgebracht haben[28].

3.2 Mehr als eine Einwilligung: Benutzerkontrolle und Vorteile für alle

Zugangsrecht und Datenübertragbarkeit

Das Recht auf Auskunft über und Berichtigung von personenbezogenen Daten ist einer der wesentlichen Grundsätze des europäischen Datenschutzrechts[29], das mit der fortschreitenden Big-Data-Analyse zunehmend an Bedeutung gewinnt. Einzelpersonen müssen in die Lage versetzt werden, ungerechte Behandlung besser zu erkennen und sich über Fehler infolge der Logik in Algorithmen zur Bestimmung von Annahmen und Vorhersagen zu beschweren, und ein starkes Recht auf Auskunft und Berichtigung ist eine Voraussetzung hierfür.

Allerdings üben nur ganze wenige Menschen diese Rechte in der Praxis aus[30]. Einer der Gründe, weshalb diese potenziell starken Auskunftsrechte sich in der Praxis nicht als leistungsstärkere Instrumente erwiesen haben, liegt darin, dass Menschen häufig keine Zeit oder auch kein Interesse daran haben, *„to indulge in transparency and access for their own sake"*[31] (sich Transparenz und Zugang um ihrer selbst willen zu leisten). Dies könnte sich allerdings dann ändern, wenn Einzelne die Möglichkeit erhalten, die sie betreffenden personenbezogenen Daten so zu nutzen, dass sie davon konkret und spürbar profitieren können. Dies könnte über die sogenannte „Featurization" des Datenschutzes erreicht werden; statt einem Verwaltungsaufwand gleichzukommen, könnte die Gewährung von

Auskunftsrechten ein Merkmal der Dienstleistung für die Kunden werden[32]. Ein Beispiel aus dem Alltag ist der Online-Zugriff auf Bankdaten.

Mit der Zunahme von Big Data verwenden Organisationen personenbezogene Daten für sekundäre Zwecke, die für die eigentliche Erbringung der Dienstleistungen nicht unbedingt notwendig sind. Sie sollten, sofern sie diese Praxis fortsetzen wollen, auch bereit sein, das durch die Verarbeitung personenbezogener Daten geschaffene Vermögen mit denjenigen zu teilen, deren Daten sie verarbeiten[33]. Dies ist ein grundsätzliches Gebot der Fairness - nicht nur ein ethisches Erfordernis.

Daten werden oft mit anderen Ressourcen verglichen, mit denen gehandelt werden kann, wie z. B. Öl, und zwar im Idealfall durch gleichermaßen gut informierte, an der Transaktion beteiligte Parteien. Die Märkte für personenbezogene Informationen sind allerdings von Transparenz, Fairness oder Effizienz weit entfernt. Die Kunden kennen in aller Regel den genauen Wert der personenbezogenen Daten, die sie im Tausch gegen „kostenlose Dienstleitungen“ hergeben, nicht. Daher erhalten sie für ihre personenbezogenen Daten auch keine angemessene Gegenleistung.

Wie und in welchem Ausmaß der Einzelne von dem Vermögen profitieren sollte, das bei der Verarbeitung seiner personenbezogenen Daten geschaffen wird, ist eine Schlüsselfrage, über die im Zusammenhang mit der Schaffung des digitalen Binnenmarktes nachgedacht werden muss.

Eine der Möglichkeiten, dem Einzelnen mehr Kontrolle an die Hand zu geben, die Vorteile von Big Data gemeinsam mit ihm zu nutzen und zugleich Anreize für eine effiziente und transparente Verarbeitung personenbezogener Daten zu schaffen, ist die Datenübertragbarkeit. Datenübertragbarkeit setzt voraus, dass Organisationen

- dem Einzelnen Zugang zu den ihn betreffenden Daten in einem portablen, interoperablen und maschinenlesbaren (mit anderen Worten, verwendbaren und wiederverwendbaren) Format gewähren,
- ihm die Änderung, Löschung, Übermittlung oder eine andere Weiterverarbeitung seiner Daten gestatten,
- ihm einen Wechsel des Anbieters gestatten (z. B. Übermittlung seiner Fotos, Bankunterlagen und Datensätze zu seiner körperlichen Leistungsfähigkeit oder seiner E-Mails an einen anderen Dienstleistungsanbieter), und
- ihm gestatten, seine Daten mithilfe von Anwendungen Dritter auszuwerten und nützliche Schlüsse daraus zu ziehen (z. B. Änderung seiner Ernährungs- oder Bewegungsgewohnheiten, Inanspruchnahme einer auf seine persönlichen Bedürfnisse abgestimmten Gesundheitsversorgung, klügere Anlageentscheidungen, Wechsel zu einem günstigeren Stromanbieter).

Mit den Möglichkeiten der Datenübertragbarkeit könnten Unternehmen und Einzelne die Vorteile von Big Data in einer ausgewogeneren und transparenteren Weise nutzen und dazu beitragen, dass das wirtschaftliche Ungleichgewicht zwischen den für die Verarbeitung Verantwortlichen einerseits und dem Einzelnen andererseits verringert wird. Damit könnte auch bewirkt werden, dass Einzelne von dem durch die Nutzung der sie betreffenden personenbezogenen Daten geschaffenen Wert profitieren: sie könnten die Daten für ihre eigenen Zwecke nutzen oder Dritten im Tausch gegen zusätzliche Dienstleistungen oder

gegen bar eine Nutzungslizenz erteilen. Außerdem könnten dadurch unlautere oder diskriminierende Praktiken auf ein Mindestmaß reduziert und die Risiken der Nutzung unrichtiger Daten für Entscheidungszwecke abgebaut werden.

Darüber hinaus ist Datenübertragbarkeit nicht nur für den Datenschutz, sondern auch für den Wettbewerb und den Verbraucherschutz von Vorteil: Sie kann insbesondere ein stärker von Wettbewerb geprägtes Marktumfeld fördern, indem die Kunden einfacher den Anbieter wechseln können (zum Beispiel im Zusammenhang mit Online-Banking oder im Fall von Energieanbietern im Rahmen intelligenter Netze). Sie kann aber auch zur Entwicklung zusätzlicher Mehrwertdienste durch Dritte beitragen, die auf Wunsch und mit der Einwilligung der Kunden Zugriff auf deren Daten haben. Damit wiederum könnten die Hindernisse beim Zugang zu neuen Märkten, die den Zugriff auf personenbezogene Daten voraussetzen, abgebaut und wettbewerbsfähigere, weniger monopolistisch ausgerichtete Marktstrukturen geschaffen werden[34].

Angesichts seiner Vorteile unterstützt der EDSB nachdrücklich die Aufnahme eines starken Rechts auf Datenübertragbarkeit in die vorgeschlagene EU-Datenschutzverordnung sowie gegebenenfalls die Aufnahme dieses Rechts in die einschlägigen sektorbezogenen Rechtsvorschriften, Verordnungen bzw. Leitfäden (z. B. in Bezug auf intelligente Verbrauchsmessung). Außerdem unterstützen wir staatliche oder private Initiativen zur Förderung der Datenübertragbarkeit.

Persönliche Datenräume

Ergänzend und auf der Grundlage der Datenübertragbarkeit könnte eine Möglichkeit, um Einzelnen eine bessere Kontrolle über ihre Daten, über diejenigen, die Zugriff darauf erhalten und zu welchem Zweck, an die Hand zu geben, die Nutzung personenbezogener Datenräume (auch als „Datenbestände“ und „Datenspeicher“ bezeichnet) sein. Zu den Beispielen für ständig aktualisierte „Big Data“ in Echtzeit, die in persönlichen Datenräumen gespeichert werden könnten, könnte der Standort eines Einzelnen gehören, der mithilfe von Sensoren in seinem Fahrzeug oder seines Mobiltelefons erfasst wird, oder sein Blutdruck und andere Daten zu seiner Gesundheit/körperlichen Leistungsfähigkeit, die anhand eines Fitness Tracker oder eines medizinischen Geräts erfasst werden.

Die Mitteilung der Europäischen Kommission zu Massendaten[35] bezieht sich speziell auf „persönliche Datenräume“[36] und fördert deren Nutzung als nutzerzentrierte, sichere und geschützte Orte für die Speicherung und den möglichen Handel mit personenbezogenen Daten. Wir teilen die Ansicht, dass innovative digitale Instrumente und Geschäftsmodelle auf der Grundlage gestärkter Verbraucherrechte gefördert werden sollten. Diese umfassen auch Mechanismen, dank derer Einzelne an der Nutzung und Verbreitung der sie betreffenden Informationen teilhaben und damit von einem solchen Datenverbund profitieren können.

Dadurch könnte eine Umstellung von Geschäftsmodellen, bei denen Organisationen zunehmend das Verhalten Einzelner online und offline verfolgen, ohne dass diese in voller Kenntnis der Sachlage sind oder ihre Einwilligung erteilt haben, auf ein Modell möglich werden, bei dem Einzelne die sie betreffenden Informationen für ihre eigenen Zwecke verwalten und einen Teil dieser Informationen austauschen, sofern sie dies wünschen, mit wem sie dies wünschen, und zwar zu einem angemessenen Wert sowie zusammen mit angemessenen Garantien[37]. Mithilfe von persönlichen Datenbeständen könnten einige der Bedenken bezüglich des Verlustes der persönlichen Kontrolle über personenbezogene Daten,

auf den vorstehend näher eingegangen wurde, als zentrale Anliegen bezüglich von Big Data ausgeräumt werden[38].

Die EU sollte prüfen, wie zuverlässige, vertrauenswürdige, benutzerfreundliche und interoperable Instrumente und Produkte gefördert werden können, und die damit verbundenen Vorteile, Einschränkungen und technologischen Herausforderungen genau unter die Lupe nehmen[39].

3.3 Neue, innovative Möglichkeiten, Einzelnen Informationen zur Verfügung zu stellen und ihnen Zugang und Kontrolle zu gewähren

Unternehmen und andere Organisationen, die viel Zeit und Mühe darauf verwenden, innovative Möglichkeiten zur Nutzung personenbezogener Daten ausfindig zu machen, sollten bei der Gestaltung **neuer, innovativer Möglichkeiten zur Bereitstellung von Informationen und zur Gewährung von Zugang und Kontrolle für Einzelne** dasselbe innovative Denken an den Tag legen[40].

Es sollten neue benutzerfreundliche Möglichkeiten entwickelt und angeboten werden, damit Einzelne eine auf Kenntnis der Sachlage gegründete Einwilligung erteilen oder diese verweigern können. Dem Einzelnen ein gewisses Maß an Kontrolle über die Datennutzung einzuräumen, ist häufig eine gesetzliche Vorgabe oder eine bewährte Vorgehensweise, die auch den für die Verarbeitung Verantwortlichen beim Aufbau von Vertrauen hilft.

So sollten Einzelne zum Beispiel in der Lage sein, mühelos die Verfolgung bzw. den Informationsaustausch auf ihren Geräten und Anwendungen an- und auszuschalten, und zwar je nach Standort, Zeit und Datum, nach Anwendung wie auch global. Es sollten aber auch bessere Möglichkeiten für die Berichtigung, Aktualisierung oder Löschung von Daten oder für die Änderung der Personen, die Zugriff darauf haben, oder die Überwachung derjenigen, die tatsächlich Zugriff darauf hatten, und für welche Zwecke, angeboten werden. Und dies bringt uns zu unserem nächsten Thema – Datenschutz und eingebauter Datenschutz.

4. Datenschutz und eingebauter Datenschutz

Mit Datenschutz und eingebautem Datenschutz sollen Privatsphäre und Datenschutz in die Gestaltungsvorgaben und die Architektur von Informations- und Kommunikationssystemen und -technologien eingebaut werden. Sie sind nicht auf technische Aspekte beschränkt, denn organisatorische Maßnahmen sind mindestens ebenso wichtig.

Technologie und privatsphärengerechte Verfahren können maßgeblich dazu beitragen, dass Transparenz und Benutzerkontrolle, wie vorstehend ausgeführt, Wirklichkeit werden. Gesetze, Verordnungen, Vertragsbedingungen, interne Verfahren und Datenschutzrichtlinien sind zwar wichtig, reichen jedoch an sich noch nicht aus. Einzelnen müssen **neue, innovative Möglichkeiten** angeboten werden, **um sie darüber zu informieren, was mit den sie betreffenden Daten geschieht, und ihnen die Kontrolle darüber zu ermöglichen.** Dies erfordert innovative und privatsphärengerechte Verfahren sowie privatsphärenfreundliche organisatorische Regelungen und Geschäftspraktiken. Innovative und verantwortungsbewusste Verfahren können u. a. die Ausübung der Zugangsrechte Einzelner, Widerspruch, Rücktrittsoption, Berichtigung sowie Datenübertragbarkeit fördern. Privatsphärenfreundliche Verfahren können aber auch von unschätzbarem Vorteil sein, wenn es um die Entwicklung neuer Geschäftsmodelle für die Wertschöpfung, beispielsweise aus Datenspeichern, geht.

Ein weiterer Bereich, in dem innovative technologische Lösungen gefördert werden müssen, bezieht sich auf den Begriff der „**Funktionstrennung**“. Falls eine Organisation, die Daten verarbeitet, daraus lediglich Trends und Zusammenhänge erkennen und keine gewonnenen Einsichten auf die betreffenden Personen anwenden möchte, könnte die „Funktionstrennung“ potenziell dazu beitragen, die Auswirkungen auf die Rechte von Einzelnen zu verringern und Organisationen zugleich die Möglichkeit einer Sekundärnutzung von Daten einzuräumen[41].

Die Funktionstrennung stellt darauf ab, technische und organisatorische Maßnahmen zu ergreifen, damit Daten, die für Forschungszwecke genutzt werden, anschließend nicht verwendet werden können, um in Bezug auf die Betroffenen „*to support measures or decisions*“ (Maßnahmen oder Entscheidungen zu unterstützen) (es sei denn, diese Betroffenen erteilen dazu ausdrücklich ihre Genehmigung)[42].

Außerdem können entsprechende **Anonymisierungstechniken** trotz all ihrer Unzulänglichkeiten nach wie vor dazu beitragen, dass Daten innerhalb einer Organisation, zwischen verschiedenen Organisationen oder bei ihrer Veröffentlichung, wie z. B. im Fall von „Offene-Daten“-Projekten, sicher genutzt oder ausgetauscht werden können[43]. Daten werden nicht einfach nur anonymisiert, indem einige unmittelbar identifizierenden Attribute aus einem Datensatz entfernt werden. Je größer und umfassender eine Datensammlung wird, desto mehr Möglichkeiten gibt es, diejenigen zu identifizieren, auf die sich die Daten beziehen, insbesondere dann, wenn die Daten für längere Zeit gespeichert und/oder ausgetauscht werden.[44]. Die sorgfältige Anwendung solcher Techniken in Verbindung mit anderen Garantien (z. B. Einschränkungen bei den Aufbewahrungsfristen, Zugangskontrolle) könnte allerdings in bestimmten Situationen zur Einhaltung der Datenschutzvorschriften beitragen.

Und schließlich muss bei Initiativen und Investitionen in die Nutzung und den Einsatz von Big Data ein angemessenes Maß an Sicherheit als wesentliche Voraussetzung für eine sozialverträgliche Nutzung von Big Data gesehen und davon ausgegangen werden, dass Risikobewertungs- und Sicherheitsmaßnahmen ein fester Bestandteil von Big Data sind.

5. Rechenschaftspflicht

Rechenschaftspflicht bedeutet, dass die für die Verarbeitung Verantwortlichen interne Mechanismen und Kontrollsysteme einrichten, die die Einhaltung der Vorgaben gewährleisten, und externen Interessengruppen, darunter Aufsichtsbehörden, Nachweise – einschließlich interner Richtlinien und Prüfberichte – vorlegen. Rechenschaftspflicht ist keine einmalige Angelegenheit: die regelmäßige Überprüfung, dass diese internen Kontrollsysteme auch weiterhin geeignet sind und alle Datenverarbeitungsvorgänge im Einklang mit den Rechtsvorschriften erfolgen, ist ein wesentlicher Bestandteil von Rechenschaftspflicht.

Bewährte und verantwortungsvolle Verfahren bestehen aus einer Vielzahl von Elementen. Privatsphäre, eingebauter Datenschutz und eine automatische, datenschutzfreundliche Voreinstellung, Datenschutzfolgenabschätzungen, Prüfungen und Zertifizierungen und die Verfügbarkeit der entsprechenden Sachkenntnis im Bereich Datenschutz, einschließlich eines Datenschutzbeauftragten in der Organisation, können allesamt zu einem verantwortungsvollen internen Kontrollsystem beitragen und einen wesentlichen Bestandteil davon ausmachen und sollten als geeignet gefordert und gefördert werden, da sie einen wichtigen Beitrag zu einer verantwortungsvollen Nutzung von Big Data leisten.

Die Entscheidung, was im Zusammenhang mit der Analyse von Big Data fair und rechtmäßig ist und was nicht, ist häufig schwierig.

Zu den wesentlichen Entscheidungen, die eine verantwortungsbewusste Organisation im Rahmen des europäischen Datenschutzrechts treffen muss, gehören die Fragen,

- ob eine Sekundärnutzung von Daten mit dem Grundsatz der Zweckbindung vereinbar ist,
- ob Daten, die ursprünglich in einem bestimmten Zusammenhang genutzt werden, für angemessen, relevant und verhältnismäßig erachtet werden, um auch in einem anderen Zusammenhang genutzt zu werden, und
- ob sich eine Organisation dann, wenn sie die Einwilligung des Einzelnen nicht erhält, bei der Verarbeitung von Daten auf ihr berechtigtes Interesse berufen kann.

Diese Einschätzungen beruhen zwar auf gesetzlichen Vorgaben, setzen jedoch häufig voraus, dass viele Faktoren umfassend gegeneinander abgewogen und geprüft werden, u. a. auch die Frage, ob die Datenverarbeitung den angemessenen Erwartungen der einzelnen Betroffenen entspricht oder ob sie zu einer unangemessenen Diskriminierung führen oder sich anderweitig negativ auf die betroffenen Personen oder die Gesellschaft insgesamt auswirken kann. Diese Einschätzungen werfen oft schwierige Fragen der Geschäftsethik und Fairness auf und lassen sich nicht darauf reduzieren, einfach nur Kästchen mit Fragen zur Compliance mechanisch abzuhaken. Je leistungsstärker Computer werden, desto akuter stellt sich auch die Herausforderung: so wurde bei Untersuchungen festgestellt, dass Computer präziser als Menschen sind, wenn es darum geht, anhand von „digitalen Fingerabdrücken" Charaktereigenschaften, politische Einstellungen und die körperliche Gesundheit vorherzusagen[45].

Aus diesen Gründen werden solche Einschätzungen am besten von einer multidisziplinären Gruppe (z. B. Informatiker, Ingenieure, Rechtsanwälte, Datenschutzbeauftragte, Statistiker, Datenforscher, Ärzte, Wissenschaftler oder Fachleute für Marketing, Versicherungswesen oder Finanzen) vorgenommen.

„Ethikräte" können gegebenenfalls einen gewissen Beitrag zu verantwortungsbewussteren internen Verfahren leisten. Sie könnten genauso wie ähnliche Gremien im Bereich der wissenschaftlichen Forschung innerhalb der Organisation Empfehlungen abgeben oder verbindliche Entscheidungen zu der Frage treffen, ob bestimmte Arten von Big-Data-Analysen rechtmäßig und ethisch vertretbar eingeführt werden können. Andere organisatorische Regelungen können jedoch genauso wirksam sein. Entscheidend ist, dass ein Handlungsrahmen eingerichtet wird, der dazu beiträgt, dass die Entscheidungen, die letztlich im Zusammenhang mit Datenverarbeitungsvorgängen getroffen werden, „ethisch", „fair" und „rechtmäßig" sind.

6. Das weitere Vorgehen: praktische Umsetzung der Grundsätze

Um den Herausforderungen in Verbindung mit Big Data gerecht werden zu können, müssen wir **Innovation zulassen und zugleich die Grundrechte schützen.** Hierzu sollten die bewährten Grundsätze des europäischen Datenschutzrechts gewahrt, jedoch auf neue Art und Weise angewandt werden.

6.1 Eine zukunftsorientierte Verordnung

Die Verhandlungen zu der vorgeschlagenen Datenschutz-Grundverordnung stehen kurz vor dem Abschluss. Wir haben die EU-Gesetzgeber nachdrücklich dazu aufgefordert, ein Datenschutzreformpaket zu verabschieden, das den rechtlichen Rahmen stärkt und

modernisiert, damit er im Zeitalter von Big Data wirksam bleibt; hierzu muss das Vertrauen des Einzelnen in Online-Aktivitäten und in den digitalen Binnenmarkt gestärkt werden[46].

In unserer Stellungnahme 3/2015 zusammen mit Empfehlungen für einen vollständigen Text des Verordnungsvorschlags haben wir deutlich gemacht, dass unsere derzeitigen Datenschutzgrundsätze, darunter Notwendigkeit, Verhältnismäßigkeit, Datensparsamkeit, Zweckbindung und Transparenz, Schlüsselprinzipien bleiben müssen. Sie bieten die Grundlage, die wir benötigen, um unsere Grundrechte in der Welt von Big Data schützen zu können[47].

Zugleich müssen diese Grundsätze gestärkt und wirksamer sowie moderner, flexibler, kreativer und innovativer angewandt werden. Sie müssen außerdem durch neue Grundsätze ergänzt werden, etwa Rechenschaftspflicht, Datenschutz und eingebauter Datenschutz und automatische, datenschutzfreundliche Voreinstellungen.

Mehr Transparenz, starke Rechte auf Auskunft über und Zugriff auf Daten sowie Datenübertragbarkeit und wirksame Rücktrittsoptionen können als Voraussetzungen dienen, damit Benutzer mehr Kontrolle über ihre Daten haben, und sie können auch zur Entwicklung effizienterer Märkte für personenbezogene Daten zugunsten von Verbrauchern wie auch Unternehmen beitragen.

Und schließlich wird auch die Ausweitung des Geltungsbereichs des EU-Datenschutzrechts auf Organisationen, die sich gezielt mit Einzelpersonen in der EU befassen, und die Ausstattung von Datenschutzbehörden mit den entsprechenden Befugnissen, um sinnvolle Rechtsbehelfe, einschließlich wirksamer Strafen im Sinne der vorgeschlagenen Verordnung, einzulegen bzw. zu verhängen, eine wesentliche Forderung für eine wirksame Durchsetzung unserer Rechtsvorschriften in einem globalen Umfeld sein. Dem Reformprozess kommt diesbezüglich eine entscheidende Rolle zu.

Für eine wirksame Durchsetzung der Rechtsvorschriften müssen unabhängige Datenschutzbehörden nicht nur mit den rechtlichen Befugnissen und mit schlagkräftigen Instrumenten, sondern auch mit den notwendigen Mitteln ausgestattet werden, damit sie ihre Kapazitäten an die Zunahme datengesteuerter Geschäfte anpassen können.

6.2 Wie bringt der EDSB diese Debatte voran?

Gute Regelungen sind zwar von maßgeblicher Bedeutung, reichen jedoch nicht aus. Unternehmen und andere Organisationen, die viel Zeit und Mühe in innovative Möglichkeiten für die Nutzung personenbezogener Daten investieren, sollten bei der Umsetzung von Datenschutzgrundsätzen das gleiche innovative Denken an den Tag legen. Datenschutzbehörden wiederum sollten die tatsächliche Einhaltung der Vorschriften durchsetzen und honorieren und es vermeiden, unnötige Bürokratie und Formalitäten aufzuerlegen.

Der EDSB möchte, wie in der EDSB-Strategie für 2015-2019 angekündigt, zur Förderung dieser Bemühungen beitragen.

Wir beabsichtigen die Einsetzung einer externen Ethik-Beratergruppe, der hochkarätige und unabhängige Persönlichkeiten mit Erfahrung in den unterschiedlichsten Fachbereichen angehören, die „*die Beziehungen zwischen Menschenrechten, Technologie, Märkten und Geschäftsmodellen im 21. Jahrhundert untersucht*“, die Auswirkungen von Big Data eingehend analysiert, die sich daraus ergebenden Veränderungen unserer Gesellschaften

bewertet und daran mitwirkt, die Themen zu benennen, die im Rahmen eines politischen Prozesses geklärt werden müssen[48].

Wir werden außerdem ein Modell für eine ehrliche Informationspolitik für EU-Organe entwickeln, die Online-Dienste anbieten, die für alle für die Verarbeitung Verantwortlichen einen Beitrag zu bewährten Verfahren leisten können.

Und schließlich werden wir auch Diskussionen fördern, beispielsweise mit dem Ziel, bewährte Verfahren zur Verbesserung von Transparenz und Benutzerkontrolle und zur Eruierung von Möglichkeiten oder persönlichen Datenspeichern und Datenübertragbarkeit aufzuzeigen, zu fördern und Anreize dafür zu bieten. Der EDSB möchte einen Workshop zum Schutz von Big Data für politische Entscheidungsträger und Personen, die große Mengen personenbezogener Daten bei EU-Einrichtungen verarbeiten, und für externe Experten organisieren und aufzeigen, wo weitere konkrete Handlungshilfen erforderlich sind, und die Arbeit des Internet Privacy Engineering Network („IPEN“) als interdisziplinäres Wissenszentrum für Techniker und Datenschutzexperten fördern.

(unterzeichnet)

Brüssel, den 19. November 2015

Giovanni BUTTARELLI

Europäischer Datenschutzbeauftragter

Anmerkungen

[1] Stellungnahme 4/2015 des EDSB.

[2] *Public Utilities Commission v. Pollak*, 343 U.S. 451, 467 (1952) (Justice William O. Douglas, dissenting).

[3] Am 25. Januar 2012 nahm die Europäische Kommission ein Paket zur Reform des europäischen Datenschutzrahmens an. Das Paket umfasst i) eine „Mitteilung“ (KOM(2012)9 endgültig), ii) einen Vorschlag für eine allgemeine „Datenschutzverordnung“ („vorgeschlagene Verordnung“) (KOM(2012)11 endgültig), und iii) einen Vorschlag für eine „Richtlinie“ zum Datenschutz im Bereich der Strafverfolgung (KOM(2012)10 endgültig).

[4] „Big Data bezieht sich auf das exponentielle Wachstum bei der Verfügbarkeit und der automatischen Nutzung von Informationen; gigantische digitale Datensätze im Besitz von Unternehmen, Regierungen und anderen großen Organisationen, die anschließend mittels Computeralgorithmen intensiv analysiert werden (daher der Name: Analytik)“, Stellungnahme 03/2013 der Artikel-29-Datenschutzgruppe zur Zweckbindung.

[5] Nachstehend folgen ein paar Beispiele für Anwendungen von Big Data. bei denen personenbezogene Daten verwendet werden (die Beispiele zeigen, welche Technologie hierzu in der Lage ist, und nicht, was unbedingt moralisch oder legal ist):

- Medizinische Forschung und patientenbezogene Medizin. Wenn Wissenschaftler Zugang zu unseren Daten über unser genetisches Profil, unsere Anamnese und unsere Lebensweise erhalten (z. B. über mobile Gesundheits- und Fitness-Apps, Daten auf sozialen Netzwerken, Daten zur Kundenbindung und Kreditkarten), könnte die medizinische Forschung bei der Verwendung dieser immensen und wertvollen Datensätze mithilfe der Analyse von Big Data möglicherweise revolutioniert werden, indem Wissenschaftler die Möglichkeit erhalten, neue Zusammenhänge und schließlich vielleicht neue Heilmittel für Krankheiten zu entdecken. Mit der Analyse von Big Data könnte auch vorhergesagt werden, ob ein Patient anfällig für eine Krankheit oder eine Nebenwirkung sein oder auf bestimmte medizinische Behandlungen ansprechen könnte. Damit könnten Ärzte wiederum eine individuellere und damit wirksamere medizinische Behandlung anbieten.
- Suchmaschinen beruhen auf Big Data, ebenso wie viele andere Online-Dienste im Bereich der Bewertung oder Empfehlung von Inhalten, Produkten oder Dienstleistungen. Verhaltensorientierte und gezielte Werbung, maßgeschneiderte Angebote und Ermäßigungen sowie personalisierte Empfehlungen von Medieninhalten, Hotels oder Gaststätten beruhen alle auf Big Data.
- Bei der Prüfung der Kreditwürdigkeit wird Big Data zur Beurteilung der Risiken einer Nichtzahlung von Finanzverbindlichkeiten genutzt.
- Bekämpfung von Steuerbetrug: Steuerbehörden, die Zugriff auf bestimmte Daten von anderen Regierungsbehörden oder von Privatunternehmen erhalten, können mithilfe von Big Data über Querabgleiche von Steuerdatenbanken mit anderen Informationen, etwa Fahrzeugbriefen, Kreditkartendaten oder Informationen im Besitz von Finanzvermittlern, Personen ausfindig machen, deren Ausgabe-/Anlageverhalten nicht mit ihren Steuerbeiträgen übereinstimmt.
- Bekämpfung von Terrorismus und organisierter Kriminalität: durch das Abhören und Sichten von Kommunikationsdaten vieler Menschen (verdächtig oder nicht) mithilfe leistungsstarker Analyse erhoffen sich Geheimdienste, Terroranschläge während der Vorbereitung aufzudecken.

[6] Vgl. beispielsweise:

- Entschließung zu Big Data vom Oktober 2014 durch die 36. Internationale Konferenz der Beauftragten für den Datenschutz und den Schutz der Privatsphäre („Entschließung der Internationalen Konferenz zu Big Data“);

- Internationale Arbeitsgruppe für Datenschutz in der Telekommunikation, Arbeitspapier zu Big Data und Datenschutz (55. Sitzung, 5./6. Mai 2014, Skopje) („Arbeitspapier der Berlin Group zu Big Data“);
- Stellungnahme der Artikel-29-Datenschutzgruppe zu den Auswirkungen der Entwicklung von Big Data auf den Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten in der EU, angenommen am 16. September 2014 („WP221“) („WP 29 Statement on big data“);
- UK Information Commissioner’s Office, Big data and data protection guide, Juli 2014 („ICO guide on big data“);
- Bericht der norwegischen Datenschutzbehörde „Big data-privacy principles under pressure“ 2013 („Norwegischer Bericht zu Big Data“).

[7] Vgl. Big Data: Seizing Opportunities, Preserving Values, Executive Office of the President, Mai 2014, Seite 10.

[8] Artikel-29-Datenschutzgruppe, Stellungnahme 3/2013 zur Zweckbindung, Anhang 2.

[9] Der Missbrauch unausgewogener Machtverhältnisse kann verschiedene Formen annehmen. Preisdiskriminierung ist eine davon. Damit können Unternehmen unterschiedlichen Menschen Waren oder Dienstleistungen zu unterschiedlichen Preisen anbieten, um so den Höchstpreis herauszuholen, den jeder Verbraucher zu zahlen bereit ist. Große Datensätze über individuelle Verhaltensmuster sind heutzutage ohne weiteres zugänglich und enthalten Informationen, die für eine personenspezifische Preisgestaltung potenziell nützlich sind. Eine gezielte Ansprache schutzwürdiger Verbraucher ist eine andere gängige Form von Missbrauch.

[10] Bruce Schneier, *Data and Goliath*, 2015, S. 238.

[11] Norwegischer Bericht zu Big Data, Seite 7, Ziffer 8.

[12] Darüber hinaus kann Big Data zur Bildung von „Filterblasen“ (bzw. persönlichen „Echokammern“) für den Einzelnen führen. In unserer zunehmend personalisierten Welt treffen Algorithmen Vorhersagen darüber, welche Informationen jeder von uns gerne angezeigt bekommen würde, und zwar auf der Grundlage dessen, was über uns bekannt ist (etwa unser Standort, unser bisheriges Klickverhalten und unsere Such- und Kaufhistorie). Jede uns angezeigte Information wird in immer komplexerer und undurchsichtigerer Weise gefiltert. Die Gefahr besteht darin, dass wir mit immer geringerer Wahrscheinlichkeit auf Informationen stoßen, die unsere Standpunkte in Frage stellen. Wir werden immer wirksamer in unseren eigenen kulturellen und ideologischen Blasen isoliert und von der übrigen Gesellschaft abgespalten.

[13] Das US National Consumer Law Center hat festgestellt, dass im Zusammenhang mit Kreditprodukten, die aufgrund nicht traditioneller datengesteuerter Prozesse verkauft wurden, ein effektiver Jahreszins von 134 % bis 748 % verlangt wurde; Big Data: A Big Disappointment for Scoring Consumer Credit Risk, März 2014. Im August 2015 wurde ein US-Patent erworben, das auch eine Technologie zur Prüfung der Bonität von Mitgliedern sozialer Netzwerke Einzelner umfasste, die mit diesen Einzelnen verbunden waren, um zu ermitteln, ob ein Darlehensantrag bearbeitet oder abgelehnt werden sollte; „Facebook Patent: Your friends could help you get a loan – or not“; (04.08.2015) http://money.cnn.com/2015/08/04/technology/facebook-loan-patent/. Im Oktober 2015 leiteten die Europäische Bankaufsichtsbehörde, die Europäische Wertpapier- und Marktaufsichtsbehörde und die Europäische Aufsichtsbehörde für das Versicherungswesen und die betriebliche Altersversorgung eine gemeinsame Untersuchung der Chancen und Risiken von Big Data ein.

[14] Zum Begriff „Black Box“ und der Bedeutung von Transparenz siehe z. B. „The Black Box Society, The Secret Algorithms That Control Money and Information“ von Frank Pasquale (Harvard University press, 2015).

[15] Gemäß Artikel 10 und 11 der Richtlinie 95/46/EG. Siehe auch Artikel 15.

[16] Zu den praxisnahen alltäglichen Beispielen, bei denen „die Logik der Entscheidungsfindung“ offen gelegt werden sollte, gehört auch eine personalisierte Kfz-Versicherung (auf der Grundlage von Daten aus einer Kfz-Sensorik zur Beurteilung des Fahrverhaltens); Bonitätsprüfdienste; oder auch ein Preisgestaltungs- und Marketingsystem, das bestimmt, wie viel Ermäßigung einem Einzelnen gewährt oder welche Medieninhalte ihm empfohlen werden.

[17] Daten, die hergeleitet werden, umfassen auch das Profil eines Einzelnen, beispielsweise seine Bonität oder das Ergebnis einer Bewertung seines Gesundheitszustands.

[18] Bei der Bewertung sollte außerdem dem Umstand Rechnung getragen werden, dass die Geheimhaltung nicht die einzige Möglichkeit zum Schutz von wirklich neuartigen Produkten und Dienstleistungen ist. So können viele wirklich innovative Algorithmen auch durch Rechte des geistigen Eigentums anstelle von Geschäftsgeheimnissen geschützt werden. Patente beispielsweise bieten ein hohes Schutzniveau für geistiges Eigentum und sorgen gleichzeitig für mehr Transparenz gegenüber einzelnen Betroffenen.

[19] In Bezug auf „qualifizierte Transparenz“ siehe z. B. Frank Pasquale: The Black Box Society, S. 160-165.

[20] Siehe beispielsweise Stellungnahme 10/2004 der Artikel-29-Datenschutzgruppe zum Thema Vorschriften über stärker harmonisierte Informationen (WP100), Stellungnahme 2/2009 der Artikel-29-Datenschutzgruppe zum Schutz der personenbezogenen Daten von Kindern (Allgemeine Leitlinien und Anwendungsfall Schulen) (WP160) und Stellungnahme 03/2013 der Artikel-29-Datenschutzgruppe zur Zweckbindung, Seite 16, sowie die Beispiele 9-10 und 11 in Anhang 3, Seite 52 und 53.

[21] Siehe Artikel 7 Buchstabe a der Richtlinie 95/46/EG.

[22] Die Stellungnahme 6/2014 der Artikel-29-Datenschutzgruppe über berechtigte Interessen bietet Handlungshilfen an und stellt eine Reihe von Kriterien vor, mit denen festgelegt werden kann, in welchen Fällen eine Organisation den Grund des berechtigten Interesses anführen kann und in welchen Fällen sie die Einwilligung der Betroffenen einholen muss.

[23] Zudem wird der Schutz der Privatsphäre häufig fälschlicherweise mit der Entscheidung gleichgesetzt, ob Einzelne gezielte Online-Werbung erhalten oder nicht, und benutzerfreundliche „Instrumententafeln“ bieten die Illusion von Kontrolle, ohne dass Einzelne tatsächlich in die Lage versetzt werden, sich gegen die Verfolgung entscheiden und trotzdem die Vorteile des Internets nutzen zu können. Nicht nur die gezielte Werbung an sich kann zu einer Verletzung der Privatsphäre führen, sondern vielmehr die Unfähigkeit Einzelner, eine Verfolgung generell zu vermeiden.

[24] Eine Organisation, die sich auf Artikel 7 Buchstabe f der Richtlinie 95/46/EG (berechtigtes Interesse) als Rechtsgrundlage für die Verarbeitung personenbezogener Daten beruft, muss Einzelnen das Recht gewähren, gemäß Artikel 14 Buchstabe a der Richtlinie unter bestimmten Umständen Widerspruch einzulegen. Zusätzlich zum Widerspruchsrecht gemäß Artikel 14 Buchstabe a kann eine Organisation aber auch beschließen, Einzelnen ein umfassenderes, allgemein anwendbares bedingungsloses Recht anzubieten, eine Rücktrittsoption auszuüben. Eine solche Rücktrittsoption ist im Fall der Direktwerbung gemäß Artikel 14 Buchstabe b der Richtlinie 95/46/EG bereits eine zwingende gesetzliche Vorgabe. Um diese Art der Rücktrittsoption „ohne Angabe von Gründen“ geht es in diesem Abschnitt. Siehe hierzu auch die Stellungnahme 6/2014 der Artikel-29-Datenschutzgruppe über berechtigte Interessen, Seite 44 ff. unter der Überschrift *„The right to object and beyond“ (Widerspruchsrecht und mehr - nur EN).*

[25] Gemäß Artikel 7 Buchstabe a der Richtlinie 95/46/EG.

[26] Stellungnahme 6/2014 der Artikel-29-Datenschutzgruppe über berechtigte Interessen gibt eine Orientierungshilfe sowie Beispiele an die Hand, unterstreicht jedoch die Bedeutung einer Einzelfallbewertung. Siehe insbesondere Seite 31-33, Seite 44-47 sowie die Beispiele 4 und 5 in Anhang 2 der Stellungnahme, Seite 59.

[27] Idem.

[28] Viel Kritik wurde insbesondere an Brancheninitiativen zugunsten einer Rücktrittsoption bei verhaltensbezogener Online-Werbung und Do Not Track geübt. Siehe zum Beispiel http://www.nytimes.com/2014/12/27 /opinion/the-slow-death-of-do-not-track.html?_r=0.

[29] Siehe Artikel 8 Absatz 2 der Charta der Grundrechte der Europäischen Union und Artikel 12 der Richtlinie 95/46/EG.

[30] Siehe beispielsweise S. 26 ff, Omer Tene and Jules Polonetsky (2012), „Big Data for All: Privacy and User Control in the Age of Analytics", 11 Northwestern Journal of Technology and Intellectual Property 239 (2013), abrufbar unter http://papers.ssrn.com/sol3/papers.cfm?abstract_id=2149364.

[31] Idem.

[32] Idem.

[33] Dieses Gebot gilt zusätzlich zum Gebot des gesunden Menschenverstandes und darüber hinaus, um die von Big-Data-Unternehmen möglicherweise verursachten negativen externen Auswirkungen auf ein Mindestmaß zu verringern und auszugleichen, etwa erhöhte Sicherheitsrisiken für diejenigen, deren Daten sie verarbeiten.

[34] Siehe auch Absatz 26 der Vorläufigen Stellungnahme des Europäischen Datenschutzbeauftragten zu Privatsphäre und Wettbewerbsfähigkeit im Zeitalter von Big Data, angenommen am 26. März 2014. Das Potenzial der Datenübertragbarkeit wird darüber hinaus aber auch in der Stellungnahme 3/2013 der Artikel-29-Datenschutzgruppe zur Zweckbindung und in ihrer Stellungnahme 6/2014 über berechtigte Interessen hervorgehoben. Beide Stellungnahmen beziehen sich auch konkret auf Initiativen wie „midata" im Vereinigten Königreich (und die entsprechende Initiative in Frankreich), die auf dem Leitprinzip beruhen, dass Daten wieder an die Kunden „zurückgegeben" werden sollten, damit sie sie für ihre eigenen Zwecke nutzen können. Weiterführende Informationen zu Midata im Vereinigten Königreich und ähnlichen Initiativen in Frankreich siehe http://www.midatalab.org.uk/, https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/34747/12-983-midata-company-briefing-pack.pdf und http://mesinfos.fing.org/.

[35] Mitteilung der Kommission „Für eine florierende datengesteuerte Wirtschaft", in der die Strategie der Kommission zu Massendaten dargelegt wird, COM(2014) 442 final.

[36] Abschnitt 4.2.3.1, Absatz 4.

[37] Siehe beispielsweise Doc Searls, *The Intention Economy: When Customers Take Charge* (Boston: Harvard Business Review Press, 2012).

[38] Siehe zum Beispiel Ira S. Rubinstein, Big Data: The End of Privacy or a New Beginning? International Data Privacy Law, 2013, Vol 3, No 2.

[39] Zu den noch offenen Fragen gehören Sicherheit, Haftung und technische Durchführbarkeit. Geklärt werden müsste außerdem, wessen Interesse persönliche Datenräume dienen. Und schließlich muss darauf hingewiesen werden, dass persönliche Datenräume personenbezogen Daten nicht „verkaufen", sondern vielmehr Dritten die Möglichkeit einräumen sollten, diese für bestimmte Zwecke und bestimmte Zeiten gemäß den Bedingungen zu „nutzen", die von den Einzelnen selbst festgelegt werden, und zwar unter Achtung aller weiteren Datenschutzgarantien.

[40] Die Einwilligung sollte ausreichend differenziert sein und sich – auch wenn die Weiterverarbeitung der Daten durch dieselbe Einrichtung erfolgt – auf die einzelnen Datenverarbeitungsvorgänge für jeden Dienst erstrecken. Auch für die Kombination von Daten für einen anderen Zweck ist eine spezielle Einwilligung einzuholen.

[41] Siehe Seiten 27, 29, 30 und Anhang 2 der Stellungnahme 3/2013 der Artikel-29-Datenschutzgruppe zur Zweckbindung.

[42] Es gibt kaum Daten über Erfahrungen mit einer wirksamen Umsetzung der Funktionstrennung außerhalb bestimmter Fachorganisationen wie z. B nationale statistische Ämter und Forschungseinrichtungen. Um Daten auch für sekundäre Anwendungen voll und ganz nutzen zu können, ist es von zentraler Bedeutung, dass andere Organisationen ihre Fachkenntnisse aufbauen und vergleichbare Garantien zum Schutz vor Datenmissbrauch anbieten.

[43] Weitere Informationen zu der Frage, wie beurteilt werden kann, wann aggregierte Datensätze als offene Daten veröffentlicht werden können, siehe Abschnitt 6 der Stellungnahme 06/2013 der Artikel-29-Datenschutzgruppe zu Offenen Daten („Open Data“) und der Weiterverwendung von Informationen des öffentlichen Sektors („PSI“).

[44] Eine Analyse der derzeit verfügbaren Anonymisierungstechniken hat die Artikel-29-Datenschutzgruppe in ihrer Stellungnahme 5/2014 zu Anonymisierungstechniken vorgelegt.

[45] Computer-based personality judgments are more, accurate than those made by humans, Wu Youyoua, Michal Kosinski und David Stillwell. Dezember 2014.

[46] Stellungnahme 3/2015 des EDSB.

[47] Wir müssen der Versuchung widerstehen, das derzeitige Schutzniveau in dem Bemühen zu verwässern, der vermeintlichen Notwendigkeit eines lascheren Regulierungsansatzes im Zusammenhang mit Big Data nachzugeben. Datenschutz muss sich auch weiterhin auf die Verarbeitung in Gänze beziehen, und zwar nicht nur einschließlich der Nutzung, sondern auch der Erhebung der Daten. Auch pauschale Ausnahmen bei der Verarbeitung pseudonymer Daten oder der Verarbeitung öffentlich zugänglicher Daten sind nicht gerechtfertigt. Die Definition des Begriffs personenbezogene Daten muss intakt bleiben, wobei allerdings weitere Erläuterungen im Text der Verordnung selbst denkbar wären. Die Definition muss sich auf alle Daten erstrecken, die Einzelne betreffen, die - durch den für die Verarbeitung Verantwortlichen oder durch andere - identifiziert und ausgewählt sind oder identifiziert und ausgewählt werden könnten.

[48] Stellungnahme 4/2015 des EDSB.